Filomat 38:2 (2024), 621–635
https://doi.org/10.2298/FIL2402621C

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

Tianxin Cai[a], Zhongyan Shen[b,*], Peng Yang[c]

[a]*Department of Mathematics, Zhejiang University, Hangzhou 310027, P. R. China*
[b]*Department of Mathematics, Zhejiang International Studies University, Hangzhou 310023, P. R. China*
[c]*School of Science, University of Science and Technology Liaoning, Anshan 114051, P. R. China*

Abstract. Let p be an odd prime. In this paper, 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, where Z_p^* denote a reduced residue system modulo p. We also establish congruences about sum and product of the quadratic residues in S_+ or in S_- modulo p. Finally, we raise a problem on how to solve Hadamard's conjecture in the last section.

1. Introduction

In 1956, Mnich asked whether the diophantine system of equations

$$x_1 + x_2 + x_3 = x_1x_2x_3 = 1 \tag{1}$$

has any solution in $\mathbb{Q}$ (see [17]). Cassels[5] knew about this question from Mordell, and in 1960, he gave a negative answer by using the arithmetic of cubic fields. Two years later, Sansone and Cassels[17] posted an elementary proof of the non-solvability. In [10], Guy recorded a generalization of Mnich's question.

In 1996, by considering the positive rational solutions of

$$x_1 + x_2 + x_3 = x_1x_2x_3 = 6,$$

2020 *Mathematics Subject Classification*. Primary 11A07; Secondary 11A15, 11R11.
Keywords. Wilson's and Wolstenholme's theorems, additive and multiplicative, congruences, quadratic residues, Hadamard's conjecture.
Received: 03 May 2023; Accepted: 21 July 2023
Communicated by Paola Bonacini
The first and second authors were supported by National Natural Science Foundation of China, Project 12071421. The third author was supported by Foundation of Liaoning Educational Committee, Project 2019LNJC08.
* Corresponding author: Zhongyan Shen
Email addresses: txcai@zju.edu.cn (Tianxin Cai), huanchenszyan@163.com (Zhongyan Shen), yangpeng-zju@hotmail.com (Peng Yang)

Schinzel[18] proved that for every k, there are infinitely many primitive sets of k triples of positive integers with the same sum and the same product. Also, many authors have considered the diophantine equation in other number fields (see [2, 3, 6, 8, 9, 14, 20, 22, 23]). In general, the diophantine equation

$$x_1 + x_2 + \cdots + x_n = x_1 x_2 \cdots x_n \tag{2}$$

has infinitely many rational solutions. It is easy to see that equation (2) has only one positive integer solution $(2, 2)$ if $n = 2$. For $n = 3$, equation (2) has only one positive integer solution $(1, 2, 3)$ with $x_1 \le x_2 \le x_3$. And for any $n \ge 3$, equation (2) has at least one solution $(\underbrace{1, 1, \cdots, 1}_{n-2}, 2, n)$. Schinzel showed that there are infinitely many rational solutions of (2) with both sum and product equal to one [19]. Zhang and Cai[24] generalized Schinzel's result in [18]. They proved that for every k, there exist infinitely many primitive sets of k n-tuples of positive integers with the same sum and the same product.

Meanwhile, the well-known Wilson's and Wolstenholme's theorems describe the product and sum properties of residue classes. There are many analogs or generalizations, and it is interesting to find analogs on subsets of residue classes. Mirimanoff[13] and Lehmer[12] gave a congruence modulo p^2 on the sum of positive integers less than $(p-1)/2$. For any prime $p \equiv 3 \pmod 4$, Mordell[15] proved that

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{1}{2}[1+h(-p)]} \pmod p$$

if $p > 3$, where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Chowla[7] extended Mordell's result for $p \equiv 1 \pmod 4$. Lebesgue[1] found a congruence relation on the sum of quadratic residues and non-residues not exceeding $(p-1)/2$, while a similar result on the product was recently found by Wu and Wang[21]. Wu and Wang proved that if $p \equiv 5 \pmod 8$, then

$$\prod_{\substack{0<x<\frac{p}{2} \\ x\in R}} x \equiv (-1)^{1+r} \pmod p,$$

where R is the set of quadratic residues modulo p and r is the number of 4th power residues modulo p in the interval $(0, p/2)$. Let N be the set of quadratic non-residues modulo p, define

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

and

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

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

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

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, see [11] and [4]. In this paper, we consider the sum and product properties of solutions of the following congruent equations

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

and

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

with $n \in Z_p^*$. Equations (3) and (4) have their own interesting properties. For example, it is not difficult to prove that $n = 1$ is a solution of (3) if and only if prime p can be expressed as $x^2 + 3y^2$, while $n = 1$ is a solution of (4) if and only if prime p can be expressed as $5x^2 - y^2$; $n = 2$ is a solution of (3) if and only if odd prime p can be expressed as $x^2 + y^2$, while $n = 2$ is a solution of (4) if and only if prime p can be expressed as $3x^2 - y^2$ or $x^2 - 3y^2$.

