Using finite binomial series to Prove results in prime numbers and congruences

By Shazly abdullah

ABSTRACT

In this work used an algebraic method that uses elementary algebra and binomial theorem. To create finite binomial series $\mathrm{L_n(k,h,x)} = \mathrm{V_n{}^q(k,h,x)} + \mathrm{S_n(k,h)}$.This is a type of series that has several properties in variables such as if $\mathrm{x} = 1$ then $\mathrm{L_n(k,h,1)} = \mathrm{S_n(k,h)}$ where $\mathrm{V_n{}^q(k,h,1)} = 0$. We used these series to prove results in congruences and prime numbers ,for example,we proved if $\mathrm{a^n} \equiv 1(\mathrm{mod\ m})$ where $\mathrm{n} = \mathrm{g} + \mathrm{d}$ and n is an odd then $\mathrm{d^n} \equiv -1(\mathrm{mod\ m})$, $\mathrm{a,d,n} \in \mathbb{N}$. And in prime to numbers , such as , if $p^m = x^2 + k$ where $k^{p^{m-1}\left(\frac{p-1}{2}\right)} \equiv -1\big(mod\ \ p^m\big)$is a also obtained several results in finite series.

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 the most important theorems in number theory because it is related to many theorems and definitions in number theory, for example, Primitive roots can be defied

In this work, elementary algebra binomial theorem, and difference of tow nth power are used to created finite series in an algebraic method, Similar the method used to solve recurrence relations in combinations[*see K.H.Rosen* 244,245] and that use generating functions and basic operations to solve the recurrence . In this work we used basic operations and binomial theorem instead of generating functions to create a kind of series with specific properties, then we used series to create congruence with specific properties. Through this process, we reached the theorem. 1 theorem.2 in primitive roots and several results in finite series.

according binomial theorem and difference of tow nth power theorem if n a positive integer and x y real numbers then

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

And

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

2. proof basic series

First we will create the basic infinite series creation is done in three parts . The first part consists of equation 2.1 to equation 2.3 in this part use basic operations and difference of tow nth power theorem to construct. It the second part consists of equation 2.4 to equation 2.9 in this part we will use equation 2.1 and the binomial theorem to create it. The third part consists of the last equation, we deduce the last equation from 2.9.

Basic infinite binomial series. Let n is an odd $k, g, u,$ real functions then

$$L^n{}_n(k, g, u) = V_n{}^n(k, g, u) + S_n(k, g)$$

Where

$$L_n{}^n(k, g, u) = \frac{u^n + (k - g)^n}{k + k - g} - m\left(\frac{g^n - 1}{g - 1}\right)$$

And

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

And

$$S_n(k, h) = -km\left(\frac{g^{n-1} - 1}{g - 1}\right) + km\sum_{j=1}^{n-2}(-1)^{j-1}(k - g)^j\left(\frac{g^{n-1} - 1}{g - 1} - \left(g^{n-2} + g^{n-3} \dots\dots\dots . g^{n-j-1}\right)\right)$$

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

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

Then

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

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

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

Then

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

We have let

2.1 $$w^q{}_n(k,g,u) = u^q(k-g)^n - m(-g)^n$$

2.2 $$z^q{}_n(k,g,u) = (u^q - m)(k-g)^n$$

2.3 $$c_n(k,g) = m\mathrm{k}\sum_{j=1}^{n}(k-g)^{j-1}(-g)^{n-j}$$

Note in this part we used expansion difference of tow nth power theorem and basic operations to create the equation(2.1) at we subtract $(k-g)^n$, and multiply m on both sides , then add $u^q(k-g)^n$ both sides then

2.4 $$W_n{}^q(k,h,x) = Z_n{}^q(k,g,u) + C_n(k,g)$$

In this second and final part to create the basic series we will use expansion of the binomial theorem and equation(2.1) to create it then according the binomial theorem , we find

$$\frac{u^n + (k-g)^n}{u+k-g}$$
$$= u^{n-1} - u^{n-2}(k-\mathrm{g}) + u^{n-3}(k-g)^2 - u^{n-4}(k-g)^3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(k-g)^{n-1}$$

