Research Article

Wang Xiao* and Aihua Li

Counting certain quadratic partitions of zero modulo a prime number

<https://doi.org/10.1515/math-2021-0032>

received September 15, 2020; accepted February 4, 2021

Abstract: Consider an odd prime number $p \equiv 2 \pmod{3}$. In this paper, the number of certain type of partitions of zero in $\mathbb{Z}/p\mathbb{Z}$ is calculated using a combination of elementary combinatorics and number theory. The focus is on the three-part partitions of 0 in $\mathbb{Z}/p\mathbb{Z}$ with all three parts chosen from the set of non-zero quadratic residues mod p . Such partitions are divided into two types. Those with exactly two of the three parts identical are classified as type I. The type II partitions are those with all three parts being distinct. The number of partitions of each type is given. The problem of counting such partitions is well related to that of counting the number of non-trivial solutions to the Diophantine equation $x^2 + y^2 + z^2 = 0$ in the ring $\mathbb{Z}/p\mathbb{Z}$. Correspondingly, solutions to this equation are also classified as type I or type II. We give the number of solutions to the equation corresponding to each type.

Keywords: partition of a number, Dirichlet character sum, Diophantine equation, solution number

MSC 2020: 11D45, 11P83, 11L10

1 Introduction

The study of Diophantine equations is one of the oldest branches of number theory and the most famous Diophantine equation is the Fermat equation: $x^n + y^n = z^n$. Conjectured by Pierre de Fermat in 1637, Fermat's last conjecture states that for any integer $n > 2$, no three positive integers can satisfy the Fermat's equation. For more than 350 years, many mathematicians have devoted their work on solving this fascinating conjecture and related Diophantine equations. It was until 1995, the conjecture became Fermat's last theorem, proved by Andrew Wiles [1].

Research has been done in the investigation of Diophantine equations "locally," in particular, over finite fields. For example, in [2], solving a Diophantine equation modulo every prime number was studied using commutative algebra techniques. Recently, many scholars have studied Diophantine equations modulo prime numbers and obtained a series of interesting results (see [3–7]).

Consider any odd prime number p . In this paper, we focus on the following three equations concerning solutions in the ring $\mathbb{Z}/p\mathbb{Z}$:

$$(1) x^2 + y^2 + z^2 = 0, \quad (2) x^3 + y^3 + z^3 = 0, \quad (3) x^6 + y^6 + z^6 = 0.$$

It is known that if $p \equiv 2 \pmod{3}$, every element $a \in \mathbb{Z}/p\mathbb{Z}$ is a perfect cube in $\mathbb{Z}/p\mathbb{Z}$. Precisely, if $p = 3m + 2$, where $m \in \mathbb{Z}$, $a = (a^{2m+1})^3$. Also, $x \mapsto x^3$ is a one-to-one and onto correspondence on $\mathbb{Z}/p\mathbb{Z}$. Thus, in the case of $p \equiv 2 \pmod{3}$, $\forall a \in \mathbb{Z}/p\mathbb{Z}$, a is a perfect square if and only if a is a perfect sixth power. Furthermore, the number of solutions to equation (1) is the same as that of equation (3). We focus on the solution triples (x, y, z)

* **Corresponding author: Wang Xiao**, School of Science, Chang'an University, Xi'an, Shaanxi 710064, P. R. China, e-mail: wangxiao_0606@chd.edu.cn

Aihua Li: Department of Mathematics, Montclair State University, New Jersey, USA, e-mail: lia@montclair.edu

with $xyz \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ and call such a solution a non-trivial solution. A non-trivial solution triple (x, y, z) is called a quadratic solution if x, y, z are all non-zero perfect squares in $\mathbb{Z}/p\mathbb{Z}$ (or non-zero quadratic residues mod p). Obviously, a quadratic solution to equation (2) gives a non-trivial solution to equation (3) and *vice versa*. Thus, the number of non-trivial solutions to equation (1) is the same as the number of quadratic solutions to equation (2). In [8–10], some character sums involving Dirichlet characters were used to determine the number of solutions to certain Diophantine equations modulo a prime number. In this paper, we apply formulas developed in [8] to determine the number of non-trivial solutions to equation (1) or that of quadratic solutions to equation (2), modulo any odd prime $p \equiv 2 \pmod{3}$.

Another way to describe a non-trivial solution (x, y, z) to equation (1) is to view it as a three-part partition of 0 modulo p . The theory of partition is another interesting branch of number theory. The concept of partitions of positive integers was given by Leonard Euler in the 18th century. Since then many prominent mathematicians, including Gauss, Jacobi, Schur, McMahon, Andrews, Ramanujan, and Hardy, have made great contributions to the study of partitions (see [11–13]). Applications of partitions of positive integers or sets can be found in many other areas such as combinatorics, computer science, and genetics. A partition of a positive integer n is a combination (unordered, with repetitions allowed) of positive integers, called the parts, that add up to n . A three-part partition of 0 in $\mathbb{Z}/p\mathbb{Z}$ has the form of $0 = x + y + z$ in $\mathbb{Z}/p\mathbb{Z}$, where x, y, z are all non-zero elements in $\mathbb{Z}/p\mathbb{Z}$. We are interested in counting the number of three-part partitions of 0 in $\mathbb{Z}/p\mathbb{Z}$, where each part is a non-zero quadratic residue modulo p . We call such a partition of 0 a *3Q-partition of 0*. For any 3Q-partition of 0 with three distinct parts, it produces six non-trivial solutions to equation (1) (six ordered solution triples). Likewise, if two of the three parts in a 3Q-partition of 0 are identical, then it gives three non-trivial solutions to equation (1). Thus, the number of 3Q-partitions of 0 is well related to the number of non-trivial solutions to equation (1), which is the same as the number of non-trivial quadratic solutions to equation (2), and can be determined consequently. We discuss these two different types of 3Q-partitions of 0 and the enumeration for each type. We start with the following definitions.

Definition 1.1. Let p be any odd prime number.