In this article, we first give some properties of the solutions of equations (3) and (4). Then, 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. Moreover, 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. Auxiliary Results

Lemma 2.1 ([16]). *For any integer k and prime p,*

$$\sum_{x=1}^{p-1} x^k \equiv \begin{cases} 0 \pmod p, & p-1 \nmid k, \\ -1 \pmod p, & p-1 \mid k. \end{cases}$$

Lemma 2.2 ([15]). *For any odd prime p, we have*

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

Lemma 2.3. *For any odd prime $p > 3$ and integer l, we have*

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

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

Proof. It is easy to check when $p = 3$ or $\frac{p-1}{2} \mid l$. For $p > 3$ and $\frac{p-1}{2} \nmid l$, we have

$$\sum_{a\in R} a^l \equiv \sum_{i=1}^{\frac{p-1}{2}} i^{2l} \equiv \frac{1}{2}\sum_{i=1}^{p-1} i^{2l} \equiv 0 \pmod p$$

by Lemma 2.1. □

Lemma 2.4. *For any odd prime p, we have*

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

$$\sum_{a\in R\setminus\{1\}} \frac{1}{a-1} \equiv \frac{3}{4} \pmod p.$$

Proof. It is well-known that $\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$ is the set of quadratic residues modulo p. Therefore, by Lemma 2.2,

$$\begin{aligned}\prod_{a\in R\setminus\{1\}}(a-1) &\equiv \prod_{a=2}^{\frac{p-1}{2}}\left(a^2-1\right) \equiv \prod_{a=2}^{\frac{p-1}{2}}(a-1)(a+1)\\ &\equiv \prod_{i=1}^{\frac{p-3}{2}} i \prod_{j=3}^{\frac{p+1}{2}} j \equiv \frac{\frac{p+1}{2}\prod_{i=1}^{\frac{p-1}{2}} i \prod_{j=1}^{\frac{p-1}{2}} j}{p-1}\\ &\equiv \frac{1}{2}(-1)^{\frac{p-1}{2}} \equiv \frac{1}{2}\left(\frac{-1}{p}\right) \pmod p\end{aligned}$$

and

$$\begin{aligned}\sum_{a\in R\setminus\{1\}}\frac{1}{a-1} &\equiv \sum_{i=2}^{\frac{p-1}{2}}\frac{1}{i^2-1} = \frac{1}{2}\left(\sum_{i=2}^{\frac{p-1}{2}}\frac{1}{i-1} - \sum_{i=2}^{\frac{p-1}{2}}\frac{1}{i+1}\right)\\ &= \frac{1}{2}\left(1+\frac{1}{2}-\frac{2}{p-1}-\frac{2}{p+1}\right) \equiv \frac{3}{4} \pmod p.\end{aligned}$$

□

3. On the solutions of equation (3)

For the rest of this article, we say that $n \pmod p$ 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 be an odd prime. Then*
1) For any $p > 3$, $n \equiv 4$ is a solution of (3), *and* (3) *has $(p-1)/2$ solutions.*
2) For each solution n, there is only one (n, a, b) that satisfying (3) *apart from the order of* (a, b).

Proof. 1) There is only one positive solution of the equation $a + b = ab = n$. That is $n = 2 \times 2 = 4$. For any $0 < a \neq 1 \leq p-1$, congruence

$$a + x - ax \equiv 0 \pmod p \tag{5}$$

has exactly one solution $x \equiv a/(a-1)$. If $a = 1$, congruence (5) has no solution. Only when $a = 2$, we have $x \equiv a$. Hence, there are $\frac{p-3}{2} + 1 = \frac{p-1}{2}$ solutions $n \equiv ab$ of (3) by symmetry.

2) Assume that both (n, a_1, b_1), (n, a_2, b_2) satisfy (3). Then, we have

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

or

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

which means $a_1 \equiv a_2 \pmod p$ or $a_1 \equiv \frac{a_2}{a_2-1} \pmod p$. □

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

$$\prod_{n\in S_+} n \equiv -2 \pmod p.$$

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

$$\prod_{n\in S_+} n \equiv \prod_{\substack{ab\in S_+\\ a\le b}} ab \equiv 2\prod_{j=2}^{p-1} j \equiv -2 \pmod p$$

by Wilson's theorem. □

Theorem 3.3. *Let p be an odd prime and arbitrary integer $k \equiv s \pmod{p-1}$ with $0 \le s < p-1$. Then the power sum of the solutions of* (3)

