Filomat 40:5 (2026), 1873–1882
https://doi.org/10.2298/FIL2605873S

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 primes II

Zhongyan Shen[a,*], Yucheng Jiang[a]

[a]*Department of Mathematics, Zhejiang International Studies University, Hangzhou 310023, P. R. China*

Abstract. Let $p > 3$ be a prime and

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

and

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

where Z_p^* denotes the set of reduced residue classes modulo p. In this work, we investigate the solution sets $|S_+ \cap S_-|$, $|\{n| \pm n \in S_+\}|$ and $|\{n|n \in S_+$ and $n + 4k \in S_+\}|$ for some given integer k. Meanwhile, we consider how many $n \in Z_p^*$ can be expressed as both a linear form and a quadratic form in two variables, and how many $n \in Z_p^*$ can be written as different quadratic forms of two variables.

1. Introduction

Let R and N be the set of quadratic residues and quadratic non-residues modulo p, in [3], 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^* denotes the set of reduced residue classes modulo p. Then

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

2020 *Mathematics Subject Classification*. primary 11A07; Secondary 11A15, 11R11.
Keywords. Additive and multiplicative congruences, Quadratic residues, Chinese Remainder Theorem.
Received: 14 August 2025; Revised: 03 December 2025; Accepted: 09 December 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), 2671201183@qq.com (Yucheng Jiang)

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, see [3], [5] and [1]. In 2024, Cai[4] etc. considered the sum and product properties of solutions of the following Diophantine equations

$$n \equiv a + b \equiv ab \pmod{p} \tag{1}$$

and

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

with $n \in Z_p^*$. Equations (1) and (2) have their own interesting properties. Analogs of Wilson's and Wolstenholme's theorems on the solution sets

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

and

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

are given in [4] and obtained $|S_+| = |S_-| = \frac{1}{2}(p-1)$. Moreover, the distribution of quadratic residues and quadratic non-residues on the solution sets were considered and they gave congruences for the sum and product of quadratic residues in those sets modulo p.

Recently, Cai and the first author [8] considered the solution sets

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

and

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

and established congruences about sum and product of the residues or quadratic residues in $S_+(p^2)$ or in $S_-(p^2)$ modulo p^2. Meanwhile, they obtained the number of solution sets based on the classification of prime numbers, where a and b are quadratic residues or quadratic non-residues, respectively.

In this paper, we consider the solution sets $|S_+ \cap S_-|$, $|\{n| \pm n \in S_+\}|$ and $|\{n|n \in S_+$ and $n + 4k \in S_+\}|$ for some given integer k. Meanwhile, we consider how many $n \in Z_p^*$ can be written in both linear and quadratic forms of two variables, and how many $n \in Z_p^*$ can be written as different quadratic forms of two variables.

For the rest of this article, we say that n is a solution modulo p of (1) if there is a pair (a, b) such that (1) holds, and we obtain the following theorems.

Theorem 1.1. *Let $p > 3$ be a prime. Then*

$$|S_+ \cap S_-| = \begin{cases} \frac{p-1}{4}, & p \equiv 1 \pmod{8}, \\ \frac{p-3}{4}, & p \equiv 3 \pmod{8}, \\ \frac{p-5}{4}, & p \equiv 5 \pmod{8}, \\ \frac{p+1}{4}, & p \equiv 7 \pmod{8}. \end{cases}$$

Theorem 1.2. *Let $p > 3$ be a prime. Then*

$$|\{n| \pm n \in S_+\}| = \begin{cases} \frac{p-1}{4}, & p \equiv 1 \pmod{8}, \\ \frac{p-3}{4}, & p \equiv 3 \pmod{8}, \\ \frac{p-5}{4}, & p \equiv 5 \pmod{8}, \\ \frac{p+1}{4}, & p \equiv 7 \pmod{8}. \end{cases}$$

Theorem 1.3. *Let $p > 3$ be a prime. Then*

$$|\{n|n \in S_+ \text{ and } n+4 \in S_+\}| = \frac{p-4-\left(\frac{-1}{p}\right)}{4}.$$

