On the Polynomials Congruent Modulo $P^a$

Ahmad Sabihi

Department of Mathematics
Sharif University of Technology, Tehran, Iran
sabihi2000@yahoo.com

Abstract. In this paper, the author presents a special polynomial function

$$f(x) = \prod_{r=1}^{\phi(p^a)} (x^n - r^n), r \in \{r_1, \ldots, r_{\phi(p^a)}\}, \phi \text{ is Euler's function.}$$

are integer numbers relatively prime to the $P^a$ and $n$ is odd integer, then he obtains

tits value congruent modulo $P^a$ where $P$ and $a$ denote an odd optional prime and

1. INTRODUCTION

Study on the polynomials modulo prime powers and their solution is the one of
the oldest researches in the mathematics world. Also, Diophantine equations and
classes of polynomials have been interested. K. Davis and W. Webb [1] obtained
a binomial coefficient congruent modulo prime powers, their work is only on the
binomial coefficients but the author obtains the coefficients of a general poly-
onomial that has integer roots of co-prime with respect to a given prime power.

Mathematics Subject Classification: Primary 11A07; Secondary 11A41, 11D79

Keywords: Prime Numbers, Congruences, Polynomials, Ring and ideal theories, Diophantine Congruences

Also, A. Granville [2], Z. W. Sun [3-5], Z. W. Sun and D. M. Davis [6], C. S. Weisman [7] have worked on the binomial coefficients and some other ones like
W. Fouché [8] on the Bernoulli coefficients as form $\beta_p(X) = \sum_{k=1}^{p-2} \frac{B_k}{k} (X^{p^{1-k}} - 1)$
where $B_k, k = 0, 1, \ldots$, are the Bernoulli numbers and $P$ an odd prime. The coefficients of this polynomial are $P$-integral. The present paper includes three sections 1- Introduction 2-The main subject 3-Corollary. At the section two, a special function is constructed by the multiplication of $\phi(p^n)$ Diophantine polynomials, then its value and coefficients congruent modulo $P^n$ are obtained. At the section three the author obtains some useful techniques of the ring and group theory at number theory to obtain divisibility by prime powers. These techniques are also applications of main subject at the section two.

\section{The Main Subject}

\textbf{Lemma 2.1} Assume there is the following polynomial function:

$$f(x) = \prod_{r=r_1}^{r_{\phi(p^n)}} (x^n - r^n)$$

so that $x \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]$. $P$ denotes an odd prime number, $a, n \in \mathbb{N}, a \geq 1, n$ is an odd integer and $r \in \{r_1, \ldots, r_{\phi(p^n)}\}, \phi$ is Euler’s function. $r_1, \ldots, r_{\phi(p^n)}$ are integer numbers relatively prime to the $P^n$. 

Prove that

$$f(x) = \left[ x^{n(\phi(p^n))} + (-1)^n \right]^p \left( \text{mod } P^n \right)$$

or

$$f(x) \equiv \begin{cases} 0 & \left( x, P^n \right) = 1 \text{ for odd values of } P \text{ & } n \\ (-1)^{n(\phi(p^n))} & \left( x, P^n \right) \not\equiv 1 \text{ for odd values of } P \text{ & } n \end{cases} \left( \text{mod } P^n \right)$$

\textbf{Proof:}

Before the proof the following Lemma should be proved:
Lemma 2.2: Assume $P$ be an odd prime and $a \geq 1$ an integer, and also assume \( r_1, \cdots, r_{\phi(P)} \) make a reduced residue system modulo $P^a$. Prove the following polynomial congruency is satisfied:

\[
(x^{P^{-1}} - 1)^{\phi(P)} \equiv (x - r_1)(x - r_2)\cdots(x - r_{\phi(P)})(\text{mod} \ P^a)
\]  

(2-3)

Proof: One theorem and one Lemma are used for the proof:

Theorem 2.3: Assume $f(x)$ be a polynomial of integer coefficients and $b_1, b_2, \cdots, b_t$ $t$ incongruent solutions of $f(x) \equiv 0 \pmod{P}$ then there is a polynomial as $q(x)$ of integer coefficients so: [9-10].

