On Sum of Powers of Numbers Having a Given Order Modulo a Power of a Prime

Yuguang Fang
Department of Electrical and Computer Engineering
University of Florida
435 Engineering Building, P.O.Box 116130
Gainesville, Florida 32611-6130
Tel: (352) 846-3043, Fax: (352) 392-0044
Email: fang@ece.ufl.edu

Proposed running title: On Sum of Powers of Numbers Having a Given Order
Abstract

Let $S_r(p^\alpha, d)$ denote the sum of $r$th powers of numbers having given order (or exponent) $d$ modulo $p^\alpha$ where $p$ is an odd prime, $r$, $d$ and $\alpha$ are positive integers and $d | \phi(p^\alpha)$ with $\phi(\cdot)$ indicating the Euler function. In this paper, we study the congruence property of this summation and obtain the following result

$$S_r(p^\alpha, d) \equiv \frac{\phi(d)}{\phi(l_0)} \mu(l_0), \quad \frac{d}{(r, d)} = p^m l_0, \quad (p, l_0) = 1, r > 0, \alpha > 0.$$

Keywords: Sum of Numbers, Residue, Congruence, Primitive roots.

AMS Subject Classification: 11A07, 11A25.

1 Introduction

Let $S_r(p^\alpha, d)$ denote the sum of $r$th powers of numbers having given order (or exponent) $d$ modulo $p^\alpha$ where $p$ is an odd prime, $r$, $d$ and $\alpha$ are positive integers and $d | \phi(p^\alpha)$ with $\phi(\cdot)$ indicating the Euler function. Gauss proved in his masterpiece ([4]) that $S_1(p, p - 1) \equiv \mu(p - 1) \pmod{p}$ where $\mu(\cdot)$ is the Möbius function. In 1830, Stern ([6]) generalized this result and obtained that $S_1(p, d) \equiv \mu(d) \pmod{p}$ for any $d | (p - 1)$. In 1883, Forsyth ([3]) studied the congruence of $S_r(p, p - 1)$ for any positive integer $r$, however, his results and proofs were very complicated. In 1952, Moller ([2]) investigated more general cases and obtained

$$S_r(p, d) \equiv \frac{\phi(d)}{\phi(d_1)} \mu(d_1) \pmod{p}, \quad d_1 = \frac{d}{(r, d)}.$$

However, Moller’s proof was still complicated. Gupta ([5]) gave a simpler proof using the concept of primitive root.

In this paper, we generalize Moller’s results to the case when the modulo is a power of a prime.

2 Main Results

The following are our main results.

**Theorem 1.** Let $\alpha$, $d$ and $r$ be positive integers, let $p$ be a prime number, $l_0$ is the number satisfying $d / (r, d) = p^m l_0$ and $(p, l_0) = 1$, then we have

$$S_r(p^\alpha, d) \equiv \frac{\phi(d)}{\phi(l_0)} \mu(l_0) \pmod{p^\alpha} \tag{1}$$

Let $h(d) = d / (r, d)$, let $p(d) = \text{pot}_p(h(d))$ denote the highest power of $p$ in $h(d)$, where $\text{pot}_p(n)$
denotes the highest power of factor \( p \) in \( n \). For \( x|\phi(p^\alpha) \), define

\[
F(x, r) = \sum_{d|x} \frac{\phi(d)}{\phi(h(d)p^{-\eta_1})} \mu(h(d)p^{-\eta_1})
\]

(2)

We have

**Theorem 2.**

\[
F(x, r) = \begin{cases} 
  x, & \text{if } p^{-\eta_1}x | r; \\
  0, & \text{otherwise.}
\end{cases}
\]

To prove our main results, we need the following lemmas.

**Lemma 1.** There exists a primitive root \( g \) modulo \( p^\alpha \) such that

\[
g^{p^l(p-1)} \equiv 1 + \eta_1 p^{l+1} \pmod{p^{l+2}}
\]

for any \( l \geq 0 \) and \( (p, \eta) = 1 \).