By subtract $m\left(\frac{g^n-1}{g-1}\right)$ from both sides of the equation $\frac{u^n+(k-g)^n}{u+k-g}$ and the distribution of the terms of the expansion of the equation $m\left(\frac{g^n-1}{g-1}\right)$ between the terms of the expansion of the equation $\frac{u^n+(k-g)^n}{u+k-g}$ then we have that

$$\frac{u^n + (k-g)^n}{u+(k-g)} - m\left(\frac{g^n-1}{g-1}\right)$$
$$= u^{n-1} - m - u^{n-2}(k-\mathrm{g}) - mg + u^{n-3}(k-g)^2 - mg^2 - u^{n-4}(k-g)^3$$
$$- mg^3 \ldots\ldots\ldots\ldots\ldots..(k-g)^{n-1} - mg^{n-1}$$

By extracting the common factor between the terms we find that

$$\frac{u^n + (k-g)^n}{u+k-g} - m\left(\frac{g^n-1}{g-1}\right)$$
$$= u^{n-1} - m - (u^{n-2}(k-\mathrm{g}) + mg) + (u^{n-3}(k-g)^2 - mg^2)$$
$$- (u^{n-4}(k-g)^3 + mg^3) \ldots\ldots\ldots\ldots((k-g)^{n-1} - mg^{n-1})$$

The terms of the $m\left(\frac{g^n-1}{g-1}\right)$ are distributed between the terms of $\frac{u^n+(k-g)^n}{u+k-g}$ and extraction of the common factor we notice that the first term $-u^{n-2}f(k-\mathrm{g})$ has changed $-(u^{n-2}(k-\mathrm{g})+mg)$ and the second term $u^{n-3}(k-g)^2$ has changed $(u^{n-3}(k-g)^2-mg^2)$ all terms changed untie last term $((k-g)^{n-1}+mg^{n-1})$ according to the equation (2.1) $w_j{}^n(k,g,u) = u^n(k-g)^j - m(-g)^j$ so it can be compensation $w^{n-2}(k,g,u)$ in second term and $-(u^{n-2}(k-\mathrm{g})-mg)$ and $w_2{}^{n-3}(k,g,u)$ in third term $(u^{n-2}(k-g)^2-mg^2)$ then it can compensation all $1 \le j \le n$ note $w_0{}^{n-1}(k,g,u) = u^{n-1} - m$ then we have

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

Let

$$L_n(k,g,u) = \frac{u^n + (k-g)^n}{u+k-g} - m\left(\frac{g^n-1}{g-1}\right)$$

Then

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

Equation(2.4) form $w^n{}_n(k,g,u) = z_n{}^n(k,g,u) + c_n(k,g)$ then we have that

2.5 $$L_n(k,g,u) = \sum_{j=0}^{n}(-1)^j z_j{}^{n-j-1}(k,g,u) + \sum_{j=0}^{n}(-1)^j c_j(k,g)$$

We note from the equation (2.1) $z_j{}^n(k,g,u) = (u^n - m)(k-g)^j$ and the equatin (2.2) $c_j(k,g) = km\sum_{r=1}^{j}(k-g)^{r-1}(-g)^{j-r}$ so by compensation the right side $z_j{}^n(k,g,u)$ and $c_j(k,g)$ in equation (2.5) also note $c_0(k,g) = 0$ then we have

$$L_n(k,g,u) = \sum_{j=0}^{n-1}(-1)^j\left(u^{n-j-1} - m\right)(k-g)^j + \mathrm{km}\sum_{j=1}^{n-1}\sum_{r=1}^{j}(-1)^j(k-g)^{r-1}(-g)^{j-r}$$

Let

$$V^n{}_n(k,g,u) = \sum_{j=0}^{n-1}(-1)^j\left(u^{n-j-1} - m\right)(k-g)^j$$

And

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

Then we have

2.6 $$L_n(k\mathrm{g},u) = V_n{}^n(k,g,u) + S_n(k,g)$$

Note $g^{j-r}(-h) = (-1)^{j-r}g^{j-r}(h)$ and $(-1)^j(-1)^{j-r} = (-1)^{2j-r} = (-1)^r$ if j and r is odd or even note we find in $s_n(k,h)$ tow signs$(-1)^j(-1)^{j-r}$ so they can by combined in $(-1)^r$ then we find that

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

Then we have

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

By analyzing all the complex terms of the $S_n(k,g)$ we find that

$$S_n(k,h) = km\Big((-1) + \big(-g + (k-g)\big) + (-g^2 + g(k-g) - (k-g)^2) - (-g^3 + g^2(k-\mathrm{g}) - g(k-g)^2 + (k-g)^3) \dots\dots\dots.. (-g^{n-1} + g^{n-2}(k-\mathrm{g}) - g^{n-3}(k-g)^2 + g^{n-4}(k-g)^3 \dots\dots\dots\dots..(k-g)^{n-2})\Big)$$