\[
f(x) \equiv (x - b_1)(x - b_2)\cdots(x - b_t)q(x) \pmod{P}
\]

(2-4)

and

\[\deg_P q(x) \leq \deg_P f(x) - t\]  

(2-5)

Lemma 2.4: Assume $P$ be a prime then could be written: the case $a = 1$ of the Lemma 2.2

\[x^{P^{-1}} - 1 \equiv (x - 1)(x - 2)\cdots(x - (P - 1)) \pmod{P}
\]

(2-6)

Proof: Based on the Fermat's theorem if $\gcd(x, P) = 1$ then the relation (2-7) will be concluded:

\[x^{P^{-1}} \equiv 1 \pmod{P}
\]

(2-7)

Also the relation (2-8) can be concluded from the relation (2-7)

\[x^P - x \equiv 0 \pmod{P}
\]

(2-8)

All the integers are all the solutions of the equation (2-8). Therefore one can apply the theorem 2.3 to the relation (2-8) and conclude the relation (2-9)

\[x^P - x \equiv x(x - 1)(x - 2)\cdots(x - (P - 1))q(x) \pmod{P}
\]

(2-9)

where $0, 1, 2, \cdots, (P - 1)$ are the solutions of the relation (2-9) and $1, 2, \cdots, (P - 1)$ are incongruent solutions of the relation (2-8) modulo $P$ and

\[\deg_P q(x) \leq P - P = 0
\]

(2-10)
Therefore \( q(x) \) is a constant polynomial as \( q(x) = b \) where \( b \) is an integer, but the coefficient of \( x^p \) is number 1 and at the right-hand of the relation (2-9) is \( b \) thus:

\[
b \equiv 1 \pmod{P}
\]  

(2-11)

Because \( \gcd(x, P) = 1 \) based on the elementary number theories [9-10] the relation (2-6) will be obtained.

Using the Lemma 2.4 for the all integers between 1 and \( P^a \), one could write as below:

\[
1, 2, \ldots, (P - 1), P, (P + 1), \ldots, (2P - 1), 2P,
\]

\[
(2P + 1), \ldots, (3P - 1), 3P, \ldots, P^{a-1}, P^{a-1} + 1, \ldots, P^a - 1, P^a
\]  

(2-12)

Therefore all the integers which are relatively co-prime with respect to \( P \) or \( P^a \) are:

\[
1, 2, \ldots, (P - 1), (P + 1), \ldots, (2P - 1),
\]

\[
(2P + 1), \ldots, (3P - 1), \ldots, P^{a-1} + 1, \ldots, P^a - 1
\]  

(2-13)

On the other word the following congruences are satisfied:

\[
1 \equiv (P + 1) \equiv (2P + 1) \equiv \cdots \equiv P^{a-1} + 1 \pmod{P}
\]

\[
2 \equiv (P + 2) \equiv (2P + 2) \equiv \cdots \equiv P^{a-1} + 2 \pmod{P}
\]

\[
\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots
\]

\[
P - 1 \equiv (2P - 1) \equiv \cdots \equiv P^a - 1 \pmod{P}
\]  

(2-14)

The number of positive integers (reduced residue system) modulo \( P^a \) is \( \phi(P^a) \) that its value is \( (P - 1)P^{(a-1)} \) thus referring to the relations (2-12) and (2-13), there are \( P^{(a-1)} \) sub-reduced residue systems of length \( (P - 1) \) between 1 and \( P^a \).

Using the above explanations and the relation (2-6) could be written:

\[
P^{a-1} \text{ times} \left\{
\begin{aligned}
(x^{P-1} - 1) &\equiv (x - 1) \cdots (x - (P - 1)) \pmod{P} \\
(x^{P-1} - 1) &\equiv (x - (P + 1)) \cdots (x - (2P - 1)) \pmod{P} \\
\vdots &\vdots \\
(x^{P-1} - 1) &\equiv (x - (P^{a-1} + 1)) \cdots (x - (P^a - 1)) \pmod{P}
\end{aligned}
\right.
\]  

(2-15)

