The relationship between the $\varphi(n)$ function and solutions of Diophantine equations

By Shazly Abdullah

**ABSTRACT.** In this work we used an algebraic method that uses elementary algebra. To create series. We used the series and Euler function $\varphi(n)$ to find solutions to some types of Diophantine equations such as $p = dn - n + 1$. We found a relationship between the solutions of the Diophantine equations and solutions of some types of congruences that use the $\varphi(n)$ function. This relationship is the results that relate the solutions of congruence to the solution of the equations.

**Key word:** series, Diophantine equation, congruences, Euler function

1. **INTRODUCTION**

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

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

And

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

2. **basic series**

**Theorem 1** let $k$ and $g$ real numbers where $n$ is odd then

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

**Theorem 2** let $\varphi(n)$ Euler function where $\varphi(m) = d(n - 1)$ where $n$ in an odd where $a^d \not\equiv 1_{(mod \ m)}$, $(a, m) = 1$, $\forall a \in \mathbb{N}$ then

\[\frac{m^n + 1}{m + 1} \equiv \frac{a^d - 1}{a^d - 1}_{(md \ m)}\]

**Theorem 3** if $p$ prime number and $p = dn - n + 1$ where $n$ is odd $(p, a) = 1$ then

1
Theorem 4 let \( p \) prime number and \( a \) a positive integer \( a^{p^{m-1}} \neq 1 \mod p^m \) then

\[
\frac{p^{mp} + 1}{p^m + 1} \equiv \frac{a^{p^m} - 1}{a^{p^{m-1}} - 1} \mod p^m
\]

In this section we will create the basic series

**Basic series.** Let \( n \) is an odd \( k, g, u \), real numbers then

\[
L_n^n(k, g, u) = V_n^n(k, g, u) + S_n(k, g)
\]

Where

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

And

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

And

\[
S_n(k, h) = -km\left(\frac{g^{n-1} - 1}{g - 1}\right)
\]

\[
+ km \sum_{j=1}^{n-2} (-1)^{j-1}(k - g)^j\left(\frac{g^{n-1} - 1}{g - 1} - (g^{n-2} + g^{n-3} \ldots \ldots + g^{n-j-1})\right)
\]

**Proof.** let \( k, g, u \) real number 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

\[
-(g)^n = -(k - g)^n + k \sum_{j=1}^{n} (k - g)^{j-1}(-g)^{n-j}
\]

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

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

Then

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

According difference nth power theorem if \( n \) is odd we have
\[
\frac{u^n + (k-g)^n}{u + k - g} = u^{n-1} - u^{n-2}(k-g) + u^{n-3}(k-g)^2 - u^{n-4}(k-g)^3 \ldots (k-g)^{n-1}
\]

And
\[
m\left(\frac{g^n - 1}{g - 1}\right) = g^{n-1} + g^{n-2} + g^{n-1} \ldots 1
\]

By subtracting \(m\left(\frac{g^n - 1}{g - 1}\right)\) from \(\frac{u^n + (k-g)^n}{u + k - g}\) then
\[
\frac{u^n + (k-g)^n}{u + (k-g)} - m\left(\frac{g^n - 1}{g - 1}\right)
\]
\[
= u^{n-1} - m - u^{n-2}(k-g) - mg + u^{n-3}(k-g)^2 - mg^2 - u^{n-4}(k-g)^3
\]
\[
- mg^3 \ldots (k-g)^{n-1} - mg^{n-1}
\]

By extracting the common factor between the terms we find that
(2) \[\frac{u^n + (k-g)^n}{u + (k-g)} - m\left(\frac{g^n - 1}{g - 1}\right)\]
\[
= u^{n-1} - m - (u^{n-2}(k-g) + mg) + (u^{n-3}(k-g)^2 - mg^2)
\]
\[
- (u^{n-4}(k-g)^3 + mg^3) \ldots ((k-g)^{n-1} - mg^{n-1})
\]