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

Proof. For each $0 < a \neq 1 \le p-1$, we have

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

and n can be written as ab or ba with $a \not\equiv b$ except when $n = 4 = 2\times 2$. Hence, for $p > 3$ and $k \equiv s \pmod{p-1}$, by Fermat's little theorem, we have

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

If $s = 0$, then $\sum_{n\in S_+} n^k \equiv \sum_{n\in S_+} n^s \equiv \frac{p-1}{2}$. If $0 < s < p-1$, then

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

by Lemma 2.1. □

Remark 3.4. *With the help of Theorem 3.3 and Fermat's little theorem, we have*

$$\sum_{n\in S_+} \frac{1}{n} \equiv \frac{1}{8} \pmod p \ (p > 3)$$

and

$$\sum_{n\in S_+}\frac{1}{n^2}\equiv\frac{1}{32}\pmod p\ (p>5).$$

Theorem 3.5. *Let p be an odd prime, R be the set of quadratic residues modulo p and N be the set of quadratic non-residues modulo p. Then*

$$|S_+\cap R|=\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right)$$

and

$$|S_+\cap N|=\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right).$$

Proof. Since $n\in S_+$, we have $n\equiv a+b\equiv ab\pmod p$, i.e., $(a-1)(b-1)\equiv 1\pmod p$. It is obvious that $a-1\equiv b-1\equiv 1\pmod p$, i.e., $a\equiv b\equiv 2\pmod p$, $n\equiv ab\equiv 4\pmod p$ and $n\in S_+$. If $a-1\equiv b-1\equiv -1\pmod p$, i.e., $a\equiv b\equiv 0\pmod p$, $n\equiv ab\equiv 0\pmod p$, but $n\notin S_+$.

If $n\in S_+\cap R$, then $\left(\frac{n}{p}\right)=1$. Since $n\equiv ab\equiv\frac{a^2}{a-1}\pmod p$, we have $\left(\frac{a-1}{p}\right)=1$, likewise, $\left(\frac{b-1}{p}\right)=1$. $|S_+\cap R|$ is the number of pairs $(a-1,b-1)\pmod p$ such that $(a-1)(b-1)\equiv 1\pmod p$ and $\left(\frac{a-1}{p}\right)=\left(\frac{b-1}{p}\right)=1$. Except $a-1\equiv b-1\equiv\pm 1\pmod p$, the remaining residues modulo p from pairs $a-1,b-1$, where $a-1\not\equiv b-1\pmod p$ such that $(a-1)(b-1)\equiv 1\pmod p$.

If $p\equiv 1\pmod 4$, then ± 1 are quadratic residues modulo p. Thus

$$|S_+\cap R|=\frac{\frac{p-1}{2}-2}{2}+1=\frac{p-1}{4}=\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right).$$

If $p\equiv 3\pmod 4$, then 1 is a quadratic residue modulo p, and -1 is a quadratic non-residue modulo p. Thus

$$|S_+\cap R|=\frac{\frac{p-1}{2}-1}{2}+1=\frac{p+1}{4}=\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right)$$

and

$$|S_+\cap N|=|S_+|-|S_+\cap R|=\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right).$$

□

Theorem 3.6. *For prime $p>3$, and arbitrary integer $k\equiv s\pmod{p-1}$ with $0\le s<p-1$, the power sum of quadratic residues in solutions of* (3) *satisfies*

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

Proof. If $s = 0$, the result follows from Theorem 3.5. For each $0 < a \neq 1 \leq p-1$, we have

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

and n can be written as ab or ba with $a \not\equiv b \pmod{p}$ except when $n = 4 = 2 \times 2$. Hence, for $p > 3$ and $0 < s < p-1$, we have

$$\begin{aligned}\sum_{n\in S_+\cap R} n^k \equiv \sum_{n\in S_+\cap R} n^s &\equiv \frac{1}{2}\left(\sum_{a-1\in R} \frac{a^{2s}}{(a-1)^s} - 2^{2s}\right) + 2^{2s} \\ &\equiv \frac{1}{2}\sum_{a-1\in R} \frac{(a-1+1)^{2s}}{(a-1)^s} + 2^{2s-1} \\ &\equiv \frac{1}{2}\sum_{a-1\in R}\sum_{t=0}^{2s}\binom{2s}{t}(a-1)^{t-s} + 2^{2s-1} \\ &\equiv \frac{1}{2}\sum_{t=0}^{2s}\binom{2s}{t}\sum_{a-1\in R}(a-1)^{t-s} + 2^{2s-1} \pmod{p}.\end{aligned}$$