If one multiplies the right and left-hand sides of the relation (2-15) together then the following relation will be obtained:
On the polynomials congruent modulo \( P^a \)

\[(x^{p-1} - 1)^{p^{(e-1)}} \equiv (x - 1) \cdots (x - (P - 1))(x - (P + 1)) \cdots (x - (2P - 1)) \cdots (x - (P^a + 1)) \cdots (x - (P^a - 1)) \pmod{P^a} \]  

(2-16)

**Theorem 2.5:** Assume \( f(x) \) be a polynomial where is of integer coefficients and \( a \) is an integer and \( n \) a natural number then \( f(a) \equiv 0 \pmod{n} \) if and only if there is a polynomial \( q(x) \) of integer coefficient so: [9-10].

\[ f(x) \equiv (x - a)q(x) \pmod{n} \]  

(2-17)

**Theorem 2.6:** Assume \( f(x) \equiv g(x) \pmod{n} \) then the solutions of \( f(x) \equiv 0 \pmod{n} \) are precisely the solutions of \( g(x) \equiv 0 \pmod{n} \). [9-10].

If the first relation of the relations (2-15) is considered, then will be obtained:

\[(x^{p-1} - 1) - (x - 1) \cdots (x - (P - 1)) = kp \]  

(2-18)

Therefore could be written:

\[ \left[ (x^{p-1} - 1) - (x - 1) \cdots (x - (P - 1)) \right]^{p^{(e-1)}} = [kp]^{p^{(e-1)}} \]  

(2-19)

The left-hand side of the above relation is extended:

\[
\begin{align*}
(x^{p-1} - 1)^{p^{(e-1)}} &= P^{(a-1)}(x^{p-1} - 1)^{p^{(a-1)-1}}(x - 1) \cdots (x - (P - 1)) + \\
&\quad \frac{P^{(a-1)}(P^{(a-1)} - 1)}{2!} (x^{p-1} - 1)^{p^{(a-1)+2}} [(x - 1) \cdots (x - (P - 1))]^2 \\
&\quad \cdots (-1)^i \frac{P^{(a-1)}(P^{(a-1)} - 1)(P^{(a-1)} - 2) \cdots (P^{(a-1)} - (i - 1))}{i!} \\
&\quad \cdots (-1)^{p^{(a-1)-i}} [(x - 1) \cdots (x - (P - 1))]^{p^{(e-1)}} \\
&\quad \cdots (-1)^{P^{(a-1)}} [(x - 1) \cdots (x - (P - 1))]^{p^{(e-1)}} = [kp]^{p^{(e-1)}}
\end{align*}
\]

(2-20)

Obviously, the right-hand side of the relation (2-20) is divided by \( P^a \) therefore the left-hand side should also be divided by \( P^a \). Consider from the second term to the before the last term for investigation of divisibility of them by \( P^a \).

The term \( (x^{p-1} - 1) \) is divisible by \( P \) based on the relation (2-7) and the right-hand side of the relation (2-6) is also divisible by \( P \) based on the theorem 2.6 thus the sum of the powers of these terms in each term of the relation (2-20) is:

\[ P^{p^{(a-1)}} \]  

(2-21)

Also, the at most power of \( P \) at the denominator of the fractional terms \( (i! \) is:
Therefore if the at most power is taken place at the one of the denominators and divides the related numerator then the following result will be obtained:

\[
P^{(a-1)}P^{(a-1)}_{P^{(a-1)}} = P^\left[p^{(a-1)} - p^{(a-1)+a-1}\right] \geq P^a
\]  

(2-23)

Because \( P^{(a-1)} - P^{(a-1)} + a - 1 \geq a \) for \( a > 1 \)

Hence all the terms from the second term to the before the last term are divisible by \( P^a \). The first and last terms are remaining as below:

\[
(x^{P-1} - 1)^{p^{(a-1)}} + (-1)^{p^{(a-1)}} [(x - 1)\cdots(x - (P - 1))]^{p^{(a-1)}} \equiv 0 \pmod{P^a}
\]  

(2-24)

If \( P \) is odd prime then \((-1)^{p^{(a-1)}} = -1\) and (2-24) will be:

\[
(x^{P-1} - 1)^{p^{(a-1)}} \equiv [(x - 1)\cdots(x - (P - 1))]^{p^{(a-1)}} \pmod{P^a}
\]  

