Filomat 39:17 (2025), 5999–6010
https://doi.org/10.2298/FIL2517999S

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

On the solution set of additive and multiplicative congruences modulo squares of primes

Zhongyan Shen[a,*], Tianxin Cai[b]

[a]*Department of Mathematics, Zhejiang International Studies University, Hangzhou 310023, P. R. China*
[b]*School of Mathematical Sciences, Zhejiang University, Hangzhou 310058, P. R. China*

Abstract. Let p be an odd prime. We consider the solution sets

$$S_+(p^2) = \{n \in Z_{p^2}^* \mid n \equiv a + b \equiv ab \pmod{p^2}\}$$

and

$$S_-(p^2) = \{n \in Z_{p^2}^* \mid n \equiv a - b \equiv ab \pmod{p^2}\},$$

where $Z_{p^2}^*$ denote a reduced residue system modulo p^2. We also establish congruences about sum and product of the residues or quadratic residues in $S_+(p^2)$ or in $S_-(p^2)$ modulo p^2. Finally, we obtain the number of solution sets based on the classification of prime numbers, where a and b are quadratic residues or quadratic non-residues, respectively.

1. Introduction

Let R and N be the set of quadratic residues and quadratic non-residues modulo p, in [2], define

$$RR = \{a \in Z_p^* \mid a \in R, a+1 \in R\}, NN = \{a \in Z_p^* \mid a \in N, a+1 \in N\}$$

and

$$RN = \{a \in Z_p^* \mid a \in R, a+1 \in N\}, NR = \{a \in Z_p^* \mid a \in N, a+1 \in R\},$$

where Z_p^* denote a reduced residue system modulo p. Then

$$|RR| = \frac{p-4-\left(\frac{-1}{p}\right)}{4}, |NN| = \frac{p-2+\left(\frac{-1}{p}\right)}{4}, \tag{1}$$

2020 *Mathematics Subject Classification*. Primary 11A07; Secondary 11A15, 11R11.
Keywords. additive and multiplicative, congruences, quadratic residues, reduced residue system.
Received: 25 September 2024; Revised: 09 April 2025; Accepted: 28 April 2025
Communicated by Paola Bonacini
Supported by National Natural Science Foundation of China, Project 12071421.
* Corresponding author: Zhongyan Shen
Email addresses: huanchenszyan@163.com (Zhongyan Shen), txcai@zju.edu.cn (Tianxin Cai)
ORCID iD: https://orcid.org/0000-0002-0467-522X (Zhongyan Shen)

$$|RN| = \frac{p - \left(\frac{-1}{p}\right)}{4}, |NR| = \frac{p - 2 + \left(\frac{-1}{p}\right)}{4}, \tag{2}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, see [2], [5] and [1]. Recently, we [3] considered the sum and product properties of solutions of the following equations

$$n \equiv a + b \equiv ab \pmod{p}$$

and

$$n \equiv a - b \equiv ab \pmod{p}$$

with $n \in Z_p^*$. Analogs of Wilson's and Wolstenholme's theorems on the solution sets

$$\{n \in Z_p^* \mid n \equiv a + b \equiv ab \pmod{p}\},$$

$$\{n \in Z_p^* \mid n \equiv a - b \equiv ab \pmod{p}\},$$

$$\{n \in R \mid n \equiv a + b \equiv ab \pmod{p}\},$$

$$\{n \in N \mid n \equiv a + b \equiv ab \pmod{p}\},$$

$$\{n \in R \mid n \equiv a - b \equiv ab \pmod{p}\},$$

and

$$\{n \in N \mid n \equiv a - b \equiv ab \pmod{p}\}$$

are given. In this paper, we consider the sum and product properties of solutions of the following congruences

$$n \equiv a + b \equiv ab \pmod{p^2} \tag{3}$$

and

$$n \equiv a - b \equiv ab \pmod{p^2} \tag{4}$$

with $n \in Z_{p^2}^*$. Define the solution sets

$$S_+(p^2) = \{n \in Z_{p^2}^* \mid n \equiv a + b \equiv ab \pmod{p^2}\}$$

and

$$S_-(p^2) = \{n \in Z_{p^2}^* \mid n \equiv a - b \equiv ab \pmod{p^2}\}.$$

We consider the distribution of quadratic residues on the solution sets and give congruences for the sum and product of quadratic residues in those sets modulo p^2.

2. Auxiliary Results

In order to prove the theorems, we need the following lemmas.

Lemma 2.1 ([3]). *For any prime $p > 3$ and integer l, we have*

$$\sum_{a \in R} a^l \equiv \begin{cases} 0 \pmod{p}, & \text{if } \frac{p-1}{2} \nmid l, \\ \frac{p-1}{2} \pmod{p}, & \text{if } \frac{p-1}{2} \mid l, \end{cases}$$

$$\sum_{a \in R} a^l \equiv 1 \pmod{3}.$$

Lemma 2.2 ([3]). *For any prime $p > 3$, we have*

$$\prod_{a\in R\setminus\{1\}} (a-1) \equiv \prod_{a\in R\setminus\{1,2\}} (a-1) \equiv \frac{1}{2}\left(\frac{-1}{p}\right) \pmod{p},$$
$$\sum_{a\in R\setminus\{1\}} \frac{1}{a-1} \equiv \frac{3}{4} \pmod{p}.$$

Lemma 2.3 ([2]). *Let $m > 1$ be an arbitrary integer. Then*

$$\prod_{\substack{1\le i\le m\\(i,m)=1}} i \equiv \begin{cases} -1 \pmod{m}, & \text{if } m = 2, 4, p^\alpha, 2p^\alpha, \\ 1 \pmod{m}, & \text{otherwise.} \end{cases}$$

Let R_m denote the set of quadratic residues modulo m.