Theorem 1.4. *Let $p \equiv \pm 1 \pmod 8$ be a prime, integer k satisfying $k^2 \equiv 2 \pmod p$. If $p \equiv 1 \pmod 8$ and $p = a^2 + b^2$, where a is positive and odd. Then*

$$|\{n|n \in S_+ \text{ and } n+4k \in S_+\}| = \begin{cases} \frac{p-3+2(-1)^{\frac{a+1}{2}}a}{4}, & p \equiv 1 \pmod 8, \\ \frac{p-3}{4}, & p \equiv -1 \pmod 8. \end{cases}$$

Theorem 1.5. *Let $p > 3$ be a prime. Then*

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

has $\frac{p}{2} - \frac{1}{2}\left(\frac{-1}{p}\right)$ solutions.

Theorem 1.6. *Let $p > 3$ be a prime and $T = \{n \in Z_p^* \mid n \equiv a^2 + b^2 \equiv ab \pmod p\}$. Then*

$$|T| = \begin{cases} \frac{p-1}{2}, & p \equiv 1 \pmod 6, \\ 0, & p \equiv 5 \pmod 6, \end{cases}$$

and

$$T = \begin{cases} R, & p \equiv 1 \pmod{12}, \\ N, & p \equiv 7 \pmod{12}. \end{cases}$$

2. Preliminaries

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

Lemma 2.1 ([2, 7]). *For any integers a, b, c and odd prime p, satisfy $p \nmid a$,*

$$\sum_{x=1}^{p} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right), & p \nmid b^2 - 4ac, \\ (p-1)\left(\frac{a}{p}\right), & p \mid b^2 - 4ac. \end{cases}$$

Lemma 2.2 ([9]). *For prime $p \equiv 1 \pmod 6$, there is an element $c' \in Z_p^*$ of order 3, such that $(2c'+1)^2 \equiv -3 \pmod p$.*

Define $S(m) = \sum_{n \pmod p} \left(\frac{n(n^2-m)}{p}\right)$, where $n \pmod p$ denotes n go through any complete residue system modulo p.

Lemma 2.3 ([1]). *If prime $p \equiv 3 \pmod 4$, then $S(m) \equiv 0 \pmod p$.*

Lemma 2.4 ([6]). *Let p be a prime $p \equiv 1 \pmod 4$ and $p = a^2 + b^2$, where a is positive and odd. Then*

$$S(1) = \begin{cases} 2(-1)^{\frac{a+1}{2}}a, & p \equiv 1 \pmod 8, \\ 2(-1)^{\frac{a-1}{2}}a, & p \equiv 5 \pmod 8. \end{cases}$$

3. Proofs of the Theorems

Proof. [Proof of Theorem 1.1]
Since $n \equiv a + b \equiv ab \pmod{p}$, by $b \equiv n - a \pmod{p}$, we have $a^2 - na + n \equiv 0 \pmod{p}$. If the discriminant $n^2 - 4n$ is a quadratic residue modulo p, then n is a solution modulo p of (1). Specifically, $n = 4$ is a solution of (1). Thus, by Lemma 2.1, (1) has

$$\frac{1}{2}\sum_{\substack{n=1\\ n\neq 4}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]+1=\frac{p}{2}+\frac{1}{2}\sum_{n=1}^{p}\left(\frac{n^2-4n}{p}\right)=\frac{p-1}{2}$$

solutions, which is obtained in [4]. Similarly, if the discriminant $n^2 + 4n$ is a quadratic residue modulo p, then n is a solution modulo p of (2). Specifically, $n = p - 4$ is a solution of (2). If $n = 4$ is also a solution of (2), then we have

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

If $n = p - 4$ is also a solution of (1), then we have

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

In addition, $n \in S_+ \cap S_-$ if and only if both $n^2 - 4n$ and $n^2 + 4n$ are quadratic residues modulo p. Therefore,

$$\begin{aligned}
&|S_+ \cap S_-|\\
&=\frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]\left[1+\left(\frac{n^2+4n}{p}\right)\right]+1+\left(\frac{2}{p}\right)\\
&=\frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}1+\frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left(\frac{n^2-4n}{p}\right)+\frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left(\frac{n^2+4n}{p}\right)\\
&+\frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left(\frac{n^2-16}{p}\right)+1+\left(\frac{2}{p}\right). \qquad (4)
\end{aligned}$$