**Proof:** Suppose \( g \) is a primitive root modulo \( p \), without loss of generality, we assume \( g^{p-1} = 1 + \eta_1 p \pmod{p^2} \) where \( (\eta_1, p) = 1 \). It is well-known ([5]) that \( g \) is also a primitive root modulo \( p^\alpha \). When \( l = 0 \), from the choice of \( g \), we know Lemma 1 is true. Suppose that Lemma 1 is true for \( l - 1 \), that is, we have

\[
g^{p^{l-1}(p-1)} = 1 + \eta_2 p^l, \ (\eta_2, p) = 1,
\]

then

\[
g^{p^l(p-1)} = (1 + \eta_2 p^l)^p = 1 + \eta_2 p^{l+1} + \left(\frac{p}{2}\right)(\eta_2 p^l)^2 + \cdots
\]

\[
\equiv 1 + \eta_2 p^{l+1} \pmod{p^{l+2}}
\]

By induction, we conclude that Lemma 1 is true.

**Lemma 2 ([5])** Let \( f(n) \) denote an arithmetical function, then

\[
S'(n) = \sum_{j < n} f(j) = \sum_{d|n} \mu(d) \{ f(d) + f(2d) + \cdots + f(n) \}
\]

where \( j < n \) represents \( j < n \) and \( (j, n) = 1 \).

**Lemma 3 ([5])**

\[
\text{pot}_p \left( \binom{p^c}{r} \right) = c - \text{pot}_p(r), \quad 0 \leq r \leq p^c, \ c > 0.
\]

**Lemma 4 ([1])** Given integers \( r, d \) and \( k \) such that \( d|k, \ d > 0, \ k \geq 1 \) and \( (r, d) = 1 \), then the number of elements in the set \( S = \{r + td : \ t = 1, 2, \ldots, k/d\} \) which are relatively prime to \( k \) is \( \phi(k)/\phi(d) \).
Now we are ready to prove our main results.

**Proof of Theorem 1:** Let \( g \) be the primitive root as in Lemma 1, set \( t = g^{\phi(p^\alpha)} / d \), then we have

\[
t^r \equiv g^{\phi(p^\alpha) r_1 / d_1} \pmod{p^\alpha} \equiv a \pmod{p^\alpha}, \quad r_1 = \frac{r}{(r, d)}, \quad d_1 = \frac{d}{(r, d)}, \quad a = g^{\phi(p^\alpha) r_1 / d_1},
\]

thus \( t^r \) and \( a \) have the same order \( d_1 \). Set

\[
\mathcal{T} = \{ t^{\lambda r} : \lambda < r \}, \quad \mathcal{K} = \{ t^{\lambda r} : j < r \}.
\]

It is observed that every element in \( \mathcal{K} \) will reappear many times in \( \mathcal{T} \) modulo \( p^\alpha \). Let \( t^{\lambda r} \) be any element in \( \mathcal{K} \), which has the order \( d_1 \), then the number of elements in the set

\[
\{ t^{\lambda r} : t^{\lambda r} \equiv t^{\lambda j} \pmod{p^\alpha}, \lambda < r \}
\]

is equal to the number of elements in the set

\[
\{ \lambda : \lambda \equiv j \pmod{d_1}, \lambda < r \}
\]

which is equal to \( \phi(d) / \phi(d_1) \) via Lemma 4. Thus, every element in \( \mathcal{K} \) will reappear exactly \( \phi(d) / \phi(d_1) \) times in \( \mathcal{T} \) modulo \( p^\alpha \).

Let \( \mathcal{K}_a = \{ a^k : k < r \} \), then we have (in what follows we will use \( \equiv \) to denote the congruence with respect to modulo \( p^\alpha \) for brevity)

\[
S_r(p^\alpha, d) \equiv \sum_{b \in \mathcal{T}} b \equiv \frac{\phi(d)}{\phi(d_1)} \sum_{b \in \mathcal{K}} b \equiv \frac{\phi(d)}{\phi(d_1)} \sum_{b \in \mathcal{K}_a} b
\]

(3)

From Lemma 2, we have

\[
\sum_{b \in \mathcal{K}_a} b = \sum_{h | d_1} \mu(h) \{ a^h + a^{2^h} + \cdots + a^{d_1} \} = \sum_{h | d_1} \mu(h) \frac{a^{d_1} - 1}{a^h - 1} a^h
\]

(4)