Lemma 2.4 ([4]). *Let p be an odd prime and $e > 1$ be an integer. Then $a \in R_{p^e}$ if and only if $a \in R_p$.*

3. On the solutions of equation (3)

For the rest of this article, we say that $n \pmod{p^2}$ is a solution of (3) or (4) if there is a pair (a, b) such that (3) or (4) holds.

Theorem 3.1. *Let $p > 3$ be a prime. For each solution n, except for the case of $a \equiv b \equiv 2 \pmod{p}$, there is only one (n, a, b) that satisfying (3) apart from the order of (a, b).*

Proof. If $a \equiv 1 \pmod{p}$, congruence (3) has no solution. For any $(a(a-1)), p^2) = 1$, congruence

$$a + b - ab \equiv 0 \pmod{p^2}$$

has exactly one solution $b \equiv a/(a-1) \pmod{p^2}$. Assume that both $(n, a_1, b_1), (n, a_2, b_2)$ satisfy (3). Then, we have

$$a_1 + \frac{a_1}{a_1 - 1} \equiv a_2 + \frac{a_2}{a_2 - 1} \pmod{p^2}$$

or

$$\frac{(a_1 + a_2 - a_1a_2)(a_1 - a_2)}{(a_1 - 1)(a_2 - 1)} \equiv 0 \pmod{p^2},$$

which means $a_1 \equiv a_2 \pmod{p^2}$ or $a_1 \equiv \frac{a_2}{a_2-1} \pmod{p^2}$ or $a_1 \equiv a_2 \equiv 2 \pmod{p}$ (Let go of the situation where $a_1 \equiv a_2 \equiv 0 \pmod{p}$). This indicates that except for the case of $a \equiv b \equiv 2 \pmod{p}$, all other solutions are unique apart from the order of (a, b).

If $a \equiv b \equiv 2 \pmod{p}$, let $a \equiv 2 + pk \pmod{p^2}$, then $b \equiv \frac{2+pk}{1+pk} \pmod{p^2}$ and

$$n \equiv a + b \equiv 2 + pk + \frac{2 + pk}{1 + pk} \equiv 4 \pmod{p^2}.$$

□

Theorem 3.2. *Let p be an odd prime. Then the product of solutions of (3)*

$$\prod_{n\in S_+(p^2)} n \equiv -\frac{1}{2^{p-2}} \pmod{p^2}.$$

Proof. From Theorem 3.1, we know that all a and b except $a \equiv b \equiv 2 \pmod{p}$ and $a \equiv b \equiv 1 \pmod{p}$ in triples (n, a, b) satisfying (3), are not congruent to each other. Hence, a and b traverse the residue class modulo p^2 exactly once except 4, if we replace n with ab in the product. Therefore

$$\prod_{n\in S_+(p^2)} n \equiv \prod_{\substack{ab\in S_+(p^2)\\ a\le b}} ab \equiv \frac{2\prod_{\substack{1\le i\le p^2\\ (i,p^2)=1}} i}{\prod_{1\le j,k\le p-1}(1+jp)(2+kp)} \equiv -\frac{1}{2^{p-2}} \pmod{p^2}.$$

by Lemma 2.3. □

Theorem 3.3. *Let $p > 3$ be a prime and integer k with $0 \le k < p-1$. Then the power sum of the solutions of* (3)

$$\sum_{n\in S_+(p^2)} n^k \equiv \begin{cases} 2^{2k} - 2^{2k-1}p - \frac{p}{2}\binom{2k}{k} \pmod{p^2}, & \text{if } 0 < k < p-1,\\ \frac{(p-1)(p-2)}{2} \pmod{p^2}, & \text{if } k = 0. \end{cases}$$

Proof. For each a with $(a(a-1), p) = 1$, we have

$$b \equiv \frac{a}{a-1} \pmod{p^2},$$

and n can be written as ab or ba with $a, b \not\equiv 2 \pmod{p}$ except when $n \equiv 4 \pmod{p^2}$. Hence, for $p > 3$, let $a \equiv ip + j \pmod{p^2}, 0 \le i \le p-1, 3 \le j \le p-1$, we have

$$\sum_{n\in S_+(p^2)} n^k \equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{j=3}^{p-1} \frac{(ip+j)^{2k}}{(ip+j-1)^k}\right) + 2^{2k} \pmod{p^2}.$$

If $k = 0$, then $|S_+(p^2)| = \sum_{n\in S_+(p^2)} n^k = \frac{p(p-3)}{2} + 1 = \frac{(p-1)(p-2)}{2}$.