1. Denote $r_p = \{\text{the non-zero quadratic residues modulo } p\}$.
2. $S_p = \{(a, b, c) \mid a, b, c \in r_p \text{ and } a + b + c = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\}$.
3. A triple $(a, b, c) \in (\mathbb{Z}/p\mathbb{Z})^3$ is called non-trivial if $abc \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. A solution triple (a, b, c) to equation (2) or to the equation $x + y + z = 0$ in $\mathbb{Z}/p\mathbb{Z}$ is called a quadratic solution if $a, b, c \in r_p$.
4. A multiset $\{a, b, c\}$ is called a 3Q-partition of 0 in $\mathbb{Z}/p\mathbb{Z}$ if $a, b, c \in r_p$ and $a + b + c = 0$. Denote $X(p) = \{\text{all 3Q-partitions of 0 in } \mathbb{Z}/p\mathbb{Z}\}$.

Note that a 3Q-partition $a + b + c = 0$ in $\mathbb{Z}/p\mathbb{Z}$ is represented by the set $\{a, b, c\}$ which may be a multiset because two of the three numbers may be identical. Next, we adopt a definition originated in [8].

Definition 1.2. [8] Given positive integers h and k and a prime number $p > 2$, $N(h, k, p)$ denotes the number of non-trivial solutions to the equation

$$x_1^h + \cdots + x_k^h = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}, \text{ where } x_1, \dots, x_k \in r_p.$$

Remark 1.3. It is known that $|r_p| = (p - 1)/2$ for every odd prime p . As mentioned previously, if $p \equiv 2 \pmod{3}$, there is a one-to-one and onto correspondence between S_p and the set of quadratic solutions to equation (2). Thus, the size of S_p is the number of quadratic solutions to equation (2), which is also the number of quadratic solutions to $x + y + z = 0$ in $\mathbb{Z}/p\mathbb{Z}$. It implies that $|S_p| = N(3, 3, p) = N(1, 3, p)$.

In [8], a character sum $A_k(p)$, where k is a positive integer, was studied and it is useful in calculating the size of S_p in this study. Originally, it was defined for any Dirichlet character $\chi \pmod{p}$. We adopt this definition with respect to the special Dirichlet character $\left(\frac{*}{p}\right)$, which is the Legendre symbol mod p .

Definition 1.4. Let p be an odd prime and k be a positive integer. The Dirichlet character sum $A_k(p)$ is defined by

$$A_k(p) = \sum_{\substack{a_1=1 \\ a_1^3+a_2^3+\dots+a_k^3=0 \\ \text{in } \mathbb{Z}/p\mathbb{Z}}}^{p-1} \sum_{a_2=1}^{p-1} \cdots \sum_{a_k=1}^{p-1} \left(\frac{a_1}{p}\right) \left(\frac{a_2}{p}\right) \cdots \left(\frac{a_k}{p}\right).$$

We consider the case when $p \equiv 2 \pmod{3}$. The above sum function $A_k(p)$ plays an important role in determining the number of solutions to equation (1) or the number of 3Q-partitions of 0 in $\mathbb{Z}/p\mathbb{Z}$. In Section 2, we apply the results about $A_k(p)$ in [8] to develop the exact number $N(3, 3, p) = N(1, 3, p)$ (Theorem 2.4). Similarly, $N(3, 2, p)$ and $N(3, 4, p)$ are calculated. At the end of Section 2, we discuss the density of solution triples over the set r_p^3 .

Next, we focus on counting the number of related restricted partitions of 0. Assume $\{a, b, c\}$ is a 3Q-partition of 0 in $\mathbb{Z}/p\mathbb{Z}$. That is, $a, b, c \in r_p$ and $a + b + c = 0 \pmod{p}$. Because p is a prime greater than 3, only two cases may occur: either exactly two out of the three numbers are identical, or all three are distinct. We divide the 3Q-partitions of 0 into two types based on this distinction. Recall that $X(p)$ denotes the set of all 3Q-partitions of 0 in $\mathbb{Z}/p\mathbb{Z}$ represented by multisets.

Definition 1.5. Let p be an odd prime.

1. $X_1(p) = \{ \{x, x, y\} \mid x, y \in r_p, x \neq y, \text{ and } x + x + y = 0 \text{ in } \mathbb{Z}/p\mathbb{Z} \}$. Any element in $X_1(p)$ is called a 3Q-partition of 0 in $\mathbb{Z}/p\mathbb{Z}$ of type I.
2. $X_2(p) = \{ \text{3Q-partitions } \{x, y, z\} \text{ of } 0 \text{ in } \mathbb{Z}/p\mathbb{Z}, \text{ where } x, y, z \text{ are all distinct} \}$. Elements in $X_2(p)$ are called 3Q-partitions of 0 in $\mathbb{Z}/p\mathbb{Z}$ of type II.
3. Correspondingly, a solution triple (a, b, c) in $\mathbb{Z}/p\mathbb{Z}$ to any equation is of type I if exactly two of the three numbers are identical. It is of type II if all the three numbers are distinct.
4. Denote $\alpha_p = |X_1(p)|$ and $\beta_p = |X_2(p)|$.

In other words, α_p is the number of 3Q-partitions of 0 of type I and β_p is the number of 3Q-partitions of 0 of type II.

Remark 1.6. Obviously, $\alpha_p + \beta_p = |X(p)|$. Assume $x + x + y = 0$ is a 3Q-partition of 0 of type I in $\mathbb{Z}/p\mathbb{Z}$. It produces three elements in S_p : (x, x, y) , (x, y, x) , and (y, x, x) . Similarly, a 3Q-partition of type II produces six triples in S_p by permutation. Thus, $|S_p| = 3|X_1(p)| + 6|X_2(p)|$, that is, $N(3, 3, p) = N(1, 3, p) = 3\alpha_p + 6\beta_p$.

In Section 3, we analyze quadratic solution types to equation (2) and give the exact formulas, respectively, for α_p and β_p . The main result is given in Theorem 3.8. In Section 4, we use the solution triples in S_p to build monomials and homogeneous polynomials in the polynomial ring $(\mathbb{Z}/p\mathbb{Z})[x, y, z]$. We give a formula for the number of such polynomials.