(2-25)

Based on the relations (2-13) and (2-14) should be written:

\[
[(x - 1)\cdots(x - (P - 1))]^{p^{(a-1)}} \equiv (x - 1)\cdots(x - (P - 1))(x - (P + 1))\cdots(x - (2P - 1))\cdots(x - (P^{a-1} + 1))\cdots(x - (P^a - 1)) \pmod{P^a}
\]  

(2-26)

Therefore for \( a > 1 \) the relation (2-27) is satisfied.

\[
(x^{P-1} - 1)^{p^{(a-1)}} \equiv (x - 1)\cdots(x - (P - 1))(x - (P + 1))\cdots(x - (2P - 1))\cdots(x - (P^{a-1} + 1))\cdots(x - (P^a - 1)) \pmod{P^a}
\]  

(2-27)

Thus the Lemma 2.2 is proved.

Just, replacing \( x \) by \( x^n \) into the relation (2-27) or (2-3), then should be obtained:

\[
(x^n)^{P-1} \equiv (x^n - 1)\cdots(x^n - (P - 1))(x^n - (P + 1))\cdots(x^n - (2P - 1))\cdots(x^n - (P^{a-1} + 1))\cdots(x^n - (P^a - 1)) \pmod{P^a}
\]  

(2-28)

If we have the odd \( n \)-th power of all the incongruence solutions then shall be written:
On the polynomials congruent modulo \( P^a \)

\[
\left[ x^{n(P-1)} + (-1)^n \right]^{\varphi(P^a)} \equiv (x^n - 1^n) \cdots (x^n - (P^a - 1^n)) (mod\ P^a)
\]

The number \( n \) must be certainly an odd number because the relation (2-28) is true for all variables \( x \) and \( n \), therefore after extending right and left-hand terms, obviously \( n \) must be an odd integer. For example: substituting \( P = 3, a = 1 \) or \( P = 3, a = 2 \) or \( P = 5, a = 1 \) into the relation (2-29) will confirm to be true the relation (2-29) for the odd integers.

Therefore if \( (x, P^a) = 1 \) then the left or right-hand side of the relation (2-29) will be zero and if \( (x, P^a) \neq 1 \) then it will be \( (-1)^{\varphi(P^a)} \) because extending left-hand side of the relation (2-29), is easily seen that left-hand side is congruent \( (-1)^{\varphi(P^a)} \) modulo \( P^a \). For establishing the relation (2-29) both integers \( P \) and \( n \) must be odd numbers.

The coefficients of the extending terms of \( f(x) \) at the relation (2-1) are available based on the relation (2-29). If the right-hand terms of (2-1) and (2-2) based on the relation (2-30) are extended simultaneously, then the coefficients of the extension will be obtained:

At the relations (2-31) to (2-39) the inequality (2-30) must be considered.

\[
k^n(P - 1) \leq \varphi(P^a) \tag{2-30}
\]

\[
\left[ x^{n(P-1)} + (-1)^n \right]^{\varphi(P^a)} \equiv \prod_{r=r_1}^{\varphi(P^a)} (x^n - r^n) \pmod{P^a} \tag{2-31}
\]

\[
\sum_{i=1}^{\varphi(P^a)} (r_i)^n \equiv 0 \pmod{P^a} \tag{2-32}
\]

\[
\sum_{i=1}^{2} \prod_{j=1}^{2} (r_j)^n \equiv 0 \pmod{P^a} \tag{2-33}
\]

\[
\vdots \vdots \\
\vdots \vdots \\
\sum_{i=1}^{[n(P-1)]} \prod_{j=1}^{[n(P-1)]} (r_j)^n \equiv \frac{(-1)^n P^{(a-1)}}{1!} \pmod{P^a} \tag{2-34}
\]
\[ \sum \prod_{i=1}^{[n(P-1)]} (r_i)^n \equiv 0 \pmod{P^a} \quad (2-35) \]

\[ \sum \prod_{i=1}^{[2n(P-1)]} (r_i)^n \equiv \frac{(-1)^{2n} P^{(a-1)}(P^{(a-1)}-1)}{2!} \pmod{P^a} \quad (2-36) \]