$$\begin{aligned}
\sum_{n\in S_+(p^2)} n^k &\equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{j=3}^{p-1} \frac{(ip+j)^{2k}}{(ip+j-1)^k}\right) + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{i=0}^{p-1}\sum_{j=3}^{p-1} \frac{j^{2k}(1+\frac{ip}{j})^{2k}}{(j-1)^k(1+\frac{ip}{j-1})^k} + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{i=0}^{p-1}\sum_{j=3}^{p-1} \frac{j^{2k}}{(j-1)^k}(1+\frac{2kip}{j})(1-\frac{kip}{j-1}) + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{i=0}^{p-1}\sum_{j=3}^{p-1} \frac{j^{2k}}{(j-1)^k}(1+\frac{2kip}{j}-\frac{kip}{j-1}) + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{j=3}^{p-1}\sum_{i=0}^{p-1} \frac{j^{2k}}{(j-1)^k}(1+\frac{2kip}{j}-\frac{kip}{j-1}) + 2^{2k}\\
&\equiv \frac{p}{2}\sum_{j=3}^{p-1} \frac{j^{2k}}{(j-1)^k} + 2^{2k} \pmod{p^2}.
\end{aligned}$$

If $0 < k < p-1$, by the proof of Theorem 3.3 in [3], we obtain $\sum_{j=3}^{p-1} \frac{j^{2k}}{(j-1)^k} \equiv -2^{2k} - \binom{2k}{k} \pmod{p}$. Hence,

$$\sum_{n\in S_+(p^2)} n^k \equiv 2^{2k} - 2^{2k-1}p - \frac{p}{2}\binom{2k}{k} \pmod{p^2}.$$

□

Theorem 3.4. *Let $p > 3$ be a prime. Then for integer k with $0 \le k < p-1$, the power sum of quadratic residues in solutions of* (3) *satisfies*

$$\sum_{n\in S_+(p^2)\cap R_{p^2}} n^k \equiv \begin{cases} \frac{p^2-4p-p\left(\frac{-1}{p}\right)+4}{4} \pmod{p^2}, & \text{if } k=0,\\ 2^{2k}-2^{2k-1}p-\frac{p}{4}\binom{2k}{k} \pmod{p^2}, & \text{if } 0<k<\frac{p-1}{2},\\ 2^{2k}-2^{2k-1}p-\frac{p}{4}\left(\binom{2k}{k}+2\binom{2k}{k-\frac{p-1}{2}}\right) \pmod{p^2}, & \text{if } \frac{p-1}{2}\le k<p-1. \end{cases}$$

Proof. Since $n \in S_+(p^2)$, we have $n \equiv \frac{a^2}{a-1} \pmod{p^2}$. If $n \in S_+(p^2)\cap R_{p^2}$, then $a-1$ is a quadratic residue modulo p^2. By Lemma 2.4, we obtain $a-1$ is also a quadratic residue modulo p. Let $a \equiv ip+j \pmod{p^2}, 0 \le i \le p-1, 3 \le j \le p-1$, if $a-1 \in R_{p^2}$, then $a-1 \in R_p$ i.e., $j-1 \in R_p$.

$$\sum_{n\in S_+(p^2)\cap R_{p^2}} n^k \equiv \frac{1}{2}\left(\sum_{a-1\in R_{p^2}} \frac{a^{2k}}{(a-1)^k} - 2^{2k}p\right) + 2^{2k}$$

$$\equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1} \frac{(ip+j)^{2k}}{(ip+j-1)^k}\right) + 2^{2k} \pmod{p^2}.$$

If $k=0$, by Lemma 2.1, we have $|S_+(p^2)\cap R_{p^2}| = \frac{p}{2}\frac{p-3}{2} - \frac{p}{2}\frac{1+\left(\frac{-1}{p}\right)}{2} + 1 = \frac{p^2-4p-p\left(\frac{-1}{p}\right)+4}{4}$. For $0 < k < p-1$, we have

$$\begin{aligned}
\sum_{n\in S_+(p^2)\cap R_{p^2}} n^k &\equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1} \frac{(ip+j)^{2k}}{(ip+j-1)^k}\right) + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{i=0}^{p-1}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1} \frac{j^{2k}}{(j-1)^k}\left(1+\frac{2kip}{j}\right)\left(1-\frac{kip}{j-1}\right) + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{i=0}^{p-1}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1} \frac{j^{2k}}{(j-1)^k}\left(1+\frac{2kip}{j}-\frac{kip}{j-1}\right) + 2^{2k}\\
&\equiv \frac{1}{2}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1}\sum_{i=0}^{p-1} \frac{j^{2k}}{(j-1)^k}\left(1+\frac{2kip}{j}-\frac{kip}{j-1}\right) + 2^{2k}\\
&\equiv \frac{p}{2}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1} \frac{j^{2k}}{(j-1)^k} + 2^{2k}\\
&\equiv \frac{p}{2}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1} \frac{(j-1+1)^{2k}}{(j-1)^k} + 2^{2k}\\
&\equiv \frac{p}{2}\sum_{t=0}^{2k}\binom{2k}{t}\sum_{\substack{j=3\\ j-1\in R_p}}^{p-1}(j-1)^{t-k} + 2^{2k}
\end{aligned}$$

$$\equiv \frac{p}{2}\sum_{t=0}^{2k}\binom{2k}{t}\left(\sum_{\substack{j=2\\ j-1\in R_p}}^{p}(j-1)^{t-k}-1-\frac{1+\left(\frac{-1}{p}\right)}{2}(-1)^{t-k}\right)+2^{2k}$$

$$\equiv \frac{p}{2}\sum_{t=0}^{2k}\binom{2k}{t}\sum_{\substack{j=2\\ j-1\in R_p}}^{p}(j-1)^{t-k}-2^{2k-1}p+2^{2k} \pmod{p^2}.$$