2 Number of solutions

In this section, we calculate the number of non-trivial solutions to equation (1) or equation (3), or the number of quadratic solutions to equation (2), by applying properties of Dirichlet characters (see [14–18]) and the character sum $A_k(p)$ defined in Definition 1.4. We focus on prime numbers p in the form of $p = 3m + 2$, where m is a positive integer. Combinatorial and number theory methods are used to derive an explicit formula for the solution number $|S_p| = N(3, 3, p) = N(1, 3, p)$.

The following lemma shows a known result in the literature. For convenience, we re-state it and provide a simple proof.

Lemma 2.1. Let p be a prime number in the form of $p = 3m + 2$, where m is a positive integer. Then every element in $\mathbb{Z}/p\mathbb{Z}$ is a cubic residue mod p .

Proof. Let $a \in \mathbb{Z}/p\mathbb{Z}$. By Fermat's little theorem $a^p \equiv a \pmod{p}$. Thus, $a \equiv a^p \cdot a^{p-1} = a^{2p-1} = (a^{2m+1})^3 \pmod{p}$. Therefore, every element in $\mathbb{Z}/p\mathbb{Z}$ is a cubic residue mod p . $\square$

Consequently, we claim

Lemma 2.2. Let p be a prime number in the form of $p = 3m + 2$, where m is a positive integer. Then

$$\begin{aligned} |S_p| &= |\{(a, b, c) | a, b, c \in r_p \text{ and } a^3 + b^3 + c^3 = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\}| \\ &= |\{(a, b, c) | a, b, c \in \mathbb{Z}/p\mathbb{Z}, abc \neq 0, \text{ and } a^6 + b^6 + c^6 = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\}| \\ &= |\{(a, b, c) | a, b, c \in r_p \text{ and } a + b + c = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\}| \\ &= |\{(a, b, c) | a, b, c \in \mathbb{Z}/p\mathbb{Z}, abc \neq 0, \text{ and } a^2 + b^2 + c^2 = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\}|. \end{aligned}$$

That is, $|S_p| = N(3, 3, p) = N(1, 3, p)$.

Proof. By Lemma 2.1, there is a one-to-one and onto correspondence between the quadratic solutions $(a, b, c) \in r_p^3$ to the equation $x + y + z = 0$ in $\mathbb{Z}/p\mathbb{Z}$ and the quadratic solutions $(a^{2m+1}, b^{2m+1}, c^{2m+1}) \in r_p^3$ to the equation $x^3 + y^3 + z^3 = 0$ in $\mathbb{Z}/p\mathbb{Z}$. $\square$

In [8], an explicit formula for $A_k(p)$ is given:

Lemma 2.3. [8] Let p be an odd prime with $p \equiv 2 \pmod{3}$. Then for every positive integer k , the Dirichlet character sum $A_k(p)$ is given by

$$A_k(p) = \begin{cases} 0 & \text{if } k \text{ is odd;} \\ (-1)^{k(p-1)/4} \cdot (p-1) \cdot p^{(k-2)/2} & \text{if } k \text{ is even.} \end{cases}$$

In particular, $A_3(p) = 0$. We use this value to help evaluating $N(3, 3, p)$ or $N(1, 3, p)$.

Theorem 2.4. If p is an odd prime with $p \equiv 2 \pmod{3}$, then

$$|S_p| = N(3, 3, p) = N(1, 3, p) = \frac{1}{8}(p-1)\left(p-2+3(-1)^{\frac{p+1}{2}}\right).$$

Proof. Since $p \equiv 2 \pmod{3}$, when a passes through a reduced residue system mod p , a^3 also passes through a reduced residue system mod p . Note that the equation $a + b + c = 0$ and $a^3 + b^3 + c^3 = 0$ involved in the proof below is over the ring $\mathbb{Z}/p\mathbb{Z}$.

$$\begin{aligned} N(3, 3, p) &= \frac{1}{8} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(1 + \left(\frac{a}{p}\right)\right) \left(1 + \left(\frac{b}{p}\right)\right) \left(1 + \left(\frac{c}{p}\right)\right) \\ &\quad \substack{a^3+b^3+c^3=0} \\ &= \frac{1}{8} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(1 + \left(\frac{a}{p}\right)\right) \left(1 + \left(\frac{b}{p}\right)\right) \left(1 + \left(\frac{c}{p}\right)\right) \\ &\quad \substack{a+b+c=0} \\ &= N(1, 3, p). \end{aligned}$$

We expand the above expression into a sum of eight parts and further into a sum with four summands:

$$\begin{aligned} N(1, 3, p) &= \frac{1}{8} \left[\sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} 1 + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{b}{p}\right) + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \right. \\ &\quad \left. + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{c}{p}\right) + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \right] \\ &= \frac{1}{8} \left[\sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} 1 + 3 \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) + 3 \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \right]. \end{aligned}$$

Furthermore, if $a + b + c = 0$ with $abc \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, then $b \neq -a$ and $c = -(a + b)$ in $\mathbb{Z}/p\mathbb{Z}$. Thus, in the above sum, the first of the four summands is calculated as follows:

$$\sum_{\substack{a=1 \\ a+b+c=0}}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} 1 = (p-1)(p-2).$$

Note that when a passes through a reduced residue system mod p , ab also passes through a reduced residue system mod p for all b with $1 \leq b \leq p-1$. Then we replace a by ab and c by cb and apply properties of Dirichlet character sums to calculate the second and the third summand:

$$\sum_{\substack{a=1 \\ a+b+c=0}}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{\substack{a=1 \\ a+1+c=0}}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = 0$$

and

$$\sum_{\substack{a=1 \\ a+b+c=0}}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \sum_{\substack{a=1 \\ a+1+c=0}}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) = (p-1) \sum_{\substack{a=1 \\ a+1+c=0}}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) = (p-1) \left[0 - \left(\frac{-1}{p}\right) \right] = (p-1)(-1)^{\frac{p+1}{2}}.$$

The last summand is 0 by Lemma 2.3:

$$A_3(p) = \sum_{\substack{a=1 \\ a+b+c=0}}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) = 0.$$

Finally, from all the above,

$$\begin{aligned} N(1, 3, p) &= \frac{1}{8} \left[(p-1)(p-2) + 3(p-1)(-1)^{\frac{p+1}{2}} \right] = \frac{p-1}{8} \left(p-2 + 3(-1)^{\frac{p+1}{2}} \right) \\ &= \begin{cases} \frac{(p-1)(p-5)}{8}, & \text{if } p \equiv 1 \pmod{4}, \\ \frac{(p-1)(p+1)}{8}, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \end{aligned}$$