In $S_n(k,h)$ a all compound terms have been dismantled note if we add for every first term in the complex term we find that $-(-1 + g \dots\dots\dots g^{n-2})$ then we adding the terms to include that $(k-\mathrm{g})$ finding that $(1 + g \dots\dots. g^{n-2})$ then the terms that include $(k-g)^2$ we find that$\left(-(1+g\ldots\ldots..g^{j-3})\right)$ 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

$$s_n(k,h) = \mathrm{km}\big(-(1+g+g^2\ldots\ldots\ldots g^{n-2}) + (k-g)\big((1+g+g^2+g^3\ldots\ldots\ldots.g^{n-3})\big)$$
$$-(k-g)^2(1+g+g^2+g^3\ldots\ldots\ldots.g^{n-4})\ldots\ldots\ldots.(k-g)^{n-1}\big)$$

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

$$-(1+g+g^2\ldots\ldots\ldots.g^{n-2}) = \frac{g^{n-1}-1}{g-1}$$

$$(k-g)(1+\mathrm{g}\ldots\ldots\ldots.g^{n-3}) = (k-g)\left(\frac{g^{n-1}-1}{g-1} - g^{n-2}\right)$$

$$(k-g)^2(1+g\ \ldots\ldots\ldots.g^{n-4}) = (k-g)^2\left(\frac{g^{n-1}-1}{g-1} - g^{n-2} - g^{n-3}\right)$$

In $S_n(k,h)$ note can abbreviation of all terms that include $(k-\mathrm{g})\,,(k-g)^2,(k-g)^3\ldots\ldots(k-g)^{n-1}$ in the second term $\left(\frac{g^{n-1}}{g-1}\right)$ in $(k-g)^2$ on $\left(\frac{g^{n-1}}{g-1} - \mathrm{g}^{n-1}\right)$ and in the third on $\left(\frac{g^{n-1}}{g-1} - \mathrm{g}^{n-1} - g^{n-2}\right)$ then all terms can be converted $(k-g)^{j-1}(1+g+g^2\ldots..g^{n-\mathrm{j}-1}) = \left(\frac{g^{n-1}}{g-1} - \mathrm{g}^{n-1} - g^{n-2}\ldots\ldots g^{n-j}\right)$all $1 \leq j \leq n-1$we notice that in $S_n(k,h)$ each term the values

$$S_n(k,h) = \mathrm{km}\left(\frac{g^{n-1}-1}{g-1}\right) + \mathrm{km}\sum_{j=1}^{n-2}(-1)^{j-1}(k-g)^j\left(\frac{g^{n-1}-1}{g^n-1} - \left(g^{n-2}+g^{n-3}\ldots\ldots.g^{n-j-1}\right)\right)$$

2.7 $$L_n(k,g,u) = \frac{u^n+(k-g)^n}{u+k-g} - m\left(\frac{g^n-1}{g-1}\right)$$

2.8 $$V^n{}_n(k,g,u) = \sum_{j=0}^{n-1}(-1)^j\left(u^{n-j-1}{}_j - m\right)(k-g)^j$$

2.9 $$S_n(k,h)$$
$$= -\mathrm{km}\left(\frac{g^{n-1}-1}{g-1}\right) + \mathrm{km}\sum_{j=1}^{n-2}(-1)^{j-1}(k-g)^j\left(\frac{g^{n-1}-1}{g-1} - \left(g^{n-2}+g^{n-3}\ldots..g^{n-j-1}\right)\right)$$

3.proof theorem.1 and theorem .2

In this section we will use the basic series $L_n(u,k,g) = V^n{}_n(u,k,g) + S_n(k,g)$ in prove the theorem.1 and use the theorem.1 to prove theorem. let in $V_n{}^n(u,k,g),\ u=1\ and\ m=1$ then we find