\[ \sum \prod_{i=1}^{[2n(P-1)]} (r_i)^n \equiv 0 \pmod{P^a} \quad (2-37) \]

\[ \sum \prod_{i=1}^{[kP(P-1)]} (r_i)^n \equiv \frac{(-1)^{kn} P^{(a-1)}(P^{(a-1)}-1)\cdots(P^{(a-1)}-(k-1))}{k!} \pmod{P^a} \quad (2-38) \]

\[ \prod_{i=1}^{i=\phi(P^a)} (r_i)^n \equiv (-1)^{a^{(a-1)}} \pmod{P^a} \quad (2-39) \]

\( k \) is the number of terms at the extension of the right-hand side of (2-31) subtract from the number one i.e. assume \( j \) denotes the number of terms starting to count from the term of the greatest power \( x \) then \( k = j - 1 \).

### 3. COROLLARY

One of the conclusions of the Section 2 is the following Lemma:

**Lemma 3.1:** Prove that if \( P > 3 \) is prime and \( a \) and \( b \) are integers and

\[ 1 + \frac{1}{2} + \cdots + \frac{1}{(P-1)} = \frac{a}{b} \quad (3-1) \]

Then could be proved that

\[ P \mid a \quad \text{and} \quad P^2 \mid a \quad (3-2) \]
On the polynomials congruent modulo $P^a$

**Proof:**

The first method of the proof

Assume

$$f(x) = (x - 1)(x - 2)\cdots(x - (P - 1))$$  \hspace{1cm} (3-3)

Then $f(x)$ will be extended as below:

$$f(x) = x^{(P-1)} - \left( \sum_{i=1}^{(P-1)} r_i \right) x^{(P-2)} + \cdots - \left( \sum_{j=1}^{\left(\frac{P-1}{P-2}\right)} \prod_{i=1}^{(P-2)} r_i \right) x + (P - 1)!$$ \hspace{1cm} (3-4)

$\left(\frac{P-1}{P-2}\right)$ denotes the permutation of $P - 2$ from $P - 1$.

If one substitute $x = P$ into the relations (3-3) and (3-4) then equalizing them will be obtained:

$$f(P) = P^{(P-1)} - \left( \sum_{i=1}^{(P-1)} r_i \right) P^{(P-2)} + \cdots - \left( \sum_{j=1}^{\left(\frac{P-1}{P-2}\right)} \prod_{i=1}^{(P-2)} r_i \right) P + (P - 1)! = (P - 1)!$$ \hspace{1cm} (3-5)

$$\Rightarrow P^{(P-1)} - \left( \sum_{i=1}^{(P-1)} r_i \right) P^{(P-2)} + \cdots + \left( \sum_{j=1}^{\left(\frac{P-1}{P-3}\right)} \prod_{i=1}^{(P-3)} r_i \right) P^2 = \left( \sum_{j=1}^{\left(\frac{P-1}{P-2}\right)} \prod_{i=1}^{(P-2)} r_i \right) P$$

Therefore, dividing right and left sides of the relation (3-5) by $P$, the relation (3-6) that is before the last term of (3-5) will be obtained.

$$\left( \sum_{j=1}^{\left(\frac{P-1}{P-2}\right)} \prod_{i=1}^{(P-2)} r_i \right)$$ \hspace{1cm} (3-6)

Hence

$$P^{(P-2)} - \left( \sum_{i=1}^{(P-1)} r_i \right) P^{(P-3)} + \cdots + \left( \sum_{j=1}^{\left(\frac{P-1}{P-3}\right)} \prod_{i=1}^{(P-3)} r_i \right) P = \left( \sum_{j=1}^{\left(\frac{P-1}{P-2}\right)} \prod_{i=1}^{(P-2)} r_i \right)$$ \hspace{1cm} (3-7)

This means that based on the relation (3-7) the relation (3-6) is divisible by $P$.

Just if at the left-hand side of the relation (3-1) is taken the common multiple will be obtained:
It is seen that the relation (3-6) is the numerator of the relation (3-8) i.e. integer $a$ at the relation (3-1). Therefore was proved that $P | a$.