By Lemma 2.1, if $0<k<\frac{p-1}{2}$, then

$$\sum_{n\in S_+(p^2)\cap R_{p^2}} n^k \equiv 2^{2k}-2^{2k-1}p-\frac{p}{4}\binom{2k}{k} \pmod{p^2}.$$

If $\frac{p-1}{2}\le k<p-1$, except $t-k=0,\pm\frac{p-1}{2}$, other terms in the first sum are congruent to 0 modulo p^2 by Lemma 2.1, thus

$$\sum_{n\in S_+(p^2)\cap R_{p^2}} n^k \equiv 2^{2k}-2^{2k-1}p+\frac{p}{2}\frac{p-1}{2}\left(\binom{2k}{k}+\binom{2k}{k-\frac{p-1}{2}}+\binom{2k}{k+\frac{p-1}{2}}\right)$$

$$\equiv 2^{2k}-2^{2k-1}p-\frac{p}{4}\left(\binom{2k}{k}+2\binom{2k}{k-\frac{p-1}{2}}\right) \pmod{p^2}.$$

□

By Theorem 3.3, Theorem 3.4 and

$$\sum_{n\in S_+(p^2)}\left(\frac{n}{p}\right)n^k=\sum_{n\in S_+(p^2)\cap R_{p^2}}n^k-\sum_{n\in S_+(p^2)\cap N_{p^2}}n^k=2\sum_{n\in S_+(p^2)\cap R_{p^2}}n^k-\sum_{n\in S_+(p^2)}n^k,$$

where N_{p^2} is the set of quadratic non-residues modulo p^2. We obtain the following corollary.

Corollary 3.5. *Let $p>3$ be a prime and arbitrary integer k with $0\le k<p-1$. Then*

$$\sum_{n\in S_+(p^2)}\left(\frac{n}{p}\right)n^k\equiv$$

$$\begin{cases}1-\frac{p}{2}\left(1+\left(\frac{-1}{p}\right)\right) \pmod{p^2}, & \text{if } k=0,\\ 2^{2k}-2^{2k-1}p \pmod{p^2}, & \text{if } 0<k<\frac{p-1}{2},\\ 2^{2k}-2^{2k-1}p-p\binom{2k}{k-\frac{p-1}{2}} \pmod{p^2}, & \text{if } \frac{p-1}{2}\le k<p-1.\end{cases}$$

In particular, we obtain

$$|S_+(p^2)\cap N_{p^2}|=|S_+(p^2)|-|S_+(p^2)\cap R_{p^2}|$$

$$=\frac{p^2-3p+2}{2}-\frac{p^2-4p-p\left(\frac{-1}{p}\right)+4}{4}$$

$$=\frac{p^2-2p+p\left(\frac{-1}{p}\right)}{4}.$$

4. On the solutions of equation (4)

Theorem 4.1. *Let $p > 3$ be a prime. For each solution n, except for the case of $a \equiv -b \equiv -2 \pmod{p}, n \equiv -4 \pmod{p^2}$, the solutions of (4) come in pairs of the form (n, a, b) and $(n, p^2 - b, p^2 - a)$.*

Proof. If $a \equiv -1 \pmod{p}$, congruence (4) has no solution. For any $(a(a+1)), p^2) = 1$, congruence

$$a - b - ab \equiv 0 \pmod{p^2}$$

has exactly one solution $b \equiv a/(a+1) \pmod{p^2}$. Assume that both $(n, a_1, b_1), (n, a_2, b_2)$ satisfy (4). Then, we have

$$a_1 - \frac{a_1}{a_1 + 1} \equiv a_2 - \frac{a_2}{a_2 + 1} \pmod{p^2}$$

or

$$\frac{(a_1 + a_2 + a_1 a_2)(a_1 - a_2)}{(a_1 + 1)(a_2 + 1)} \equiv 0 \pmod{p^2},$$

which means $a_1 \equiv a_2 \pmod{p^2}$ or $a_1 \equiv -\frac{a_2}{a_2+1} \pmod{p^2}$ or $a_1 \equiv a_2 \equiv -2 \pmod{p}$ (Let go of the situation where $a_1 \equiv a_2 \equiv 0 \pmod{p}$). This indicates that except for the case of $a \equiv -b \equiv -2 \pmod{p}$, all other solutions come in pairs of the form (n, a, b) and $(n, p^2 - b, p^2 - a)$.