□

Example 2.5. Consider $p = 17$. The set of non-zero quadratic residues mod 17 has eight numbers:

$$r_{17} = \{1, 2 = 6^2, 4, 8 = 5^2, 9, 13 = 8^2, 15 = 7^2, 16\}.$$

By Theorem 2.4, $|S_{17}| = N(1, 3, 17) = (1/8)(17-1)(17-2+3(-1)^9) = 24$. That is, there are 24 triples from r_{17}^3 whose elements add up to 0 modulo 17. They are given as follows:

$$\begin{aligned} S_{17} = \{ & (1, 1, 15), (1, 15, 1), (15, 1, 1), (1, 8, 8), (8, 8, 1), (8, 1, 8), (4, 9, 4), (4, 4, 9), \\ & (9, 4, 4), (9, 16, 9), (16, 9, 9), (9, 9, 16), (16, 2, 16), (16, 16, 2), (2, 16, 16), (13, 8, 13), \\ & (8, 13, 13), (13, 13, 8), (2, 13, 2), (13, 2, 2), (2, 2, 13), (15, 15, 4), (15, 4, 15), (4, 15, 15) \}. \end{aligned}$$

For any prime number $p \equiv 2 \pmod{3}$, $p \equiv 5, 11, 17$, or $23 \pmod{24}$. It is obvious that the number $|S_p|$, or $N(1, 3, p)$, is a multiple of 3 since $3|(p-2)$. We further claim that

Corollary 2.6. *If p is an odd prime with $p \equiv 2 \pmod{3}$, then $|S_p|$ is divisible by 6 when $p \equiv 5, 17$, or $23 \pmod{24}$. However, $|S_p|$ is divisible by 3 but not by 6 if $p \equiv 11 \pmod{24}$.*

Proof. Theorem 2.4 gives

$$|S_p| = \begin{cases} \frac{(p-1)(p-5)}{8}, & \text{if } p \equiv 5 \text{ or } 17 \pmod{24}; \\ \frac{(p-1)(p+1)}{8}, & \text{if } p \equiv 11 \text{ or } 23 \pmod{24}. \end{cases}$$

The proof follows immediately. □

Now we discuss the solution number $N(3, 2, p)$, which is the number of non-trivial quadratic solutions to the equation $x^3 + y^3 = 0$ over $\mathbb{Z}/p\mathbb{Z}$. When $p \equiv 2 \pmod{3}$, $N(3, 2, p)$ is the same as the number $N(1, 2, p)$ of non-trivial quadratic solutions to the equation $x + y = 0$ and is also the number of non-trivial solutions to the equation $x^6 + y^6 = 0$ over $\mathbb{Z}/p\mathbb{Z}$. It is obvious that if -1 is a quadratic non-residue mod p , then all of these equations have no solution, that is, $N(3, 2, p) = N(1, 2, p) = 0$. However, if -1 is a quadratic residue mod p , then $\forall a \in r_p$, $(a, -a)$ is a non-trivial quadratic solution to the equation $x^3 + y^3 = 0$ and all of the non-trivial quadratic solutions to the equation $x^3 + y^3 = 0$ are of this form. Thus, $N(3, 2, p) = N(1, 2, p) = \frac{p-1}{2}$. By a similar proof as in the proof of Theorem 2.4, we also can obtain the same result. In summary,

Proposition 2.7. *Let p be an odd prime with $p \equiv 2 \pmod{3}$. Then*

$$N(3, 2, p) = N(1, 2, p) = \frac{1}{4}(p-1)\left[1 + (-1)^{\frac{p-1}{2}}\right].$$

The situation for $N(3, 4, p)$, the number of non-trivial solutions to $x^6 + y^6 + z^6 + u^6 = 0$ in $\mathbb{Z}/p\mathbb{Z}$, is similar. It can be evaluated as follows.

Theorem 2.8. *If p is an odd prime with $p \equiv 2 \pmod{3}$, then*

$$N(3, 4, p) = N(1, 4, p) = \frac{1}{16}(p-1)\left[p^2 - 2p + 3 + 6(-1)^{\frac{p-1}{2}}\right].$$

Proof. As before, the equation $x^6 + y^6 + z^6 + u^6 = 0$ is considered over the ring $\mathbb{Z}/p\mathbb{Z}$. Similarly as in the proof of Theorem 2.4,

$$\begin{aligned} N(3, 4, p) &= \frac{1}{16} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} \sum_{d=1}^{p-1} \left(1 + \left(\frac{a}{p}\right)\right) \left(1 + \left(\frac{b}{p}\right)\right) \left(1 + \left(\frac{c}{p}\right)\right) \left(1 + \left(\frac{d}{p}\right)\right) \\ &\quad_{a^3+b^3+c^3+d^3=0} \\ &= \frac{1}{16}(p-1)\left(p^2 - 2p + 3 + 6(-1)^{\frac{p-1}{2}}\right). \end{aligned}$$

The second equality above involves steps similar to those in the proof of Theorem 2.4. We skip the details. $\square$

Research has been done on the distribution and density of solutions to a Diophantine equation in the set of all the possible elements. For example, in [19], the number $N(p)$ of the integer solutions modulo a prime p to the equation $y^2 = x^5 - x$ is studied. It is shown that $|N(p) - p|$ is relatively small compared to p . More precisely, $|N(p) - p| < 4\sqrt{p}$ and the constant 4 is the best possible. In our study, all the non-trivial solutions to equation (1) are chosen from the set r_p^3 whose size is $(p-1)^3/8$. Table 1 shows the ratio of the number of solutions to the size of r_p^3 for the first six primes which reflects the density of the solutions in the set r_p^3 .

It seems when p is larger and larger, the density is smaller and smaller. We define the density function as follows.