The first sum in (4) is equal to $p - 3$. The second, third and fourth sums are relatively easy to evaluate by Lemma 2.1, we obtain

$$\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left(\frac{n^2-4n}{p}\right)=\sum_{n=1}^{p}\left(\frac{n^2-4n}{p}\right)-\left(\frac{2}{p}\right)=-1-\left(\frac{2}{p}\right), \qquad (5)$$

$$\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left(\frac{n^2+4n}{p}\right)=\sum_{n=1}^{p}\left(\frac{n^2+4n}{p}\right)-\left(\frac{2}{p}\right)=-1-\left(\frac{2}{p}\right), \qquad (6)$$

$$\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left(\frac{n^2-16}{p}\right)=\sum_{n=1}^{p}\left(\frac{n^2-16}{p}\right)-\left(\frac{-1}{p}\right)=-1-\left(\frac{-1}{p}\right). \qquad (7)$$

Combining equations (4)-(7), we obtain

$$\begin{aligned}&|S_+ \cap S_-|\\ &= \frac{p-3}{4} - \frac{1}{4} - \frac{1}{4}\left(\frac{2}{p}\right) - \frac{1}{4} - \frac{1}{4}\left(\frac{2}{p}\right) - \frac{1}{4} - \frac{1}{4}\left(\frac{-1}{p}\right) + 1 + \left(\frac{2}{p}\right)\\ &= \frac{p-2+2\left(\frac{2}{p}\right)-\left(\frac{-1}{p}\right)}{4}. \end{aligned} \tag{8}$$

Since

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8,\\ -1, & p \equiv \pm 3 \pmod 8, \end{cases} \tag{9}$$

and

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4,\\ -1, & p \equiv 3 \pmod 4, \end{cases} \tag{10}$$

by equations (8)-(10) and Chinese Remainder Theorem, we have

$$|S_+ \cap S_-| = \begin{cases} \frac{p-1}{4}, & p \equiv 1 \pmod 8,\\ \frac{p-3}{4}, & p \equiv 3 \pmod 8,\\ \frac{p-5}{4}, & p \equiv 5 \pmod 8,\\ \frac{p+1}{4}, & p \equiv 7 \pmod 8. \end{cases}$$

This completes the proof of Theorem 1.1. □

Example 3.1. *If $p = 5$, then $S_+ = \{2,4\}$, $S_- = \{1,3\}$, $|S_+ \cap S_-| = 0$. If $p = 7$, then $S_+ = \{1,3,4\}$, $S_- = \{3,4,6\}$, $|S_+ \cap S_-| = 2$. If $p = 11$, then $S_+ = \{4,5,6,9,10\}$, $S_- = \{1,2,5,6,7\}$, $|S_+ \cap S_-| = 2$. If $p = 17$, then $S_+ = \{2,4,7,8,10,11,13,14\}$, $S_- = \{3,4,6,7,9,10,13,15\}$, $|S_+ \cap S_-| = 4$.*

Proof. [Proof of Theorem 1.2]
If $4 \in S_+$ and $p-4 \in S_+$, by the proof of Theorem 1.1, we have $1 + \left(\frac{2}{p}\right)$ solutions. In addition, if $n \in S_+$ and $p-n \in S_+$, then both n^2-4n and $(p-n)^2-4(p-n)$ are quadratic residues modulo p. Therefore,

$$\begin{aligned}&|\{n| \pm n \in S_+\}|\\ &= \frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]\left[1+\left(\frac{(p-n)^2-4(p-n)}{p}\right)\right] + 1 + \left(\frac{2}{p}\right)\\ &= \frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]\left[1+\left(\frac{n^2+4n}{p}\right)\right] + 1 + \left(\frac{2}{p}\right), \end{aligned}$$

together with equation (4), we obtain

$$|\{n| \pm n \in S_+\}| = |S_+ \cap S_-| = \begin{cases} \frac{p-1}{4}, & p \equiv 1 \pmod 8,\\ \frac{p-3}{4}, & p \equiv 3 \pmod 8,\\ \frac{p-5}{4}, & p \equiv 5 \pmod 8,\\ \frac{p+1}{4}, & p \equiv 7 \pmod 8. \end{cases}$$