If $a \equiv -2 \pmod{p}$, let $a \equiv -2 + pk \pmod{p^2}$, then $b \equiv \frac{-2+pk}{-1+pk} \pmod{p^2}$ and

$$n \equiv a - b \equiv -2 + pk - \frac{-2 + pk}{-1 + pk} \equiv -4 \pmod{p^2}.$$

□

Theorem 4.2. *Let $p > 3$ be a prime and integer k with $0 \le k < p - 1$. Then the power sum of the solutions of (4)*

$$\sum_{n \in S_-(p^2)} n^k \equiv \begin{cases} (-1)^k \left(2^{2k} - 2^{2k-1} p - \frac{p}{2}\binom{2k}{k}\right) \pmod{p^2}, & \text{if } 0 < k < p - 1, \\ \frac{(p-1)(p-2)}{2} \pmod{p^2}, & \text{if } k = 0. \end{cases}$$

Proof. For each a with $(a(a+1), p) = 1$, we have

$$b \equiv \frac{a}{a+1} \pmod{p^2},$$

and n can be uniquely written as ab or $(p^2 - b)(p^2 - a)$ except $n \equiv -4 \equiv -2 \times 2 \pmod{p^2}$. Hence, for $p > 3$, let $a \equiv ip + j \pmod{p^2}, 0 \le i \le p - 1, 1 \le j \le p - 3$, we have

$$\sum_{n \in S_-(p^2)} n^k \equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{j=1}^{p-3} \frac{(ip + j)^{2k}}{(ip + j + 1)^k}\right) + (-4)^k \pmod{p^2}.$$

If $k = 0$, then $|S_-(p^2)| = \frac{p(p-3)}{2} + 1 = \frac{(p-1)(p-2)}{2}$. If $0 < k < p - 1$, similar to the proof of Theorem 3.3, we obtain

$$\begin{aligned} \sum_{n \in S_-(p^2)} n^k &\equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{j=1}^{p-3} \frac{(ip + j)^{2k}}{(ip + j + 1)^k}\right) + (-4)^k \\ &\equiv (-1)^k \left(2^{2k} - 2^{2k-1} p - \frac{p}{2}\binom{2k}{k}\right) \pmod{p^2}. \end{aligned}$$

□

Theorem 4.3. *Let p be a prime, then the product of solutions of* (4)

$$\prod_{m\in S_-(p^2)} m \equiv -\frac{1}{2^{p-2}}\left(\frac{-1}{p}\right) \pmod{p^2}.$$

Proof. We see that $(a, \frac{a}{a-1}), (-\frac{a}{a-1}, a)$ satisfy congruences (3), (4) separately. Therefore, by Theorem 4.2

$$\prod_{m\in S_-(p^2)} m \equiv (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{n\in S_+(p^2)} n \equiv (-1)^{\frac{p-1}{2}} \prod_{n\in S_+(p^2)} n \pmod{p^2}.$$

Then, by Theorem 3.2, we obtain the theorem. □

Theorem 4.4. *Let $p > 3$ be a prime. Then for integer k with $0 \le k < p-1$, the power sum of quadratic residues in solutions of* (4) *satisfies*

$$\sum_{n\in S_-(p^2)\cap R_{p^2}} n^k \equiv$$
$$\begin{cases} \frac{p^2-4p-(p-2)\left(\frac{-1}{p}\right)+2}{4} \pmod{p^2}, & \text{if } k=0,\\ (-4)^{k-1}\left(1+\left(\frac{-1}{p}\right)\right)(p-2)-\frac{(-1)^k p}{4}\binom{2k}{k} \pmod{p^2}, & \text{if } 0<k<\frac{p-1}{2},\\ (-4)^{k-1}\left(1+\left(\frac{-1}{p}\right)\right)(p-2)-\frac{(-1)^k p}{4}\left(\binom{2k}{k}+2\left(\frac{-1}{p}\right)\binom{2k}{k-\frac{p-1}{2}}\right) \pmod{p^2}, & \text{if } \frac{p-1}{2}\le k<p-1. \end{cases}$$

Proof. Since $n \in S_-(p^2)$, we have $n \equiv \frac{a^2}{a+1} \pmod{p^2}$. If $n \in S_-(p^2) \cap R_{p^2}$, then $a+1$ is a quadratic residue modulo p^2. By Lemma 2.4, we obtain $a+1$ is also a quadratic residue modulo p. Let $a \equiv ip + j \pmod{p^2}, 0 \le i \le p-1, 1 \le j \le p-3$, if $a+1 \in R_{p^2}$, then $a+1 \in R_p$ i.e., $j+1 \in R_p$.

$$\sum_{n\in S_-(p^2)\cap R_{p^2}} n^k \equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{\substack{j=1\\ j+1\in R_p}}^{p-3}\frac{(ip+j)^{2k}}{(ip+j+1)^k}\right)+(-4)^k\frac{1+(\frac{-4}{p})}{2} \pmod{p^2}.$$