By Lemma 2.3, if $0 < s < \frac{p-1}{2}$, then

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

If $\frac{p-1}{2} \leq s < p-1$, except $t - s = 0, \pm\frac{p-1}{2}$, other terms in the first sum are congruent to 0 modulo p by Lemma 2.3, thus

$$\begin{aligned}\sum_{n\in S_+\cap R} n^k &\equiv 2^{2s-1} + \frac{p-1}{4}\left(\binom{2s}{s} + \binom{2s}{s-\frac{p-1}{2}} + \binom{2s}{s+\frac{p-1}{2}}\right) \\ &\equiv 2^{2s-1} - \frac{1}{4}\left(\binom{2s}{s} + 2\binom{2s}{s-\frac{p-1}{2}}\right) \pmod{p}.\end{aligned}$$

□

In particular, let $k = -1, -2$ in Theorem 3.6, we have

$$\sum_{n\in S_+\cap R} \frac{1}{n} \equiv \frac{1}{8} - \frac{1}{32}\left(\frac{-1}{p}\right) \pmod{p}$$

and

$$\sum_{n\in S_+\cap R} \frac{1}{n^2} \equiv \frac{1}{32} - \frac{3}{2^9}\left(\frac{-1}{p}\right) \pmod{p}\ (p > 5).$$

By Theorem 3.3, Theorem 3.6 and

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

we obtain the following corollary.

Corollary 3.7. *Let $p > 3$ be a prime and arbitrary integer $k \equiv s \pmod{p-1}$ with $0 \le s < p-1$. Then*

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

In particular, let $p > 5$ be a prime and $k = \pm 1, \pm 2$ in Corollary 3.7, we obtain

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

$$\sum_{n\in S_+}\left(\frac{n}{p}\right)n^2 \equiv 8 \pmod{p},$$

$$\sum_{n\in S_+}\left(\frac{n}{p}\right)\frac{1}{n} \equiv \frac{1}{8}-\frac{1}{16}\left(\frac{-1}{p}\right) \pmod{p}$$

and

$$\sum_{n\in S_+}\left(\frac{n}{p}\right)\frac{1}{n^2} \equiv \frac{1}{32}-\frac{3}{256}\left(\frac{-1}{p}\right) \pmod{p}.$$

Theorem 3.8. *For prime $p > 3$, the product of quadratic residues in solutions of (3) satisfies*

$$\prod_{n\in S_+\cap R} n \equiv \frac{3}{2}-\frac{5}{2}\left(\frac{-1}{p}\right) \pmod{p}.$$

Proof. By the proof of Theorem 3.5, we have

$$\prod_{n\in S_+\cap R} n \equiv \frac{1}{4}\prod_{\substack{ab\in S_+\cap R\\ ab\not\equiv 4 \pmod{p}}} ab \equiv \frac{1}{4}\prod_{\substack{a-1\in R\\ a-1\not\equiv \pm 1 \pmod{p}}} a. \tag{6}$$

If $p \equiv 1 \pmod 4$, then ± 1 are quadratic residues modulo p, and if $a-1$ ranges over $R \setminus \{-1\}$, then also $1-a$ ranges over $R \setminus \{1\}$. Thus

$$\begin{aligned}\prod_{\substack{a-1\in R\\ a-1\not\equiv \pm 1 \pmod{p}}} a &\equiv \prod_{\substack{a-1\in R\\ a-1\not\equiv \pm 1 \pmod{p}}} [(a-1)+1]\\ &\equiv \frac{1}{2}\prod_{a-1\in R\setminus\{-1\}} [(a-1)+1]\\ &\equiv \frac{1}{2}\prod_{a-1\in R\setminus\{1\}} [-(a-1)+1]\\ &\equiv \frac{(-1)^{\frac{p-3}{2}}}{2}\prod_{a-1\in R\setminus\{1\}} [(a-1)-1] \pmod{p}.\end{aligned} \tag{7}$$

By Lemma 2.4 and combining (6) and (7), we have

$$\prod_{n\in S_+\cap R} n \equiv 4\cdot\frac{(-1)^{\frac{p-3}{2}}}{2}\cdot\frac{1}{2} \equiv -1 \equiv \frac{3}{2}-\frac{5}{2}\left(\frac{-1}{p}\right) \pmod{p}.$$

If $p \equiv 3 \pmod 4$, then 1 is a quadratic residue modulo p and -1 is a quadratic non-residue modulo p. If $a-1$ ranges over R, then also $1-a$ ranges over N, where N is the set of quadratic non-residues modulo p. Thus

$$\begin{aligned}\prod_{\substack{a-1\in R\\ a-1\not\equiv\pm1 \pmod p}} a &\equiv \prod_{a-1\in R\setminus\{1\}} [(a-1)+1]\\ &\equiv \frac{1}{2}\prod_{a-1\in R}[(a-1)+1]\\ &\equiv \frac{1}{2}\prod_{a-1\in N}[-(a-1)+1]\\ &\equiv \frac{(-1)^{\frac{p-1}{2}}}{2}\prod_{a-1\in N}[(a-1)-1] \pmod p. \end{aligned} \tag{8}$$