This completes the proof of Theorem 1.2. □

Remark 3.2. *With the proof of Theorem 1.2, we obtain the following relations,*

$$|\{n| \pm n \in S_-\}| = |\{n| \pm n \in S_+\}| = |S_+ \cap S_-|.$$

Proof. [Proof of Theorem 1.3]
Whether $8 \in S_+$, it depends on whether the Legendre symbol $\left(\frac{2}{p}\right)$ takes the value of 1. In addition, if $n \in S_+$ and $n+4 \in S_+$, then both n^2-4n and $(n+4)^2-4(n+4)$ are quadratic residues modulo p. Therefore,

$$\begin{aligned}
&|\{n|n \in S_+ \text{ and } n+4 \in S_+\}| \\
&= \frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]\left[1+\left(\frac{(n+4)^2-4(n+4)}{p}\right)\right]+\frac{1+\left(\frac{2}{p}\right)}{2}\\
&= \frac{1}{4}\sum_{\substack{n=1\\ n\neq 4,p-4}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]\left[1+\left(\frac{n^2+4n}{p}\right)\right]+\frac{1+\left(\frac{2}{p}\right)}{2}.
\end{aligned}$$

together with equation (4), (8), we obtain

$$|\{n|n \in S_+ \text{ and } n+4 \in S_+\}| = \frac{p-4-\left(\frac{-1}{p}\right)}{4}.$$

This completes the proof of Theorem 1.3. □

Example 3.3. *If $p=5$, then $S_+ = \{2,4\}$, $|\{n|n \in S_+$ and $n+4 \in S_+\}| = 0$. If $p=7$, then$S_+ = \{1,3,4\}$,*

$$|\{n|n \in S_+ \textit{ and } n+4 \in S_+\}| = |\{4\}| = 1.$$

If $p=11$, then $S_+ = \{4,5,6,9,10\}$, $|\{n|n \in S_+$ and $n+4 \in S_+\}| = |\{5,6\}| = 2$. If $p=17$, then

$$S_+ = \{2,4,7,8,10,11,13,14\},\ |\{n|n \in S_+ \textit{ and } n+4 \in S_+\}| = |\{4,7,10\}| = 3.$$

Proof. [Proof of Theorem 1.4]
If $n \in S_+$ and $n+4k \in S_+$, then both n^2-4n and $(n+4k)^2-4(n+4k)$ are quadratic residues modulo p. Therefore,

$$\begin{aligned}
&|\{n|n \in S_+ \text{ and } n+4k \in S_+\}| \\
&= \frac{1}{4}\sum_{\substack{n=1\\ n\neq 4\\ n\not\equiv -4k \pmod p\\ n\not\equiv 4-4k \pmod p}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)\right]\left[1+\left(\frac{(n+4k)^2-4(n+4k)}{p}\right)\right]+\frac{1+\left(\frac{4k(4k+4)}{p}\right)}{2}+\frac{1+\left(\frac{-4k(-4k+4)}{p}\right)}{2}\\
&= \frac{1}{4}\sum_{\substack{n=1\\ n\neq 4\\ n\not\equiv -4k \pmod p\\ n\not\equiv 4-4k \pmod p}}^{p-1}\left[1+\left(\frac{n^2-4n}{p}\right)+\left(\frac{(n+4k)(n+4k-4)}{p}\right)\right.\\
&\left.+\left(\frac{n(n-4)(n+4k)(n+4k-4)}{p}\right)\right]+\frac{1+\left(\frac{k(k+1)}{p}\right)}{2}+\frac{1+\left(\frac{k(k-1)}{p}\right)}{2}. \qquad (11)
\end{aligned}$$