Just should be proved that the term

$$\frac{\sum_{j=1}^{p-1} \prod_{i=1}^{p-2} r_j}{(p-1)!}$$

of the relation (3-7) is also divided by $P$. Therefore the right-hand side of the relation (3-7) should be divided by $P^2$.

Based on the Lemma 2.4 and the relation (3-6), $f(x)$ (from the relation (3-3)) could be written:

$$f(x) = (x-1)(x-2)\cdots(x-(P-1)) \equiv x^{(p-1)} - 1 \pmod{P}$$

$$\Rightarrow x^{(p-1)} - 1 \equiv x^{(p-1)} - (\sum_{j=1}^{p-1} r_j)x^{(p-2)} + \cdots + \left(\sum_{j=1}^{p-1} \prod_{i=1}^{p-2} r_j\right)x \pmod{P}$$

$$-(\sum_{j=1}^{p-1} \prod_{i=1}^{p-2} r_j)x + (P-1)! \pmod{P}$$

If we compare the coefficients of left and right-hand extensions of the relation (3-10) then we will see the following relations:

$$\sum_{i=1}^{p-1} r_i \equiv 0 \pmod{P}$$

$$\vdots$$

$$\sum_{j=1}^{p-1} \prod_{i=1}^{p-3} r_i \equiv 0 \pmod{P}$$

$$\sum_{j=1}^{p-1} (\prod_{i=1}^{p-2} r_i) \equiv 0 \pmod{P}$$

$$(P-1)! - 1 \equiv -1 \pmod{P}$$

Regarding the relation (3-12) and the relation (3-7) is concluded that;
On the polynomials congruent modulo $P^a$  

$$\left(\sum_{j=1}^{[P-1][P-2]} \prod_{i=1}^{r_j}\right) \equiv 0 \pmod{P^2} \quad (3-15)$$

This means that $P^2 | a$ and the proof is completed.

The second method of the proof

It has been known that numbers $0$ to $(P-1)$ construct an algebraic field with respect to addition and multiplication operations. Assume $Z_p = \{[0],[1],\ldots,[P-1]\}$ be an equivalence class field and $[0],[1],\ldots,[P-1]$ be partitions of sets congruent modulo $P$. $Z_p$ is a field because if $[x],[y] \in Z_p$ then $[x]+[y]=[z] \in Z_p$ and $[x][y]=[z] \in Z_p$ therefore for every member as $[x]$ there is a reverse member of addition operation as $-[x]$ and a reverse member of multiplication operation as $[x]^{p^{-2}}$ because

$$[x][x]^{p^{-2}} \equiv 1 \pmod{P} \quad (3-16)$$

Because $[0],[1],\ldots,[P-1]$ construct an abelian group with respect to addition operation then based on the following theorem that is a cyclic group.

Theorem 3.2 Lagrange’s Theorem: every group of a prime order is a cyclic group.

There is $\phi(P)$ elements of $P$ order. Hence in here, there is $P-1$ elements of $P$ order and each non-zero member of $Z_p$ can be represented as a power of the other member.

$$[x]=[y]^i \quad i \in \{1,\ldots,(P-1)\} \quad (3-17)$$

Assume the fraction numerator at the relation (3-1) can be written as the following:

$$y_1 = y_2 = \cdots = y_{(P-1)} = y = (P-1)! + \frac{(P-1)!}{2} + \cdots + (P-2)! \quad (3-18)$$

Based on the theorem 3.2, because $Z_p$ is an abelian group with respect to addition operation therefore each non-zero member could be written as a multiple of two other members.

$$x,n,a \in Z_p' = \{Z_p - \{[0]\}\} = \{[1],\ldots,[P-1]\} \Rightarrow x = na \quad (3-19)$$
Generally,
\[ x_i, n_i, a_i, i \in Z_p' = \left\{ Z_p - \{0\} \right\} = \{[1], \ldots, [P-1]\} \Rightarrow x_i = n_i a_i \quad (3-20) \]

Therefore we could define an ideal set onto ring \( Z_p \) to be equal to set \( Z_p' \), then each right hand term of the relation (3-18) is able to be replaced by an equivalence member of \( Z_p' \).