By Lemma 2.4 and Wilson's Theorem, we have

$$\prod_{a-1\in N}[(a-1)-1] \equiv \frac{\prod_{a-1=2}^{p-1}[(a-1)-1]}{\prod_{a-1\in R\setminus\{1\}}[(a-1)-1]} \equiv \frac{(p-2)!}{\frac{1}{2}\left(\frac{-1}{p}\right)} \equiv -2 \pmod p. \tag{9}$$

Combining (6),(8) and (9), we have

$$\prod_{n\in S_+\cap R} n \equiv 4\cdot\frac{(-1)^{\frac{p-1}{2}}}{2}\cdot(-2) \equiv 4 \equiv \frac{3}{2}-\frac{5}{2}\left(\frac{-1}{p}\right) \pmod p.$$

□

4. On the solutions of equation (4)

Now, we discuss the solutions of equation (4).

Theorem 4.1. *Let p be an odd prime. Then*
1) For any $p>3$, (4) has $(p-1)/2$ solutions.
2) For all n, the solutions of (4) come in pairs of the form $(n,a,b),(n,p-b,p-a)$ with $(n,a,b)\neq(n,p-a,p-b)$ unless $n\equiv 2(p-2) \pmod p$.

Proof. 1) For any $0<a<p-1$, equation

$$a-x-ax\equiv 0 \pmod p \tag{10}$$

has unique solution

$$x\equiv\frac{a}{a+1} \pmod p.$$

If $a=p-1$, congruence (10) has no solution. If (n,a,b) satisfies equation (4), then $(n,p-b,p-a)$ satisfies equation (4) too. That is because

$$p-b-(p-a)-(p-b)(p-a)\equiv a-b-ab \pmod p.$$

If $a=p-b$, then

$$a-(p-a)-a(p-a)\equiv a^2+2a\equiv 0 \pmod p.$$

Since $p \nmid a$, we have $p = a + 2$ and $(a, b) = (p - 2, 2)$. Thus, $n = ab$ run over the solutions twice except $2(p-2) \pmod p$ when a run over the residue class modulo p. Therefore, equation (4) has $\frac{p-3}{2} + 1 = \frac{p-1}{2}$ solutions.
2) If both $(n, a_1, b_1), (n, a_2, b_2)$ satisfy congruence (4), then

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

i.e.

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

Therefore, we have

$$a_1 \equiv a_2 \pmod p$$

or

$$a_1 \equiv -\frac{a_2}{a_2+1} \equiv p - b_2 \pmod p.$$

□

Theorem 4.2. *Let p be an odd prime, then the product of solutions of* (4)

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

Proof. For $2 \le a \le p-1$, equation

$$x - a - xa \equiv 0 \pmod p$$

has unique solution

$$x \equiv -\frac{a}{a-1} \pmod p$$

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

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

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

From the relation between $(a, \frac{a}{a-1}), (-\frac{a}{a-1}, a)$ described in the proof of Theorem 4.2, it is easy to conclude the following results:

Theorem 4.3. *Let p be an odd prime and arbitrary integer* $k \equiv s \pmod{p-1}$ *with* $0 \le s < p-1$. *Then the power sum of the solutions in* (4) *satisfies*