Let \( d_1 = p^{r_0 l_0}, l_0 | (p - 1) \). Define

\[
l(r) = \begin{cases} 0, & \text{if } r = 0; \\ 1, & \text{if } r > 0. \end{cases}
\]

Then, we obtain

\[
\sum_{b \in \mathcal{K}_a} b = \sum_{h | d_1} \mu(h) \frac{a^{d_1} - 1}{a^h - 1} a^h = \sum_{0 \leq k \leq r_0 l_0} \mu(p^k l) \frac{a^{d_1} - 1}{a^{p^k l} - 1} a^{p^k l} \\
= \sum_{l | l_0} \mu(l) \frac{a^{d_1} - 1}{a^l - 1} a^l + l(r_0) \sum_{l | l_0} \mu(l) \frac{a^{d_1} - 1}{a^{p^k l} - 1} a^{p^k l} \\
= \sum_{l | l_0} \mu(l) \frac{a^{d_1} - 1}{a^l - 1} a^l - l(r_0) \sum_{l | l_0} \mu(l) \frac{a^{d_1} - 1}{a^{p^k l} - 1} a^{p^k l}
\]

(5)
For $l > 0$, if $(a^l - 1, p^\alpha) \neq 1$, then we have $a^l \equiv 1 \pmod{p}$, i.e., $g^{\phi(p^\alpha)l_{r_1}^{\alpha}/d_1} \equiv 1 \pmod{p}$. Since $g$ is a primitive root modulo $p$, then we have $(p - 1)\phi(p^\alpha)l_{r_1}^{\alpha}/d_1$, i.e., $(p - 1)|p^{\alpha-1-r_0}l_{r_1}(p - 1)/l_{r_0}$. However, since $l_{r_0}d_{r_1} = 1$ and $(l_{r_0}, p) = 1$, we have $l_{r_0}|l$. Therefore, for $0 < l < l_{r_0}$, we must have $(a^l - 1, p^\alpha) = 1$, hence

$$a^{d_1} - 1 \equiv 0 \pmod{p^\alpha}.$$ 

Similarly, we can obtain

$$a^{d_1} - 1 \equiv 0 \pmod{p^\alpha}, \quad 0 < l < l_{r_0}.$$ 

Taking these two equations into Eq. (5), we obtain

$$\sum_{b \in \mathbb{K}_a} b \equiv \mu(l_{r_0})a^{d_1} - 1 \equiv l(r_0)\mu(l_{r_0})a^{d_1} - 1 \equiv \phi(p^{\alpha}) \pmod{p^\alpha} \quad (6)$$

Applying Lemma 3, we can obtain the following

$$\text{pot}_p \left( \left( \frac{p^r}{k} \right)^{p^{\beta}} \right) \geq \alpha + \beta, \quad \text{if} \quad \beta \geq \alpha - r, \quad 1 \leq r < \alpha, \quad 2 \leq k \leq p^r \quad (7)$$

In fact, we only need to prove

$$\text{pot}_p \left( \left( \frac{p^r}{k} \right)^{p^{\beta}} \right) = \text{pot}_p \left( \left( \frac{p^r}{k} \right)^{p^{\beta}} \right) + \text{pot}_p(p^{\beta}) = r - \text{pot}_p(k) + k\beta \geq \alpha + \beta,$$

or $r - \text{pot}_p(k) + (k-1)\beta \geq \alpha$. Because $\beta \geq \alpha - r$, we then only need to prove $r - \text{pot}_p(k) + (k-1)(\alpha - r) \geq 0$ which is obvious by noticing that $\text{pot}_p(k) \leq r$. Thus, we obtain the proof of Eq. (7).