The first sum in (11) is equal to $p-4$. The second and third sums in (11) are relatively easy to evaluate by Lemma 2.1 and $k^2 \equiv 2 \pmod{p}$, we obtain

$$\begin{aligned}
&\sum_{\substack{n=1\\ n\neq 4\\ n\not\equiv -4k \pmod{p}\\ n\not\equiv 4-4k \pmod{p}}}^{p-1} \left(\frac{n^2-4n}{p}\right)\\
&=\sum_{n=1}^{p}\left(\frac{n^2-4n}{p}\right)-\left(\frac{-4k(-4k-4)}{p}\right)-\left(\frac{-4k(-4k+4)}{p}\right)\\
&=-1-\left(\frac{k+2}{p}\right)-\left(\frac{2-k}{p}\right), \qquad (12)
\end{aligned}$$

$$\begin{aligned}
&\sum_{\substack{n=1\\ n\neq 4\\ n\not\equiv -4k \pmod{p}\\ n\not\equiv 4-4k \pmod{p}}}^{p-1} \left(\frac{(n+4k)(n+4k-4)}{p}\right)\\
&=\sum_{n=1}^{p}\left(\frac{(n+4k)(n+4k-4)}{p}\right)-\left(\frac{4k(4k+4)}{p}\right)-\left(\frac{4k(4k-4)}{p}\right)\\
&=-1-\left(\frac{k+2}{p}\right)-\left(\frac{2-k}{p}\right). \qquad (13)
\end{aligned}$$

The fourth sum in (11)

$$\begin{aligned}
&\sum_{\substack{n=1\\ n\neq 4\\ n\not\equiv -4k \pmod{p}\\ n\not\equiv 4-4k \pmod{p}}}^{p-1} \left(\frac{n(n-4)(n+4k)(n+4k-4)}{p}\right)\\
&=\sum_{n=1}^{p-1}\left(\frac{n(n-4)(n+4k)(n+4k-4)}{p}\right)\\
&=\sum_{n=1}^{p-1}\left(\frac{(1-\frac{4}{n})(1+\frac{4k}{n})(1+\frac{4k-4}{n})}{p}\right). \qquad (14)
\end{aligned}$$

Since $n \not\equiv 0 \pmod{p}$, there exists an m such that $mn \equiv 1 \pmod{p}$. Thus, (14) becomes

$$\begin{aligned}
&\sum_{m=1}^{p-1}\left(\frac{(1-4m)(1+4km)(1+(4k-4)m)}{p}\right)\\
&=\left(\frac{-4\cdot 4k(4k-4)}{p}\right)\sum_{m=1}^{p-1}\left(\frac{(m-\frac{1}{4})(m+\frac{1}{4k})(m+\frac{1}{4k-4})}{p}\right)\\
&=\left(\frac{k-2}{p}\right)\left[\sum_{m=0}^{p-1}\left(\frac{(m-\frac{1}{4})(m+\frac{1}{4k})(m+\frac{1}{4k-4})}{p}\right)-\left(\frac{-\frac{1}{4}\frac{1}{4k}\frac{1}{4k-4}}{p}\right)\right]. \qquad (15)
\end{aligned}$$

Let $m+\frac{1}{4k}=l$, since

$$\frac{1}{4k}+\frac{1}{4}\equiv\frac{1+k}{4k}\equiv\frac{k+k^2}{4k^2}\equiv\frac{k+2}{8} \pmod{p}$$

and

$$\frac{1}{4k-4}-\frac{1}{4k}\equiv\frac{1}{4k(k-1)}\equiv\frac{k(k+1)}{4k^2(k^2-1)}\equiv\frac{k+2}{8}\pmod{p}.$$

Then (15) becomes

$$\begin{aligned}&\left(\frac{k-2}{p}\right)\left[\sum_{l=0}^{p-1}\left(\frac{l(l-\frac{1}{4k}-\frac{1}{4})(l-\frac{1}{4k}+\frac{1}{4k-4}}{p}\right)-\left(\frac{-2(k+2)}{p}\right)\right]\\ =&\left(\frac{k-2}{p}\right)\left[\sum_{l=0}^{p-1}\left(\frac{l(l^2-\frac{(k+2)^2}{64})}{p}\right)-\left(\frac{-2(k+2)}{p}\right)\right].\end{aligned}\tag{16}$$