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

In particular, when $k = -1$ or $k = -2$, by Theorem 4.3, we obtain

$$\sum_{n\in S_-} \frac{1}{n} \equiv -\frac{1}{8} \pmod p \ (p > 3)$$

and

$$\sum_{n\in S_-}\frac{1}{n^2}\equiv\frac{1}{32}\pmod p\ (p>5).$$

Theorem 4.4. *Let p be an odd prime. Then*

$$|S_-\cap R|=\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right)$$

and

$$|S_-\cap N|=\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right).$$

Proof. Since $n\in S_-$, we have $n\equiv a-b\equiv ab\pmod p$, i.e., $(a+1)(1-b)\equiv 1\pmod p$. It is obviously that $a+1\equiv 1-b\equiv 1\pmod p$, i.e., $a\equiv b\equiv 0\pmod p$, $n\equiv ab\equiv 0\pmod p$ and $n\notin S_-$. But $a+1\equiv 1-b\equiv -1\pmod p$, i.e., $a\equiv -b\equiv -2\pmod p$, $n\equiv ab\equiv -4\pmod p$ and $n\in S_-$.
If $n\in S_-\cap R$, then $\left(\frac{n}{p}\right)=1$. Since $n\equiv ab\equiv\frac{b^2}{1-b}\pmod p$, we have $\left(\frac{1-b}{p}\right)=1$, likewise, $\left(\frac{a+1}{p}\right)=1$. $|S_-\cap R|$ is the number of pairs $(a+1,1-b)\pmod p$ such that $(a+1)(1-b)\equiv 1\pmod p$ and $\left(\frac{a+1}{p}\right)=\left(\frac{1-b}{p}\right)=1$. Except $a+1\equiv 1-b\equiv\pm1\pmod p$, the remaining residues modulo p from pairs $a+1,1-b$, where $a+1\not\equiv 1-b\pmod p$ such that $(a+1)(1-b)\equiv 1\pmod p$.

If $p\equiv 1\pmod 4$, then ±1 are quadratic residues modulo p. Thus

$$|S_-\cap R|=\frac{\frac{p-1}{2}-2}{2}+1=\frac{p-1}{4}=\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right).$$

If $p\equiv 3\pmod 4$, then 1 is a quadratic residue modulo p, and -1 is a quadratic non-residue modulo p. Thus

$$|S_-\cap R|=\frac{\frac{p-1}{2}-1}{2}=\frac{p-3}{4}=\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right)$$

and

$$|S_-\cap N|=|S_-|-|S_-\cap R|=\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right).$$

□

Theorem 4.5. *For prime $p>3$, and arbitrary integer $k\equiv s\pmod{p-1}$ with $0\le s<p-1$. Then the sum of quadratic residues in solutions of* (4) *satisfies*

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

Proof. If $s=0$, this is just the result of Theorem 4.4. For each $0<b\neq 1\leq p-1$, we have

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

and n can be written as ab or ba with $a\not\equiv -b \pmod p$ except when $n=2(p-2)$. If $p\equiv 1 \pmod 4$, we have $n=2(p-2)\in S_-\cap R$. If $p\equiv 3 \pmod 4$, we have $n=2(p-2)\notin S_-\cap R$. Hence, for $p\equiv 1 \pmod 4$ and $0<s<p-1$, we have

$$\begin{aligned}\sum_{n\in S_-\cap R} n^k \equiv \sum_{n\in S_-\cap R} n^s &\equiv \frac{1}{2}\left(\sum_{1-b\in R}\frac{b^{2s}}{(1-b)^s}-(-4)^s\right)+(-4)^s\\ &\equiv \frac{1}{2}\sum_{1-b\in R}\frac{(b)^{2s}}{(1-b)^s}+(-1)^s 2^{2s-1} \pmod p.\end{aligned}$$

For $p\equiv 3 \pmod 4$ and $0<s<p-1$, we have

$$\sum_{n\in S_-\cap R} n^k \equiv \frac{1}{2}\sum_{1-b\in R}\frac{b^{2s}}{(1-b)^s} \pmod p.$$

Hence, for $p>3$ and $0<s<p-1$, we have

$$\begin{aligned}\sum_{n\in S_-\cap R} n^k &\equiv \frac{1}{2}\left(\sum_{1-b\in R}\frac{b^{2s}}{(1-b)^s}\right)+(-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}\\ &\equiv \frac{1}{2}\sum_{1-b\in R}\frac{(1-b-1)^{2s}}{(1-b)^s}+(-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}\\ &\equiv \frac{1}{2}\sum_{1-b\in R}\sum_{t=0}^{2s}(-1)^t\binom{2s}{t}(1-b)^{t-s}+(-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}\\ &\equiv \frac{1}{2}\sum_{t=0}^{2s}(-1)^t\binom{2s}{t}\sum_{1-b\in R}(1-b)^{t-s}+(-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2} \pmod p.\end{aligned}$$

By Lemma 2.3, if $0<s<\frac{p-1}{2}$, then

$$\begin{aligned}\sum_{n\in S_-\cap R} n^k &\equiv (-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}+\frac{(-1)^s}{2}\binom{2s}{s}\frac{p-1}{2}\\ &\equiv (-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}-\frac{(-1)^s}{4}\binom{2s}{s} \pmod p.\end{aligned}$$

If $\frac{p-1}{2}\leq s<p-1$, except $t-s=0,\pm\frac{p-1}{2}$, other terms in the first sum are congruent to 0 modulo p by Lemma 2.3, thus

$$\begin{aligned}\sum_{n\in S_-\cap R} n^k &\equiv (-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}+\frac{p-1}{4}\left((-1)^s\binom{2s}{s}+2(-1)^{s-\frac{p-1}{2}}\binom{2s}{s-\frac{p-1}{2}}\right)\\ &\equiv (-1)^s\left(1+\left(\frac{-1}{p}\right)\right)2^{2s-2}-\frac{(-1)^s}{4}\left(\binom{2s}{s}+2\left(\frac{-1}{p}\right)\binom{2s}{s-\frac{p-1}{2}}\right) \pmod p.\end{aligned}$$