From Lemma 1, there exists a $\eta > 0$ with $(\eta, \alpha) = 1$ such that

$$a^{l_0} = \left( g^{\phi(p^\alpha)r_1/d_1} \right)^{l_0} = \left( g^{p^{\alpha-1}(p-1)} \right)^{r_1} = 1 + \eta p^\beta$$

where $\beta \geq \alpha - r_0$. Thus, we have

$$\frac{a^{d_1} - 1}{a^{l_0} - 1} = \frac{\frac{a^{d_1} - 1}{a^{l_0} - 1}}{\frac{a^{d_1} - 1}{a^{l_0} - 1}} = \frac{(1 + \eta p^\beta)p^{\alpha} - 1}{\eta p^\beta} \equiv p^{\alpha} \pmod{p^\alpha}$$

and

$$\frac{a^{d_1} - 1}{a^{l_0} - 1}a^{l_0} \equiv p^{\alpha} \pmod{p^\alpha} \quad (8)$$

Similarly, we can obtain

$$\frac{a^{d_1} - 1}{a^{l_0} - 1}a^{l_0} \equiv p^{\alpha-1} \pmod{p^\alpha}, \quad r_0 > 0 \quad (9)$$

Taking Eq. (8) and Eq. (9) into Eq. (6), we obtain

$$\sum_{b \in \mathbb{K}_a} b \equiv \mu(l_{r_0})p^{\alpha} - l(r_0)\mu(l_{r_0})p^{\alpha-1} \pmod{p^\alpha}$$

$$\equiv \mu(l_{r_0})p^{\alpha} - l(r_0)p^{\alpha-1} \equiv \mu(l_{r_0})\phi(p^{\alpha}) \pmod{p^\alpha}$$
Taking this into Eq. (3) we finally obtain

$$S_r(p^\alpha, d) \equiv \frac{\phi(d)}{\phi(d_1)} \mu(l_0) \phi(p^{r_0}) \pmod{p^\alpha} \equiv \frac{\phi(d)}{\phi(l_0)} \mu(l_0) \pmod{p^\alpha}.$$

This completes the proof of Theorem 1.

When $\alpha = 1$, $d|(p - 1)$, $r_0 = 0$ and $l_0 = d/(r, d) = d_1$, we have

$$S_r(p, d) \equiv \frac{\phi(d)}{\phi(d_1)} \mu(d_1) \pmod{p}$$

which is exactly the result obtained by Moller ([2]).

**Proof of Theorem 2**: Notice that $h(d)$ is multiplicative, and $p(d)$ is additive, therefore

$$\frac{\phi(d)\mu(h(d)p^{-p(d)})}{\phi(h(d)p^{-p(d)})}$$

is multiplicative. Moreover, it can be easily shown that $F(x, r)$ is multiplicative in $x$.

Suppose that $q$ is a prime, when $(q, p) = 1$, we have

$$F(q^{\alpha_1}, r) = \sum_{d|q^\alpha_1} \frac{\phi(d)}{\phi(h(d))} \mu(h(d)) = \sum_{k=0}^{\alpha_1} \frac{\phi(q^k)}{\phi(q^k)} \mu\left(\frac{q^k}{(r, q^k)}\right).$$

If $(q^{\alpha_1}, r) = q^\beta$, $0 < \beta < \alpha_1$, then

$$F(q^{\alpha_1}, r) = \sum_{i=0}^{\beta} \frac{\phi(q^i)}{\phi(q)} \mu(q) + \frac{\phi(q^{\beta+1})}{\phi(q)} \mu(q)$$

$$= \sum_{i=0}^{\beta} \phi(q^i) - \phi(q^{\beta+1}) = q^\beta - q^\beta = 0$$

If $(q^{\alpha_1}, r) = q^{\alpha_1}$, then $F(q^{\alpha_1}, r) = \sum_{d|q^\alpha_1} \phi(d_1) = q^{\alpha_1}$. When $q = p$,

$$F(p^\beta, r) = \sum_{d|p^\beta} \frac{\phi(d)}{\phi(h(d)p^{-p(d)})} \mu(h(d)p^{-p(d)}) = \sum_{d|p^\beta} \phi(d) = p^\beta.$$

Therefore, if $x = p^{\beta_1}p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the canonical prime factorization, then we have

$$F(x, r) = F(p^{\beta_1}, r)F(p_1^{\alpha_1}, r) \cdots F(p_k^{\alpha_k}, r)$$

$$= \left\{ \begin{array}{ll} p^{\beta_1}p_1^{\alpha_1} \cdots p_k^{\alpha_k} = x, & \text{if } p^{-p\alpha_k}(x) \nmid r; \\ 0, & \text{otherwise.} \end{array} \right.$$

This completes the proof of Theorem 2.
References