Therefore based on the relations (3-19) and (3-20) could be written:
\[
\begin{align*}
(P - 1)! &= 1 \times 2 \times \cdots \times (P - 1) = 1 \times 2a_1 \times \cdots \times (P - 1)a_1 = \frac{(P - 1)!}{n_1} a_1^{(p-2)} \\
\frac{(P - 1)!}{2} &= 1 \times 3 \times 4 \times \cdots \times (P - 1) = 1 \times 3a_1 \times 4a_1 \times \cdots \times (P - 1)a_1 = \frac{(P - 1)!}{n_2} a_1^{(p-2)} \\
&\vdots \\
(P - 2)! &= \frac{(P - 1)!}{n_{(p-1)}} a_1^{(p-2)}
\end{align*}
\]

Then
\[
y_1 = (P - 1)! + \cdots + (P - 2)! = a_1^{(p-2)} \left[ \frac{(P - 1)!}{n_1} + \cdots + \frac{(P - 1)!}{n_{(p-1)}} \right] \quad (3-22)
\]

For all the other members \( a_2 \) through \( a_{(p-1)} \) could be written like the relation (3-22).

Therefore
\[
y_1 = a_1^{(p-2)} \left[ \frac{(P - 1)!}{n_1} + \cdots + \frac{(P - 1)!}{n_{(p-1)}} \right], i = 2, \ldots, (P - 1) \quad (3-23)
\]

Hence a mean value of the variables \( y_1, y_2, \cdots, y_{(p-1)} \) could be written for \( y \) at the relation (3-18).

\[
y = \frac{y_1 + \cdots + y_{(p-1)}}{(P - 1)} = \left[ \frac{a_1^{(p-2)} + \cdots + a_{(p-1)}^{(p-2)}}{(P - 1)} \right] \left[ \frac{(P - 1)!}{n_1} + \cdots + \frac{(P - 1)!}{n_{(p-1)}} \right] \quad (3-24)
\]

\[
K = \left[ \frac{(P - 1)!}{n_1} + \cdots + \frac{(P - 1)!}{n_{(p-1)}} \right] \equiv -1 + 2^{-1} (P - 1) + \cdots + (P - 2)^{-1} (P - 1) + 1 \pmod{P} \quad (3-25)
\]

In obtaining the relation (3-25) the following relations are used:
\[
(P - 1)! \equiv -1 \pmod{P} \\
(P - 2)! \equiv 1 \pmod{P} \quad (3-26)
\]
All the members of $Z_p'$ except 1 and $(P - 1)$ have the distinctive reverse members because the reverse members of 1 and $(P - 1)$ are themselves.

Therefore

$$K \equiv -1 + (P - 1)\left[2^{-1} + \cdots + (P - 2)^{-1}\right] + 1 \equiv (P - 1)\left[2^{-1} + \cdots + (P - 2)^{-1}\right] \pmod{P} \quad (3-27)$$

On the other side because the members $2^{-1}, \cdots, (P - 2)^{-1}$ are among the members $2, \cdots, (P - 2)$ hence could be written:

$$(P - 1)\left[2^{-1} + \cdots + (P - 2)^{-1}\right] = (P - 1)\left[2 + \cdots + (P - 2)\right] \quad (3-28)$$

or

$$K \equiv (P - 1)\left[2 + \cdots + (P - 2)\right] = \frac{P(P - 1)(P - 3)}{2} \equiv 0 \pmod{P} \quad (3-29)$$

Assume

$$Z = a_1^{(p-2)} + \cdots + a_{(p-1)}^{(p-2)} \quad (3-30)$$

Because $a_1^{(p-2)}, \cdots, a_{(p-1)}^{(p-2)} \in Z_p'$ therefore

$$Z = \frac{P(P - 1)}{2} \quad (3-31)$$

Then the numerator of the relation (3-1) i.e. $y$ is obtained as:

$$y = \frac{KZ}{(P - 1)} = \frac{P^2(P - 1)(P - 3)}{4} \quad (3-32)$$

And this means that $P^2 \mid y$

REFERENCES


Received: July 3, 2008