□

Remark 4.6. *Let $k = -1, -2$ in Theorem 4.5, we have*

$$\sum_{n\in S_-\cap R} \frac{1}{n} \equiv -\frac{1}{16}\left(\frac{-1}{p}\right) - \frac{1}{32} \pmod p$$

and

$$\sum_{n\in S_-\cap R} \frac{1}{n^2} \equiv \frac{1}{64}\left(\frac{-1}{p}\right) + \frac{5}{2^9} \pmod p \; (p > 5).$$

By Theorem 4.3, Theorem 4.5 and

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

we obtain the following corollary.

Corollary 4.7. *Let $p > 3$ be a prime and integer $k \equiv s \pmod{p-1}$ with $0 \le s < p-1$. Then*

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

In particular, let $p > 5$ be a prime and $k = \pm 1, \pm 2$ in Corollary 4.7 , then

$$\sum_{n\in S_-}\left(\frac{n}{p}\right)n \equiv -2\left(\frac{-1}{p}\right) \pmod p,$$

$$\sum_{n\in S_-}\left(\frac{n}{p}\right)n^2 \equiv 8\left(\frac{-1}{p}\right) \pmod p,$$

$$\sum_{n\in S_-}\left(\frac{n}{p}\right)\frac{1}{n} \equiv -\frac{1}{8}\left(\frac{-1}{p}\right) \pmod p$$

and

$$\sum_{n\in S_-}\left(\frac{n}{p}\right)\frac{1}{n^2} \equiv \frac{1}{32}\left(\frac{-1}{p}\right) \pmod p.$$

Theorem 4.8. *For prime $p > 3$, the product of quadratic residues in solutions of* (4) *satisfies*

$$\prod_{n\in S_-\cap R} n = -\frac{1}{4}\left(\frac{2}{p}\right) - \frac{3}{4}\left(\frac{-2}{p}\right) \pmod p.$$

Proof. If $p \equiv 1 \pmod 4$, then ± 1 are quadratic residues modulo p. By the proof of Theorem 4.4 and Lemma 2.4, we have

$$\begin{aligned}
\prod_{n \in S_- \cap R} n &\equiv -4 \prod_{\substack{ab \in S_- \cap R \\ ab \not\equiv -4 \pmod p}} ab \\
&\equiv (-1)^{\frac{\frac{p-1}{2}}{2}} 4 \prod_{1-b \in R \setminus \{1,-1\}} [(1-b)-1] \\
&\equiv (-1)^{\frac{p-5}{4}} 2 \prod_{1-b \in R \setminus \{1\}} [(1-b)-1] \\
&\equiv (-1)^{\frac{p-5}{4}} 2 \cdot \frac{1}{2} \left(\frac{-1}{p}\right) \\
&\equiv -\frac{1}{4}\left(\frac{2}{p}\right) - \frac{3}{4}\left(\frac{-2}{p}\right) \pmod p.
\end{aligned}$$

If $p \equiv 3 \pmod 4$, then 1 is a quadratic residue modulo p. By the proof of Theorem 4.4 and Lemma 2.4, we have

$$\begin{aligned}
\prod_{n \in S_- \cap R} n &\equiv \prod_{ab \in S_- \cap R} ab \\
&\equiv (-1)^{\frac{\frac{p-1}{2}-1}{2}} \prod_{1-b \in R \setminus \{1\}} [(1-b)-1] \\
&\equiv (-1)^{\frac{p-3}{4}} \frac{1}{2} \left(\frac{-1}{p}\right) \\
&\equiv -\frac{1}{4}\left(\frac{2}{p}\right) - \frac{3}{4}\left(\frac{-2}{p}\right) \pmod p.
\end{aligned}$$

□

5. Problem

In this section, we raise a problem for further research. Let A be a real square matrix of order n such that all its entries $a_{ij} = \pm 1$ and the rows (columns) of A are all orthogonal to each other, then we call A an Hadamard matrix (see [4]). There is a famous conjecture in combinatorics.

Hadamard's Conjecture *For any positive integer n being a multiple of 4, there exits an Hadamard matrix of order n.*

In 1933, Raymond Paley found a beautiful and efficient way to construct Hadamard matrix by using the theory of quadratic residues.