If $k=0$, by Lemma 2.1, we have $|S_-(p^2)\cap R_{p^2}| = \frac{p}{2}\frac{p-3}{2} - \frac{p}{2}\frac{1+\left(\frac{-1}{p}\right)}{2} + \frac{1+(\frac{-1}{p})}{2} = \frac{p^2-4p-(p-2)\left(\frac{-1}{p}\right)+2}{4}$. For $0<k<p-1$, we have

$$\begin{aligned} &\sum_{n\in S_-(p^2)\cap R_{p^2}} n^k\\ &\equiv \frac{1}{2}\left(\sum_{i=0}^{p-1}\sum_{\substack{j=1\\ j+1\in R_p}}^{p-3}\frac{(ip+j)^{2k}}{(ip+j+1)^k}\right)+(-4)^k\frac{1+(\frac{-1}{p})}{2}\\ &\equiv \frac{1}{2}\sum_{i=0}^{p-1}\sum_{\substack{j=1\\ j+1\in R_p}}^{p-3}\frac{j^{2k}}{(j+1)^k}(1+\frac{2kip}{j})(1-\frac{kip}{j+1})+(-4)^k\frac{1+(\frac{-1}{p})}{2} \end{aligned}$$

$$\equiv \frac{p}{2}\sum_{\substack{j=1\\ j+1\in R_p}}^{p-3}\frac{j^{2k}}{(j+1)^k}+(-4)^k\frac{1+(\frac{-1}{p})}{2}$$

$$\equiv \frac{p}{2}\sum_{\substack{j=1\\ j+1\in R_p}}^{p-3}\frac{(j+1-1)^{2k}}{(j+1)^k}+(-4)^k\frac{1+(\frac{-1}{p})}{2}$$

$$\equiv \frac{p}{2}\sum_{t=0}^{2k}(-1)^{2k-t}\binom{2k}{t}\sum_{\substack{j=1\\ j+1\in R_p}}^{p-3}(j+1)^{t-k}+(-4)^k\frac{1+(\frac{-1}{p})}{2}$$

$$\equiv \frac{p}{2}\sum_{t=0}^{2k}(-1)^{t}\binom{2k}{t}\left(\sum_{\substack{j=0\\ j+1\in R_p}}^{p-2}(j+1)^{t-k}-1-\frac{1+\left(\frac{-1}{p}\right)}{2}(-1)^{t-k}\right)+(-4)^k\frac{1+(\frac{-1}{p})}{2}$$

$$\equiv \frac{p}{2}\sum_{t=0}^{2k}(-1)^{t}\binom{2k}{t}\left(\sum_{\substack{j=0\\ j+1\in R_p}}^{p-2}(j+1)^{t-k}-\frac{1+\left(\frac{-1}{p}\right)}{2}(-1)^{t-k}\right)+(-4)^k\frac{1+(\frac{-1}{p})}{2} \pmod{p^2}.$$

By Lemma 2.1, if $0<k<\frac{p-1}{2}$, then

$$\sum_{n\in S_-(p^2)\cap R_{p^2}} n^k \equiv (-4)^k\frac{1+(\frac{-1}{p})}{2}+\frac{p}{2}(-1)^k\binom{2k}{k}\frac{p-1}{2}-\frac{p}{2}(-4)^k\frac{1+\left(\frac{-1}{p}\right)}{2}$$

$$\equiv (-4)^{k-1}\left(1+\left(\frac{-1}{p}\right)\right)(p-2)-\frac{(-1)^k p}{4}\binom{2k}{k} \pmod{p^2}.$$

If $\frac{p-1}{2}\le k<p-1$, except $t-k=0,\pm\frac{p-1}{2}$, other terms in the first sum are congruent to 0 modulo p^2 by Lemma 2.1, thus

$$\sum_{n\in S_-(p^2)\cap R_{p^2}} n^k \equiv$$

$$(-4)^k\frac{1+(\frac{-1}{p})}{2}+\frac{p}{2}\frac{p-1}{2}\left((-1)^k\binom{2k}{k}+(-1)^{k-\frac{p-1}{2}}\binom{2k}{k-\frac{p-1}{2}}+(-1)^{k+\frac{p-1}{2}}\binom{2k}{k+\frac{p-1}{2}}\right)$$

$$-\frac{p}{2}(-4)^k\frac{1+\left(\frac{-1}{p}\right)}{2}$$

$$\equiv (-4)^k\frac{1+(\frac{-1}{p})}{2}-\frac{p}{4}\left((-1)^k\binom{2k}{k}+2(-1)^{k-\frac{p-1}{2}}\binom{2k}{k-\frac{p-1}{2}}\right)-\frac{p}{4}(-4)^k\left(1+\left(\frac{-1}{p}\right)\right)$$

$$\equiv (-4)^{k-1}\left(1+\left(\frac{-1}{p}\right)\right)(p-2)-\frac{(-1)^k p}{4}\left(\binom{2k}{k}+2\left(\frac{-1}{p}\right)\binom{2k}{k-\frac{p-1}{2}}\right) \pmod{p^2}.$$

□

By Theorem 4.2, Theorem 4.4 and

$$\sum_{n\in S_-(p^2)}\left(\frac{n}{p}\right)n^k=\sum_{n\in S_-(p^2)\cap R_{p^2}}n^k-\sum_{n\in S_-(p^2)\cap N_{p^2}}n^k=2\sum_{n\in S_-(p^2)\cap R_{p^2}}n^k-\sum_{n\in S_-(p^2)}n^k,$$

we obtain the following corollary.