Theorem.1 let d g a positive integers and n is an odd where $m = g + d$then

If

$$g^n \equiv 1(mod\ m)$$

Then

$$d^n \equiv -1(mod\ m)$$

Proof theorem.1

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

Then

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

Then

$$L_n(u,k,1) = 0 + S_n(k,g)$$

According to the equations, (2,7, 2.8 ,2.9) we find that

$$\frac{1+(k-g)^n}{1+k-g} - \frac{g^n-1}{g-1}$$
$$= -\mathrm{k}\left(\frac{g^{n-1}-1}{g-1}\right)$$
$$+ \mathrm{k}\sum_{j=1}^{n-2}(-1)^{j-1}(k-g)^j\left(\frac{g^{n-1}-1}{g-1} - \left(g^{n-2}+g^{n-3}\ldots\ldots.g^{n-j-1}\right)\right)$$

Let

$$k = d + g$$

Then

$$\frac{1+(d+g-g)^n}{1+d+g-g} - \frac{g^n-1}{g-1}$$
$$= -(d+g)\left(\frac{g^{n-1}-1}{g-1}\right)$$
$$+ (d+g)\sum_{j=1}^{n-2}(-1)^{j-1}(d+g-g)^j\left(\frac{g^{n-1}-1}{g-1} - \left(g^{n-2}+g^{n-3}\ldots\ldots..g^{n-j-1}\right)\right)$$

We have that

$$\frac{1+d^n}{1+d} - \frac{g^n-1}{g-1}$$
$$= -(d+g)\left(\frac{g^{n-1}-1}{g-1}\right)$$
$$+ (d+g)\sum_{j=1}^{n-2}(-1)^{j-1}d^j\left(\frac{g^{n-1}-1}{g-1} - \left(g^{n-2}+g^{n-3}\ldots\ldots..g^{n-j-1}\right)\right)$$

Then

$$\frac{d^n+1}{d+1} = \frac{g^n-1}{g-1} - (d+g)\left(\frac{g^{n-1}-1}{g-1}\right)$$
$$+ (d+g)\sum_{j=1}^{n-2}(-1)^{j-1}d^j\left(\frac{g^{n-1}-1}{g-1} - g^{n-2} - g^{n-3}\ldots\ldots.g^{n-j-1}\right)$$

Then we note from 3.1 $(d+1, d+g) = (\mathrm{g}-1, d+\mathrm{g}) = 1$ then we find that if n is an odd $g^n \equiv 1(mod\, m)$ where $m = d+g$ then $d^n \equiv -1(mod\, m)$

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

Theorem.2 if $q = g^{2^m} + d\ and\ \ \varphi(q) = 2^m n$ where $m > 0$ and n is an odd $\varphi(q)$ Euler function then

$$d^n \equiv -1(mod\, n)$$

Proof. according theorem.1 if $g^n \equiv 1(mod\ m)$ where $m = g + d$ and n is an odd then $d^n \equiv -1(mod\ m)$

Then let $q = g^{2^k} + d$ and $\varphi(q) = 2^k n$ where n is an odd according Euler theorem $(g)^{\varphi(q)} \equiv 1(mod\ q) = \left(g^{2^k}\right)^n \equiv 1(mod\ q)$ then form theorem.1 $d^n \equiv -1(mod\ q)$

Theorem.3 let p prime number and $p = x^2 + g$ where $p = 4n + 3$ then

$$g^{n+1} \equiv -1(mod\ p)$$

Proof. Let $q = p\ and\ \ k = 1$

4.Diophantine Equations and prime numbers

Theorem.4 Let p prime number where $p^m = x^2 + j\ \ and\ \ p \equiv 1(mod\ \ 2)$ then

$$j^{p^{m-1}\left(\frac{p-1}{2}\right)} \equiv -1(mod\ \ p^m)$$

Proof. Let in theorem.2 $q = p^m\ \ and\ \ \ k = 1$

Theorem.5 let v p g prime numbers where $vgp \equiv 1(mod\ \ 8)$ and $gpv = x^8 + y^2$ then

$$y^{\frac{\varphi(pgv)}{4}} \equiv -1(mod\ \ qgp)$$

Proof. Let in theorem.2 $q = vpg\ \ \ \ and\ \ \ k = 3$

Theorem.6 if $y^2 = x^3 - h$ where x is an odd and $x = 4n + 3$ then

$$h^{x^2(n+1)} \equiv -1(nod\ \ x^3)$$

Proof. We find $y^2 = x^3 - h = x^3 = y^2 + h\ \ then$ Let in theorem.1 $q = x^3\ \ \ k = 1\ \ \ d = h$

References

1. H. S. Rose . A Course in Number Theory " Oxford Science publications (1988).
2. K. M. Rose, Elementary Number Theory" 4th Edition Addison- Wesley (2000)
3. James. 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