In (16), let $l=\frac{k+2}{8}n$, we have

$$\left(\frac{k-2}{p}\right)\left(\frac{\frac{k+2}{8}}{p}\right)\left[\sum_{n=0}^{p-1}\left(\frac{n(n^2-1)}{p}\right)-\left(\frac{-1}{p}\right)\right]=\left(\frac{-1}{p}\right)S(1)-1.\tag{17}$$

Combining equations (11)-(17), by Lemma 2.3 and Lemma 2.4, we obtain

$$\begin{aligned}&|\{n|n\in S_+\text{ and }n+4k\in S_+\}|=\frac{p-2}{4}+\frac{1}{4}\left(\frac{-1}{p}\right)S(1)-\frac{1}{4}\\ =&\begin{cases}\frac{p-3+2(-1)^{\frac{a+1}{2}}a}{4}, & p\equiv 1\pmod{8},\\ \frac{p-3}{4}, & p\equiv 7\pmod{8}.\end{cases}\end{aligned}$$

This completes the proof of Theorem 1.4. □

Example 3.4. *If $p=31$, then*

$$S_+=\{1,3,4,5,8,9,14,15,17,18,20,21,26,27,30\}$$

and $8^2\equiv 2\pmod{31}$, $8\times 4\equiv 1\pmod{31}$. *Then*

$$\begin{aligned}&|\{n|n\in S_+\textit{ and }n+1\in S_+\}|\\ =&|\{3,4,8,14,17,20,26\}|\\ =&7=\frac{31-3}{4},\end{aligned}$$

this means that there are 7 pairs of consecutive integers that are the solutions of (1) *modulo 31.*

If $p=41$, then $p=5^2+4^2$,

$$S_+=\{2,4,5,7,8,9,11,15,17,19,20,25,26,28,30,34,36,37,38,40\}$$

and $(-17)^2\equiv 2\pmod{41}$, $-17\times 4\equiv 14\pmod{41}$. *Then*

$$\begin{aligned}&|\{n|n\in S_+\textit{ and }n+14\in S_+\}|\\ =&|\{5,11,20,26,34,36,38\}|\\ =&7=\frac{41-3-2\times 5}{4}.\end{aligned}$$

If $p = 71$, then

$$\begin{aligned}S_+ = \{&4,5,6,8,9,10,11,12,16,17,19,20,21,24,26,29,35,36,\\ &39,40,46,49,51,54,55,56,58,59,63,64,65,66,67,69,70\}\end{aligned}$$

and $(-12)^2 \equiv 2 \pmod{71}, -12 \times 4 \equiv 23 \pmod{71}$. *Then*

$$\begin{aligned}&|\{n|n \in S_+ \text{ and } n+23 \in S_+\}|\\ &= |\{6,12,16,17,26,35,36,40,46,54,56,58,59,64,65,67,69\}|\\ &= 17 = \frac{71-3}{4}.\end{aligned}$$

Proof. [Proof of Theorem 1.5]
Since $n \equiv a+b \equiv a^2+b^2 \pmod{p}$, by $b \equiv n-a \pmod{p}$, we have $2a^2 - 2na + n^2 - n \equiv 0 \pmod{p}$. If the discriminant $-4n^2+8n$ is a quadratic residue modulo p, then n is a solution modulo p of (3). Specifically, $n = 2$ is a solution of (3). Thus, by Lemma 2.1, (3) has

$$\begin{aligned}&\frac{1}{2}\sum_{\substack{n=1\\ n\neq 2}}^{p-1}\left[1+\left(\frac{-4n^2+8n}{p}\right)\right]+1\\ &= \frac{p}{2}+\frac{1}{2}\sum_{n=1}^{p}\left(\frac{-4n^2+8n}{p}\right)\\ &= \frac{p}{2}-\frac{1}{2}\left(\frac{-1}{p}\right)\end{aligned}$$