Corollary 4.5. *Let $p > 3$ be a prime and arbitrary integer k with $0 \le k < p-1$. Then*

$$\sum_{n\in S_-(p^2)} \left(\frac{n}{p}\right) n^k \equiv$$
$$\begin{cases} \left(\frac{-1}{p}\right) - \frac{p}{2}\left(1+\left(\frac{-1}{p}\right)\right) \pmod{p^2}, & \text{if } k=0, \\ (-4)^k\left(1-\frac{p}{2}\right)\left(\frac{-1}{p}\right) \pmod{p^2}, & \text{if } 0<k<\frac{p-1}{2}, \\ \left((-4)^k\left(1-\frac{p}{2}\right) - (-1)^k p\binom{2k}{k-\frac{p-1}{2}}\right)\left(\frac{-1}{p}\right) \pmod{p^2}, & \text{if } \frac{p-1}{2} \le k < p-1. \end{cases}$$

In particular, we obtain

$$\begin{aligned} |S_-(p^2)\cap N_{p^2}| &= |S_-(p^2)| - |S_-(p^2)\cap R_{p^2}| \\ &= \frac{p^2-3p+2}{2} - \frac{p^2-4p-(p-2)\left(\frac{-1}{p}\right)+2}{4} \\ &= \frac{p^2-2p+(p-2)\left(\frac{-1}{p}\right)+2}{4}. \end{aligned}$$

5. Problem

In the last section, we further consider the solution sets

$$S_+(RR) = \{n \in Z^*_{p^2} \mid n \equiv a+b \equiv ab \pmod{p^2}, a, b \in R_{p^2}\},$$

$$S_+(NN) = \{n \in Z^*_{p^2} \mid n \equiv a+b \equiv ab \pmod{p^2}, a, b \in N_{p^2}\},$$

$$S_+(RN) = \{n \in Z^*_{p^2} \mid n \equiv a+b \equiv ab \pmod{p^2}, a \in R_{p^2}, b \in N_{p^2}\},$$

$$S_+(NR) = \{n \in Z^*_{p^2} \mid n \equiv a+b \equiv ab \pmod{p^2}, a \in N_{p^2}, b \in R_{p^2}\},$$

$$S_-(RR) = \{n \in Z^*_{p^2} \mid n \equiv a-b \equiv ab \pmod{p^2}, a, b \in R_{p^2}\},$$

$$S_-(NN) = \{n \in Z^*_{p^2} \mid n \equiv a-b \equiv ab \pmod{p^2}, a, b \in N_{p^2}\}$$

$$S_-(RN) = \{n \in Z^*_{p^2} \mid n \equiv a-b \equiv ab \pmod{p^2}, a \in R_{p^2}, b \in N_{p^2}\}$$

and

$$S_-(NR) = \{n \in Z^*_{p^2} \mid n \equiv a-b \equiv ab \pmod{p^2}, a \in N_{p^2}, b \in R_{p^2}\}.$$

If $n \in S_+(RR)$, since $n \equiv a+b \equiv ab \pmod{p^2}, a, b \in R_{p^2}$, we have $b \equiv \frac{a}{a-1} \pmod{p^2}$ and $a-1 \in R_{p^2}$. Then both $a-1$ and a are quadratic residues modulo p^2. Due to symmetry, $|S_+(RR)|$ is half the number of pairs $(a,b) \pmod{p^2}$ such that $n \equiv a+b \equiv ab \pmod{p^2}, a, b \in R_{p^2}$ or half the number of pairs $(a-1, a) \pmod{p^2}$ such that both $a-1$ and a are quadratic residues modulo p^2, except $a \equiv 2 \pmod{p^2}$. Since

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8, \end{cases} \tag{5}$$

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1,3 \pmod 8, \\ -1, & p \equiv 5,7 \pmod 8, \end{cases} \left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1,5 \pmod 8, \\ -1, & p \equiv 3,7 \pmod 8, \end{cases} \tag{6}$$

By Lemma 2.4 and (5), we obtain $a-1$ and a are also quadratic residues modulo p. Let $a \equiv ip+j \pmod{p^2}, 0 \le i \le p-1, 3 \le j \le p-1$, $j-1, j \in R_p$, where $j=2 \in R_p$ *or* N_p needs to be considered separately. we have

$$|S_+(RR)| = \begin{cases} p\frac{|RR|-1}{2}+1, & p \equiv \pm 1 \pmod 8, \\ p\frac{|RR|}{2}, & p \equiv \pm 3 \pmod 8. \end{cases}$$

Similarly, we can obtain

$$|S_+(NN)| = \begin{cases} p\frac{|RN|}{2}, & p \equiv \pm 1 \pmod 8, \\ p\frac{|RN|-1}{2}+1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

If $n \in S_+(RN)$ or $n \in S_+(NR)$, due to symmetry, we have

$$|S_+(RN)| = |S_+(NR)| = \frac{1}{2}\left|S_+(p^2) \cap N_{p^2}\right|.$$

Similarly, by Lemma 2.4 and (6), we obtain a and $a+1$ are also quadratic residues modulo p. Let $a \equiv ip+j \pmod{p^2}, 0 \le i \le p-1, 1 \le j \le p-3$, $j, j+1 \in R_p$,where $j=p-2 \in R_p$ *or* N_p needs to be considered separately. we can obtain

$$|S_-(RR)| = \begin{cases} p\frac{|RR|-1}{2}+1, & p \equiv 1 \pmod 8, \\ p\frac{|RR|}{2}, & p \equiv 3,5,7 \pmod 8. \end{cases}$$

$$|S_-(NN)| = \begin{cases} p\frac{|NR|}{2}, & p \equiv 1,3,7 \pmod 8, \\ p\frac{|NR|-1}{2}+1, & p \equiv 5 \pmod 8. \end{cases}$$

$$|S_-(RN)| = \begin{cases} p\frac{|RN|}{2}, & p \equiv 1,5,7 \pmod 8, \\ p\frac{|RN|-1}{2}+1, & p \equiv 3 \pmod 8. \end{cases}$$

$$|S_-(NR)| = \begin{cases} p\frac{|NN|}{2}, & p \equiv 1,3,5 \pmod 8, \\ p\frac{|NN|-1}{2}+1, & p \equiv 7 \pmod 8. \end{cases}$$