Table 1: Density of solution number in r_p^3

p	5	11	17	23	29	41
$N(1, 3, p)$	0	15	24	66	84	180
$ r_p^3 $	2^3	5^3	8^3	11^3	14^3	20^3
$N(1, 3, p)/ r_p^3 $	0	0.12	0.046875	0.049587	0.030612245	0.0225

Definition 2.9. Let p be a prime number. Define $D(p) = \frac{N(1, 3, p)}{|r_p^3|}$ and call it the density function of the solutions to equation (1) in the set r_p^3 .

In the next theorem, we give the explicit formula for the density function which indicates that when p is approaching to infinity, the density function acts similarly as $1/p$. Note that, when $p \equiv 2 \pmod{3}$, $p \equiv 5, 11, 17$, or 23 modulo 24 .

Theorem 2.10. Let p be an odd prime number with $p \equiv 2 \pmod{3}$. Then

1.

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

2.

$$\lim_{p \rightarrow \infty} \frac{N(1, 3, p)}{|r_p^3|} = 0 \quad \text{and} \quad \frac{N(1, 3, p)}{|r_p^3|} = O(1/p).$$

Proof.

1. From Theorem 2.4,

$$D(p) = \frac{N(1, 3, p)}{|r_p^3|} = \frac{\frac{1}{8}(p - 1)(p - 2 + 3(-1)^{\frac{p+1}{2}})}{\left(\frac{p-1}{2}\right)^3} = \frac{p - 2 + 3(-1)^{\frac{p+1}{2}}}{(p - 1)^2}.$$

2. Immediately from (1),

$$\lim_{p \rightarrow \infty} \frac{N(1, 3, p)}{|r_p^3|} = \lim_{p \rightarrow \infty} \frac{p - 2 + 3(-1)^{\frac{p+1}{2}}}{(p - 1)^2} = 0$$

and

$$\lim_{p \rightarrow \infty} \frac{\frac{N(1, 3, p)}{|r_p^3|}}{1/p} = \lim_{p \rightarrow \infty} \frac{p - 2 + 3(-1)^{\frac{p+1}{2}}}{(p - 1)^2/p} = 1. \quad \square$$

It confirms that the density function $D(p)$ is approaching to 0 when p goes to infinity. Actually, $D(p) = O(1/p)$.

3 Solution types and the resulting partitions

A classical number theory problem is on the partitions of positive integers. Many researchers have studied counting the number of integers partitions and that of restricted partitions, conjugate and self-conjugate partitions, graphical representations of partitions, and so on. There are many applications of integer partitions in other fields such as molecular chemistry, crystallography, and quantum mechanics. In modern algebra, it is well related to the study of symmetric polynomials, which we will see in Section 4.

Let p be a prime number with $p \equiv 2 \pmod{3}$. Theorem 2.4 states that the number of non-trivial solutions to the equation $x^2 + y^2 + z^2 = 0$ in $\mathbb{Z}/p\mathbb{Z}$, or the number of non-trivial quadratic solutions to $x + y + z = 0$ in $\mathbb{Z}/p\mathbb{Z}$, is $N(1, 3, p)$ and the set of such solutions is S_p . Also,

$$|S_p| = N(1, 3, p) = \frac{1}{8}(p - 1)(p - 2 + 3(-1)^{\frac{p+1}{2}}).$$

For $a, b, c \in \mathbb{Z}/p\mathbb{Z}$ with $a + b + c = 0$, we can view $\{a, b, c\}$ as a partition of 0 in $\mathbb{Z}/p\mathbb{Z}$. Furthermore, if a, b, c are chosen from r_p , we obtain a 3Q-partition of 0 in $\mathbb{Z}/p\mathbb{Z}$ defined in 1.5. It is straightforward to check that there is no quadratic triple $(a, b, c) \in r_5^3$ satisfying $a + b + c \equiv 0 \pmod{5}$. Thus, $S_5 = \emptyset$. The aforementioned formula also confirms that $|S_5| = N(3, 3, 5) = N(1, 3, 5) = 0$. For any prime $p \equiv 2 \pmod{3}$ which is greater than 5, $|S_p| \neq 0$. Next we consider primes p greater than 5 with $p \equiv 2 \pmod{3}$. For such a prime number p , $S_p \neq \emptyset$ and in $\mathbb{Z}/p\mathbb{Z}$, $3a \neq 0$ if $a \neq 0$. We examine the quadratic triples $(a, b, c) \in S_p$. Among these triples, only two cases may occur: (1) two of the three are identical but not all the same or (2) all three numbers a, b, c are distinct. By Definition 1.5, these two cases correspond to solutions of type I or type II. We concern the number of triples in S_p of each type. Later we show that, for certain prime numbers p , S_p has no triples of type II.

In Definition 1.5, the sets of all 3Q-partitions of 0 in r_p , those of type I, and those of type II, are denoted as $X(p)$, $X_1(p)$, $X_2(p)$. Recall that for any $(a, b, c) \in S_p$, $a + b + c = 0$ in $\mathbb{Z}/p\mathbb{Z}$ and $a, b, c \in r_p$. Thus, every triple in S_p produces one 3Q partition of 0 in r_p . On the other hand, for every 3Q-partition $\{a, b, c\}$ of 0 in r_p , that is, $\{a, b, c\} \in X(p)$, it gives three or six solution triples in S_p , depending on (a, b, c) being of type I or II. If $\{a, a, c\} \in X_1(p)$, where $a \neq c$, $a, c \in r_p$, and $a + a + c = 0$, it produces three solutions of type I in S_p : (a, a, c) , (a, c, a) , and (c, a, a) . Similarly, for $\{a, b, c\} \in X_2(p)$, six solutions in S_p of type II are produced by permutation. Recall that $\alpha_p = |X_1(p)|$ and $\beta_p = |X_2(p)|$. The relationships between α_p , β_p , and $|S_p|$ are given as follows:

Lemma 3.1. *Let p be a prime with $p \equiv 2 \pmod{3}$. Then*

$$|S_p| = 3\alpha_p + 6\beta_p = \frac{1}{8}(p-1)\left(p-2+3(-1)^{\frac{p+1}{2}}\right).$$

Also note that, for any $(a, b, c) \in S_p$, $\lambda(a, b, c) \in S_p$ as well for any $\lambda \in r_p$. We define an equivalence relation on S_p . One can easily check the equivalence property.