solutions. This completes the proof of Theorem 1.5. □

Remark 3.5. *We can use this method in Theorem 1.5 to solve both linear and quadratic congruence equations* $n \equiv xa + yb \equiv ua^2 + vab + wb^2 \pmod{p}$ *for given integers* x, y, u, v, w. *For example, both* $n \equiv a+b \equiv ab \pmod{p}$ *and* $n \equiv a-b \equiv ab \pmod{p}$ *have* $\frac{p-1}{2}$ *solutions, both* $n \equiv a+b \equiv a^2+b^2 \pmod{p}$ *and* $n \equiv a-b \equiv a^2+b^2 \pmod{p}$ *have* $\frac{p}{2} - \frac{1}{2}\left(\frac{-1}{p}\right)$ *solutions.*

Next, we consider congruences where addition and multiplication are homogeneous.

Proof. [Proof of Theorem 1.6]
It is obvious that

$$T = \{n \in Z_p^* \mid n \equiv (2a-b)^2 \equiv -3b^2 \pmod{p}\}.$$

We know that

$$\left(\frac{-3}{p}\right) = \begin{cases}1, & p \equiv 1 \pmod{6},\\ -1, & p \equiv 5 \pmod{6}.\end{cases} \tag{18}$$

When $p \equiv 5 \pmod{6}$, we have $|T| = 0$. When $p \equiv 1 \pmod{6}$, there exits an element c such that $c^2 \equiv -3 \pmod{p}$. Thus,

$$n \equiv (2a-b)^2 \equiv -3b^2 \equiv (bc)^2 \pmod{p},$$

$$2a - b \equiv \pm bc \pmod{p} \to a \equiv \frac{1 \pm c}{2}b \pmod{p} \to n \equiv \frac{1 \pm c}{2}b^2 \pmod{p}.$$

Since

$$\frac{1+c}{2}\frac{1-c}{2} \equiv \frac{1-c^2}{4} \equiv 1 \pmod{p},$$

both $\frac{1+c}{2}b^2$ and $\frac{1-c}{2}b^2$ are either quadratic residues or quadratic non-residues modulo p. Therefore when $p \equiv 1 \pmod{6}$, we have $|T| = \frac{p-1}{2}$.

By Lemma 2.2, there exits an element $c' \in Z_p^*$ of order 3 and c' is a quadratic residue modulo p, such that $(2c'+1)^2 \equiv -3 \pmod{p}$. We obtain

$$\frac{1-c}{2} \equiv \frac{1-2c'-1}{2} \equiv -c' \pmod{p}.$$

When $p \equiv 1 \pmod{4}$, $\frac{1-c}{2}b^2$ is a quadratic residue modulo p. When $p \equiv 3 \pmod{4}$, $\frac{1-c}{2}b^2$ is a quadratic non-residue modulo p.

By Chinese Remainder Theorem, this completes the proof of Theorem 1.6. □

Remark 3.6. *We can use this method in Theorem 1.6 to solve quadratic congruence equations* $n \equiv ua^2 + vb^2 \equiv wab \pmod{p}$ *for given integers* u, v, w.

References

[1] G. E. Andrews, *Number Theory*, Dover Publications, Inc. New York, 1994.
[2] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, Wiley-Interscience, New York, 1998.
[3] T. X. Cai, *A Modern Introduction to Classical Number Theory*, World Scientific, Singapore, 2021.
[4] T. X. Cai, Z. Y. Shen, P. Yang, *On the solution set of additive and multiplicative congruences modulo primes*, Filomat, **38** (2024), 621–635.
[5] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*,(2nd edition), Springer, New York, 1990, 64.
[6] M. G. Monzingo, *On the distribution of consecutive triples of quadratic residues and quadratic nonresidues and related topics*, Fibonacci Quarterly, **23** (1985), 133–138.
[7] L. Rudolf, N. Harald, *Finite fields, Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, 1997.
[8] Z. Y. Shen, T. X. Cai, *On the solution set of additive and multiplicative congruences modulo squares of primes*, Filomat, **39** (2025), 5999–6010.
[9] W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer, 2009.