Theorem(Paely) *Let p be a prime of the form* $4k+3$, *and let R and N denote the set of quadratic residues and nonresidues modulo p, respectively. Define a square matrix B of order p, with its entries*

$$b_{ij} = \begin{cases} 1, j-i \in R, \\ -1, j-i \in N \text{ or } i = j. \end{cases}$$

Let A be a square matrix of order $p+1$ *such that all entries in its first row and column are* 1, *and let its lower right submatrix of order p be B. Then A is an Hadamard matrix of order* $p+1$.

Similarly, Paley constructed Hadamard matrices of order $2(q+1)$, where q is a prime of the form $4k+1$. We can say that Paley made the biggest contribution to the theory of the existence of Hadamard matrices. So far, there are 13 multiples of 4 less than or equal to 2000 for which no Hadamard matrix of that order is known. They are: $668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948$ and 1964.

Since for any odd prime p, both (3) and (4) have exactly $(p-1)/2$ solutions, i.e., both set S_+ and set S_- have the same number of elements as the quadratic residues, we would raise the following problem:

Problem 5.1. *How to construct Hadamard matrics and solve Hadamard's conjecture by using the properties of sets S_+ or S_-.*

Acknowledgments

The authors wish to thank the referee for constructive suggestions and careful reading of the manuscript.

References

[1] C. Aebi, G.Cairns, *Sums of Quadratic Residues and Nonresidues*, Am. Math. Mon., **124** (2017).
[2] A. Bremner, *The equation $xyz = x + y + z = 1$ in integers of a cubic field*, Manuscripta Math., **65** (1989), 479–487.
[3] A. Bremner, The equation $xyz = x + y + z = 1$ in integers of a quartic field. Acta Arith., **57** (1991), 375–385.
[4] T. X. Cai, *A Modern Introduction to Classical Number Theory*, World Scientific, Singapore, 2021.
[5] J. Cassels, *On a diophantine equation*, Acta Arith., **6** (1960), 47–52.
[6] K. Chakraborty, M. V. Kulkarni, *Solutions of cubic equations in quadratic fields*, Acta Arith., **89** (1999), 37–43.
[7] S. Chowla, *On the Class Number of Real Quadratic Fields*, Proc. Natl. Acad. Sci., **47** (1961), 878.
[8] H. Edgar, J. Gordon,L. C. Zhang, *On unit solutions of the equation $xyz = x + y + z$ in totally imaginary quartic fields*, J. Number Theory, **40** (1992), 255–263.
[9] H. Grundman, L. Hall-Seelig, *Solutions to $xyz = 1$ and $x + y + z = k$ in algebraic integers of small degree I*, Acta Arith., **4** (2014), 381–392.
[10] R. K. Guy, *Unsolved Problems in Number Theory*,(3rd edition), Springer, New York, 1994, 172.
[11] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*,(2nd edition), Springer, New York, 1990, 64.
[12] E. Lehmer, *On Congruences Involving Bernoulli Numbers and the Quotients of Fermat and Wilson*, Ann. Math., **39** (1938).
[13] D. Mirimanoff, *Sur les nombres de Bernoulli*, L'Enseignement Math., **36** (1937), 228–235.
[14] R. Mollin, C. Small, K. Varadarajan, P. Walsh, *On unit solutions of the equation $xyz = x + y + z$ in the ring of integers of a quadratic field*, Acta Arith., **48** (1987), 341–345.
[15] L. J. Mordell, *The Congruence $(p-1/2)! \equiv \pm 1 (\bmod p)$*, Am. Math. Mon., **68** (1961), 145–146.
[16] M. R. Murty, *Introduction to p-adic Analytic Number Theory*, Am. Math. Soc., **27** (2009).
[17] G. Sansone, J. Cassels, *Sur le probleme de M. Werner Mnich*, Acta Arith., **7** (1962), 187–190.
[18] A. Schinzel, *Triples of positive integers with the same sum and the same product*, Serdica Math. J., **22** (1996), 587–588.
[19] W. Sierpinski, *Ungeleste Probleme Nr. 14*, Elemente der Mathematik, **11** (1956), 109–110.
[20] C. Small, *On the Equation $xyz = x + y + z = 1$*, Am. Math. Mon., **89** (1982), 736–749.
[21] H. L. Wu, L. Y. Wang, *Products of quadratic residues and related identities*, Colloq. Math., **167** (2022), 197–206.
[22] L. C. Zhang, J. Gordon, *On unit solutions of the equation $xyz = x + y + z$ in a number field with unit group of rank 1*, Acta Arith., **57** (1991), 155–158.
[23] L. C. Zhang, J. Gordon, *On Unit Solutions of the Equation $xyz = x + y + z$ in Not Totally Real Cubic Fields*, Can. Math. Bull., **34** (1991), 141–144.
[24] Y. Zhang,T. X. Cai, *N-tuples of positive integers with the same sum and the same product*, Math. Comput., **82** (2013), 617–623.