Definition 3.2. Let p be a prime number with $p \equiv 2 \pmod{3}$. For any two triples $(a, b, c), (u, v, w) \in S_p$, $(a, b, c) \sim (u, v, w)$ if and only if there exists $\lambda \in r_p$ such that $(a, b, c) = (\lambda u, \lambda v, \lambda w)$. The equivalence class containing (x, y, z) is denoted as $[(a, b, c)]$. The set of equivalence classes is denoted by $\overline{S_p}$.

Proposition 3.3. *Let p be a prime number with $p \equiv 2 \pmod{3}$. Then*

$$|\overline{S_p}| = \frac{1}{4}\left(p-2+3(-1)^{\frac{p+1}{2}}\right) \text{ and } \forall (a, b, c) \in S_p, |[a, b, c]| = \frac{p-1}{2}.$$

Proof. Obviously, $|r_p| = (p-1)/2 = |[a, b, c]|$. The number of equivalence classes, $|\overline{S_p}|$, is given by $|S_p|/((p-1)/2)$. $\square$

In this section, we provide formulas for α_p , β_p , and correspondingly the number of type I and type II solutions in S_p . We first examine the situations for $p = 29$ and $p = 41$.

Example 3.4. Consider $p = 29$. The set of non-zero quadratic residues mod p is $r_{29} = \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$. From Proposition 3.3, $|\overline{S_{29}}| = 6$. The six equivalence classes are as follows:

$$\overline{S_{29}} = \{[(1, 4, 24)], [(4, 1, 24)], [(1, 24, 4)], [(24, 1, 4)], [(24, 4, 1)], [(4, 24, 1)]\},$$

which are all represented by a triple of type II. Thus, all the triples in S_{29} are of type II. It implies that $X_1(29) = \emptyset$ and so $\alpha_{29} = 0$. The class $[(1, 4, 24)]$ gives all the 14 partitions of 0 in r_{29} : $\lambda + 4\lambda + 24\lambda \equiv 0 \pmod{29}$, where $\lambda \in r_{29}$. Thus, $X_2(29) = \{\{\lambda, 4\lambda, 14\lambda\} \mid \lambda \in r_{29}\}$ and $\beta_{29} = |r_{29}| = 14$. Consequently, the total number of solutions in S_{29} is $6 \cdot 14 = 84$, which confirms the result from Theorem 2.4: $|S_{29}| = N(1, 3, 29) = N(3, 3, 29) = 28(27-3)/8 = 84$.

For the prime number $p = 41$, we obtain solutions of both types.

Example 3.5. For $p = 41$, there are three equivalence classes of type I: $[(1, 1, 39)]$, $[(1, 39, 1)]$, $[(39, 1, 1)]$. There are six equivalence classes of type II: $[(1, 4, 36)]$, $[(1, 36, 4)]$, $[(4, 36, 1)]$, $[(4, 1, 36)]$, $[(36, 1, 4)]$, $[(36, 4, 1)]$.

In this example, $|r_{41}| = 20$, so each equivalence class has 20 triples from S_{41} . Thus, S_{41} has $3 \cdot 20 = 60$ solutions of type I and $6 \cdot 20 = 120$ solutions of type II. Altogether, $|S_{41}| = 60 + 120 = 180$. From Theorem 2.4, we also can calculate that $|S_{41}| = (40/8)(39 - 3) = 180$.

The equivalence classes $[(1, 1, 39)]$ and $[(1, 4, 36)]$ give the set of the partitions of 0 of type I and type II in r_{41} , respectively. In particular,

$$X_1(41) = \{ \{ \lambda, \lambda, 39\lambda \} \mid \lambda \in r_{41} \} \text{ and } X_2(41) = \{ \{ \lambda, 4\lambda, 36\lambda \} \mid \lambda \in r_{41} \}.$$

So $\alpha_{41} = \beta_{41} = |r_{41}| = 20$. Altogether, there are 40 3Q-partitions of 0 in r_{41} , that is, $|X(41)| = 40$. The size of S_{41} can also be viewed as $|S_{41}| = 3\alpha_{41} + 6\beta_{41} = 3 \cdot 20 + 6 \cdot 20 = 180$.

Proposition 3.6. Let p be a prime number greater than 5 and $p \equiv 2 \pmod{3}$.

1. If $p \equiv 5$ or $23 \pmod{24}$, then all the solutions in S_p are of type II and $|S_p|$ is divisible by 6.
2. If $p \equiv 11$ or $17 \pmod{24}$, then there are exactly $3(p-1)/2$ solutions of type I in S_p .
3. $S_5 = \emptyset$ and S_{11} has no solutions of type II.

Proof. Let $(a, a, c) \in S_p$, a solution triple of type I. Then $a, c \in r_p$ and $a + a + c \equiv 0 \pmod{p} \Rightarrow -2a \equiv c \pmod{p}$. It implies that -2 is a quadratic residue mod p .

1. Assume $p \equiv 5$ or $23 \pmod{24}$. Then -2 is not a quadratic residue of p . From the above, S_p does not have solution triples of type I. Thus, all the solution triples in S_p are of type II and $\alpha_p = 0$. By Lemma 3.1, $|S_p|$ is divisible by 6.
2. Assume $p \equiv 11$ or $17 \pmod{24}$. Then -2 is a quadratic residue mod p . Consider any solution triple $(a, a, c) \in S_p$ of type I as above. Since $a \in r_p$, $-2a \equiv k \pmod{p}$ for a unique $k \in r_p$. It is obvious that all the three triples (a, a, k) , (a, k, a) , and (k, a, a) are solutions in S_p of type I and there are exactly $3(p-1)/2 = 3\alpha_p$ of them. Every solution triple of type I in S_p must also be of such a form. Thus, S_p has exactly $3(p-1)/2$ many solutions of type I.
3. From (2), S_{11} has $3(11-1)/2 = 15$ solutions of type I. By Lemma 3.1,

$$|S_p| = \frac{1}{8}(11-1)\left(11-2+3(-1)^{\frac{11-1}{2}}\right) = 15.$$

Thus, S_{11} has no solutions of type II. □

Next, we focus on 3Q-partitions of 0 in r_p . We derive formulas α_p , β_p , and relationships between them. We examine an example first.