Combining (1), (2) and Corollary 3.5, Corollary 4.5, we can calculate the specific value of $S_+(RR)$, $S_+(NN)$, $S_+(RN)$, $S_+(NR)$ and $S_-(RR), S_-(NN), S_-(RN), S_-(NR)$.

Define the solution sets

$$S_+(p^\alpha) = \{n \in Z^*_{p^\alpha} \mid n \equiv a+b \equiv ab \pmod{p^\alpha}\}.$$

We know that $|S_+(p)| = \frac{p-1}{2}$ in [3] and $|S_+(p^2)| = \frac{(p-1)(p-2)}{2}$ by Theorem 3.3. By the proof of Theorem 3.1, we obtain that except for the case of $a \equiv b \equiv 2 \pmod p$, all other $\frac{p^{\alpha-1}(p-3)}{2}$ solutions are unique apart from the order of (a, b).

Let $a \equiv 2+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1} \pmod{p^\alpha}, 0 \le k_i \le p-1, 1 \le i \le \alpha-1$, then

$$b \equiv \frac{2+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}}{1+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}} \pmod{p^\alpha}.$$

And

$$\begin{aligned}
n \equiv a+b &\equiv 2+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}+\frac{2+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}}{1+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}} \\
&\equiv 2+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}+(2+pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1}) \\
&\quad [1-(pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1})+(pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1})^2 \\
&\quad +\ldots+(-1)^{\alpha-1}(pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1})^{\alpha-1}] \\
&\equiv 4+(pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1})^2-(pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1})^3 \\
&\quad +\ldots+(-1)^{\alpha-1}(pk_1+p^2k_2+\ldots+p^{\alpha-1}k_{\alpha-1})^{\alpha-1} \\
&\overset{def}{\equiv} 4+\sum_{l=2}^{\alpha-1}p^l s_l \pmod{p^\alpha},
\end{aligned}$$

where

$$\begin{aligned}
s_l = &\sum_{\substack{a_1+a_2=l \\ a_1,a_2\geq 1}} k_{a_1}k_{a_2}-\sum_{\substack{a_1+a_2+a_3=l \\ a_1,a_2,a_3\geq 1}} k_{a_1}k_{a_2}k_{a_3} \\
&+\ldots+(-1)^{\alpha-1}\sum_{\substack{a_1+a_2+\ldots+a_{\alpha-1}=l \\ a_1,a_2,\ldots,a_{\alpha-1}\geq 1}} k_{a_1}k_{a_2}\ldots k_{a_{\alpha-1}}.
\end{aligned}$$

We have $s_2 = k_1^2, s_3 = 2k_1k_2 - k_1^3, s_4 = 2k_1k_3 + k_2^2 - 3k_1^2k_2 + k_1^4, s_5 = 2k_1k_4 + 2k_2k_3 - 3k_1^2k_3 - 3k_1k_2^2 + 4k_1^3k_2 - k_1^5, \ldots$.

If k_1 runs through a complete set of residues modulo p, then k_1^2 runs through $\frac{p+1}{2}$ classes of residues modulo p. Hence,

$$|S_+(p^3)| = \frac{p^2(p-3)}{2}+\frac{p+1}{2} = \frac{(p-1)(p^2-2p-1)}{2}.$$

If $k_1 = 0$, then $s_2 = 0, s_3 = 0, n \equiv 4 \pmod{p^4}$. If k_1 runs through a reduced set of residues modulo p, then k_1^2 runs through $\frac{p-1}{2}$ classes of residues modulo p and $2k_1k_2 - k_1^3$ runs through p classes of residues modulo p according to the given k_1. Hence,

$$|S_+(p^4)| = \frac{p^3(p-3)}{2}+1+\frac{p(p-1)}{2} = \frac{(p-1)(p^3-2p^2-p-2)}{2}.$$

What would be the result of the solution set about additive and multiplicative congruences for modulo higher powers of prime, or modulo any integers?

Acknowledgments

The authors wish to thank Dr. Peng Yang for his kind help in calculation, and also the authors thank the referee for his constructive suggestion and careful reading of the manuscript.

References

[1] George E. Andrews, Number Theory. Dover Publications, Inc. New York, 1994.
[2] T. X. Cai, A Modern Introduction to Classical Number Theory. World Scientific, Singapore, 2021.
[3] T. X. Cai, Z. Y. Shen, P. Yang, On the solution set of additive and multiplicative congruences modulo primes, Filomat **38:2** (2024), 621–635.
[4] Gareth A. Jones, J. Mary Jones, Elementary Number Theory. Springer, 2006.
[5] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*,(2nd edition), Springer, New York, 1990, 64.