So we note in equation (2) term (1) equal \(u^{n-1} - m\) and term(2) equal \(u^{n-2}(k-g) + mg\) and term (3) equal \(u^{n-3}(k-g)^2 - mg^2\) so From equation (1) we have
\[u^q(k-g)^n - m(-g)^n = (u^q - m)(k-g)^n + mk\sum_{j=1}^{n} (k-g)^{j-1}(-g)^{n-j}\]

Let \(W_n^q(k,g,u) = u^q(k-g)^n - m(-g)^n\)

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

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

So (3) \[W_n^q(k,g,u) = Z_n^q(k,g,u) + C_n(k,g)\]

From equation (3) and term (1) in equation (2) \[u^{n-1} - m = W_0^{n-1-0}(k,g,u)\]

From equation (3) and term (2) in equation (2) \[u^{n-2}(k-g) + mg = W_1^{n-2}(k,g,u)\]

Term (3) and equation (2) \[u^{n-3}(k-g)^2 - mg^2 = W_2^{n-3}(kgu)\]
4

Last term in equation (2)

\[(k - g)^{n-1} - mg^{n-1} = W^{n-1-n+1}_{n-1}(k, g, u)\]

Then we have that

\[
\frac{u^n + (k - g)^n}{u + k - g} - m \left(\frac{g^n - 1}{g - 1}\right) = \sum_{j=0}^{n-1} (-1)^j W^{n-1-j}_{j}(k, g, u)
\]

We note from equation (3)

\[W_n^q(k, g, u) = Z_n^q(k, g, u) + C_n(k, g)\]

Where

\[Z_n^q(k, g, u) = (u^q - m)(k - g)^n\]

And

\[C_n(k, g) = mk \sum_{j=1}^{n} (k - g)^{j-1}(-g)^{n-j}\]

From equation (3) and (4) we have

\[
\frac{u^n + (k - g)^n}{u + k - g} - m \left(\frac{g^n - 1}{g - 1}\right) = \sum_{j=0}^{n-1} (u^{n-1-j} - m)(k - g)^j + km \sum_{j=1}^{n-1} \sum_{r=1}^{j} (-1)^j(k - g)^{r-1}(-g)^{j-r}
\]

Let

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

And

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

And

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

Then we have
\[ L_n(k, g, u) = V_n^n(k, g, u) + S_n(k, g) \]

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 \( S_n(k, h) \)

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

Then we have

\[
s_n(k, g) = km \left( \sum_{r=3}^{1} (-1)^r(k - g)^{r-1} g^{1-r} + \sum_{r=1}^{2} (-1)^r(k - g)^{r-1} g^{2-r} + \sum_{r=1}^{n-1} (-1)^r(k - g)^{r-1} g^{n-r} \right)
\]

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

\[
S_n(k, h) = km \left( (-1) + (-g + (k - g)) + (-g^2 + g(k - g) - (k - g)^2) \right.
\]
\[
- (-g^3 + g^2(k - g) - g(k - g)^2 + (k - g)^3) \ldots \ldots \ldots (-g^{n-1} + g^{n-2}(k - g)
\]
\[
- g^{n-3}(k - g)^2 + g^{n-4}(k - g)^3 \ldots \ldots \ldots (k - g)^{n-2} \right)
\]

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

\[
s_n(k, h) = km(-1 + g + g^2 \ldots \ldots g^{n-2}) + (k - g)((1 + g + g^2 + g^3 \ldots \ldots g^{n-3}))
\]
\[
- (k - g)^2(1 + g + g^2 + g^3 \ldots \ldots g^{n-4}) \ldots \ldots (k - g)^{n-1})
\]

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

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

Then we have that

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

Then

\[
L_n(k, g, u) = \frac{u^n + (k - g)^n}{u + k - g} - m \left( \frac{g^{n-1} - 1}{g - 1} \right)
\]
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 2 let in $V^n_n(u,k,g)$, $u = 1$ and $m = 1$ then we find

$$V^n_n(k,h,1) = \sum_{j=1}^{n-1} (-1)^j ((1)^{n-j} - 1)(k-g)^j = 0$$

Then

$$L_n(u,k,1) = V^n_n(u,k,1) + S_n(k,g)$$

According to the equations, (2.7, 2.8, 2.9) we find that

$$\frac{1 + (k-g)^n}{1 + k - g} = \frac{g^n - 1}{g - 1}$$

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

**Proof.**

According to Euler’s theorem $\phi(n)$ Euler function then $a^\phi(n) \equiv 1 \pmod{n}$ see [K.M 244]