Example 3.7. Consider $p = 11$. $r_{11} = \{1, 4, 9, 5 = 4^2, 3 = 5^2\}$. From Proposition 3.6, $X_2(11) = \emptyset$.

$$X(11) = \{ \{1, 1, 9\}, \{1, 5, 5\}, \{3, 3, 5\}, \{3, 4, 4\}, \{4, 9, 9\} \} = X_1(11).$$

Each above partition produces three solutions of type I in S_{11} . The set S_{11} is given as follows:

$$S_{11} = \{ (1, 1, 9), (1, 9, 1), (9, 1, 1), (1, 5, 5), (5, 1, 5), (5, 5, 1), (3, 3, 5), (3, 5, 3), \\ (5, 3, 3), (3, 4, 4), (4, 3, 4), (4, 4, 3), (4, 9, 9), (9, 4, 9), (9, 9, 4) \}.$$

S_{11} is divided into three equivalence classes: $\overline{S_{11}} = \{ [(1, 1, 9)], [(1, 9, 1)], [(9, 1, 1)] \}$. Each of the equivalence class is of size 5. For example,

$$[(1, 1, 9)] = \{ (1, 1, 9), 4(1, 1, 9) = (4, 4, 3), 9(1, 1, 9) = (9, 9, 4), 5(1, 1, 9) = (5, 5, 1), 3(1, 1, 9) = (3, 3, 5) \}.$$

We see that $|S_{11}| = |\overline{S_{11}}| \cdot |r_{11}| = 3 \cdot 5 = 15$. Also, $\alpha_{11} = 5$ and $\beta_{11} = 0$.

We now give the formulas for α_p , β_p and show relationship between them.

Theorem 3.8. Let p be a prime number with $p \equiv 2 \pmod{3}$.

1. If $p \equiv 5$ or $23 \pmod{24}$, $\alpha_p = 0$ and

$$\beta_p = \frac{1}{48}(p-1)\left(p-2+3(-1)^{\frac{p+1}{2}}\right).$$

2. If $p \equiv 11$ or $17 \pmod{24}$, then $\alpha_p = (p-1)/2$, and

$$\beta_p = \frac{1}{48}(p-1)\left(p-14+3(-1)^{\frac{p+1}{2}}\right).$$

3. The number $|X(p)| = \alpha_p + \beta_p$ of all the 3Q-partitions of 0 in r_p is given as follows:

$$|X(p)| = \alpha_p + \beta_p = \begin{cases} \frac{(p-1)(p-5)}{48}, & \text{if } p \equiv 5 \pmod{24}; \\ \frac{(p-1)(p+13)}{48}, & \text{if } p \equiv 11 \pmod{24}; \\ \frac{(p-1)(p+7)}{48}, & \text{if } p \equiv 17 \pmod{24}; \\ \frac{(p-1)(p+1)}{48}, & \text{if } p \equiv 23 \pmod{24}. \end{cases}$$

Proof.

1. If $p \equiv 5$ or $23 \pmod{24}$, then there is no quadratic solution of type II by Proposition 3.6(1). Thus, $\alpha_p = 0$. From Lemma 3.1,

$$\beta_p = \frac{|S_p|}{6} = \frac{(p-1)(p-2+3(-1)^{(p+1)/2})}{48}.$$

2. For $p \equiv 11$ or $17 \pmod{24}$, there are $3(p-1)/2$ many solutions of type I by Proposition 3.6(2). Since the three permutations from one solution provides one 3Q-partitions of 0, $\alpha_p = (p-1)/2$. Lemma 3.1 implies that

$$\beta_p = \frac{1}{6}(|S_p| - 3\alpha_p) = \frac{1}{6}\left[\frac{1}{8}(p-1)\left(p-2+3(-1)^{\frac{p+1}{2}}\right) - \frac{3}{2}(p-1)\right] = \frac{1}{48}(p-1)\left(p-14+3(-1)^{\frac{p+1}{2}}\right).$$

3. Note that $(p+1)/2$ is odd when $p \equiv 5$ or $17 \pmod{24}$ and is even when $p \equiv 11$ or $23 \pmod{24}$. When $p \equiv 5$ or $23 \pmod{24}$, $\alpha_p = 0$. Then $\alpha_p + \beta_p = \beta_p$ and the result follows from (1). For $p \equiv 11$ or $17 \pmod{24}$, $\alpha_p = \frac{p-1}{2}$ by Proposition 3.6(2). Add α_p to β_p obtained from (1) above, we have

$$\begin{aligned} \alpha_p + \beta_p &= \frac{p-1}{2} + \frac{(p-1)\left(p-14+3(-1)^{\frac{p+1}{2}}\right)}{48} = \frac{(p-1)(p+10+3(-1)^{\frac{p+1}{2}})}{48} \\ &= \begin{cases} \frac{(p-1)(p+13)}{48}, & \text{if } p \equiv 11 \pmod{24}; \\ \frac{(p-1)(p+7)}{48}, & \text{if } p \equiv 17 \pmod{24}. \end{cases} \quad \square \end{aligned}$$

Corollary 3.9. Let p be a prime number with $p \equiv 2 \pmod{3}$.

(1) If $\beta_p = 0$, then $p = 11$ or $p = 17$. That is, S_p has no solutions of type II only when $p = 11$ or 17 .

(2) If $p \equiv 11$ or $17 \pmod{24}$ and $p \neq 11$, $p \neq 17$, then

$$\frac{24}{p-11} \leq \frac{\alpha_p}{\beta_p} \leq \frac{24}{p-17}.$$

(3) If $p \equiv 11$ or $17 \pmod{24}$ and $p \neq 11$, $p \neq 17$, then $12\beta_p < \alpha_p^2 < 24\beta_p$.

Proof. For (1), from Theorem 3.8, the only way to make $\beta_p = 0$ is when $p - 14 + 3(-1)^{(p+1)/2} = 0$. This only can occur when $p = 11$ or $p = 17$.