**Proof.**

**Theorem 2** from theorem 1 if $n$ is odd and $k$ $g$ real number we have

$$\frac{1 + (k-g)^n}{1 + k - g} = \frac{g^n - 1}{g - 1}$$

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

Let in theorem 1 $k = a^d + m$ and $g = a^d$ then $k - g = m$ so we have
Then

\[\frac{1 + m^n}{1 + m} - \frac{a^{dn} - 1}{a^d - 1} = -(a^d + m) \left(\frac{a^{d(n-1)} - 1}{a^{d-1}}\right) + (a^d + m) \sum_{j=1}^{n-2} (-1)^{j-1} m^j \left(\frac{a^{dn-d} - 1}{a^{d-1}} - (a^{dn-2d} + a^{dn-3d} \ldots a^{dn-jd-1d})\right)\]

Let \(V\) equal

\[V = (a^d + m) \sum_{j=1}^{n-2} (-1)^{j-1} m^j \left(\frac{a^{dn-d} - 1}{a^{d-1}} - (a^{dn-2d} + a^{dn-3d} \ldots a^{dn-jd-1d})\right)\]

From equation (10) and (11) we have that

\[\frac{1 + m^n}{1 + m} - \frac{a^{dn} - 1}{a^d - 1} = -(a^d + m) \left(\frac{a^{d(n-1)} - 1}{a^{d-1}}\right) + mV\]

Let \(\varphi(m) = d(n - 1)\) where \(\varphi(m)\) Euler function then we note in rigor side equation

\[\frac{1 + m^n}{1 + m} - \frac{a^{dn} - 1}{a^d - 1} = -(a^d + m) \left(\frac{a^{\varphi(m)} - 1}{a^d - 1}\right) + mV\]

According Euler theorem

\[a^{\varphi(m)} \equiv 1 (mod m)\]

From equation (13) and Euler theorem if \(a^d \not\equiv 1 (mod m)\) we have

\[\frac{m^n + 1}{m + 1} \equiv \frac{a^{dn} - 1}{a^d - 1} (mod m)\]

**Proof. Theorem 3** from equation (13) we have that

\[\frac{1 + m^n}{1 + m} - \frac{a^{dn} - 1}{a^d - 1} = -(a^d + m) \left(\frac{a^{\varphi(m)} - 1}{a^d - 1}\right) + mV\]

Let \(m = p\) where \(p\) prime number according Euler function \(\varphi(p) = p - 1 = d(n - 1)\) and \(n\) is odd then we have

\[\frac{1 + p^n}{1 + p} - \frac{a^{dn} - 1}{a^d - 1} = -(a^d + p) \left(\frac{a^{p-1} - 1}{a - 1}\right) + pV\]

Then If \(p - 1 = d(n - 1)\) we \(n\) is odd we have
\[
\frac{p^n + 1}{p + 1} \equiv \frac{a^{dn} - 1}{a^d - 1} \quad (\text{mod } p)
\]

**Proof. Theorem 4** according theorem 2 if \( \varphi(m) = d(n - 1) \) where \( n \) is odd we have

\[
\frac{m^n + 1}{m + 1} \equiv \frac{a^{dn} - 1}{a^d - 1} \quad (\text{mod } m)
\]

let in theorem 1 \( m = p^m \) and \( n = p \) then according Eulere function \( \varphi(p^m) = p^{m-1}(p - 1) \) so \( d = p^{m-1} \) and \( dn = p^m \) we have that

\[
\frac{p^{mp} + 1}{p^m + 1} \equiv \frac{a^{p^m} - 1}{a^{p^{m-1}} - 1} \left( \text{mod } p^m(a^{p^{m-1}} + p^m) \right)
\]

Student: Shazly Abdullah Fdl
Faculty of mathematics sciences & statistics
Aleenlain University Sudan
Email address: Shazlyabdullah3@gmail.com