For (2), $p \equiv 11$ or $17 \pmod{24}$. We apply Theorem 3.8 (2) and Proposition 3.6 (2) to obtain

$$\frac{\alpha_p}{\beta_p} = \frac{\frac{p-1}{2}}{\frac{(p-1)(p-14+3(-1)^{(p+1)/2})}{48}} = \frac{24}{p-14+3(-1)^{(p+1)/2}}.$$

Since $p - 17 \leq p - 14 + 3(-1)^{(p+1)/2} \leq p - 11$, we obtain the required result.

Similar to the proof of (2), for (3), assume $p \equiv 11$ or $17 \pmod{24}$, $p \neq 11$, and $p \neq 17$. It implies that $p > 33$. We have

$$\frac{\alpha_p^2}{\beta_p} = \frac{\frac{(p-1)^2}{4}}{\frac{(p-1)(p-14+3(-1)^{(p+1)/2})}{48}} = \frac{12(p-1)}{p-14+3(-1)^{(p+1)/2}}.$$

Because $p > 33$, $p - 1 < 2(p - 17)$, thus $12(p - 1)/(p - 17) < 24$. Then

$$12 = \frac{12(p-11)}{p-11} < \frac{12(p-1)}{p-11} \leq \frac{12(p-1)}{p-14+3(-1)^{(p+1)/2}} \leq \frac{12(p-1)}{p-17} < 24. \quad \square$$

Corollary 3.9(1) claims two cases and the only two cases when type II solution does not exist. It happens only when $p = 11$ or $p = 17$. Example 3.7 confirms the truth when $p = 11$. For $p = 17$, we use Theorem 2.4 to calculate $|S_{17}| = 24$. S_{17} has three equivalence classes each of which is of size 8: $[(1, 1, 15)]$, $[(1, 15, 1)]$, $[(15, 1, 1)]$. They produce all the 24 solutions in S_{17} and they are all of type I which confirms that there is no solution of type II in S_{17} .

Corollary 3.9(2) estimated the ratio α_p/β_p when $\alpha_p \neq 0$. However, the value of β_p is closer to the value of α_p^2 when $\alpha_p \neq 0$. Corollary 3.9(3) provides a comparison of these two values.

4 Counting monomials in three variables of certain degree in $\mathbb{Z}/p\mathbb{Z}[x, y, z]$

Polynomials are important functions which have many interesting properties and they play important roles in many areas of mathematics and science. For example, polynomials are used to approximate other complex functions. In advanced mathematics, polynomial rings and algebraic varieties over a field are central concepts in algebra and algebraic geometry. Among the polynomials with multiple variables, homogeneous polynomials are those with all the monomials having the same degree. Homogeneous polynomials are building blocks of the multivariable polynomials and they often appear in physics as a consequence of dimensional analysis, where measured quantities must match in real-world problems. Any non-zero polynomial can be decomposed, in a unique way, as a sum of homogeneous polynomials of different degrees. Consider a polynomial ring $R = K[x_1, x_2, \dots, x_n]$ over a field K and a positive integer d . It is known that the set R_d of all homogeneous polynomials of degree d forms a vector space whose dimension is the number of different monomials of degree d (see [20]). We are interested in applying the results from the previous sections to calculate the number of certain monomials of the same degree d , for some values of d .

Consider the polynomial ring $R = (\mathbb{Z}/p\mathbb{Z})[x, y, z]$ with p being prime and a monomial $x^a y^b z^c \in R$, where a, b, c are non-negative integers. By Fermat's little theorem, $r^p = r$ for all $r \in \mathbb{Z}/p\mathbb{Z}$. Thus, we are only interested in the monomials $x^a y^b z^c$ with $0 \leq a, b, c \leq p - 1$. When $a + b + c = d$, we say $x^a y^b z^c$ is of degree d . For any non-constant monomial $x^a y^b z^c$ of degree d with $0 \leq a, b, c \leq p - 1$ (or $a, b, c \in \mathbb{Z}/p\mathbb{Z}$), $0 < d \leq 3(p - 1)$. We write $x^a y^b z^c = \mathbf{x}^\alpha$ where $\mathbf{x} = (x, y, z)$ and $\alpha = (a, b, c)$. A polynomial $f(\mathbf{x}) = f(x, y, z) \in R = (\mathbb{Z}/p\mathbb{Z})[x, y, z]$ has the form of

$$f(\mathbf{x}) = \sum_{\alpha \in T} a_\alpha \mathbf{x}^\alpha,$$

where T is a subset of $(\mathbb{Z}/p\mathbb{Z})^3$ and $a_\alpha \in \mathbb{Z}/p\mathbb{Z}$.

Table 2: Values of $|S_p|$, $|S_1|$, and $|S_2|$

p	11	17	23	29	41	47	53	59	71	83	89	101	...
$ S_p $	15	24	66	84	180	276	312	435	630	861	924	1,200	...
$ S_1 $	12	12	60	42	90	228	156	285	504	525	462	600	...
$ S_2 $	3	12	6	42	90	48	156	150	126	336	462	600	...

Definition 4.1. Consider the polynomial ring $R = (\mathbb{Z}/p\mathbb{Z})[x, y, z]$, where p is odd and $p \equiv 2 \pmod{3}$. Let d be a non-negative integer. A polynomial in R is called a homogeneous polynomial of degree d if the degrees of all the involved monomials are of the same degree d .

Consider $\alpha = (a, b, c)$, where $a, b, c \in r_p$ and $a + b + c \equiv 0 \pmod{p}$, that is, $(a, b, c) \in S_p$. It implies that $a + b + c = p$ or $a + b + c = 2p$. In this section, we count the number of monomials of degree p or $2p$.

Definition 4.2. Define

$$S_1 = \{(a, b, c) \in S_p | a + b + c = p\};$$

$$S_2 = \{(a, b, c) \in S_p | a + b + c = 2p\}.$$

The number $N(1, 3, p)$ is the number of monomials $x^a y^b z^c$ of degree p or $2p$, where $(a, b, c) \in S_p = S_1 \cup S_2$, a disjoint union. Then $N(1, 3, p) = |S_p| = |S_1| + |S_2|$. The values of $|S_p|$, $|S_1|$, and $|S_2|$ for small primes are indicated in Table 2.

We note that in Table 2, $|S_1| = |S_2|$ for some primes such as 17, 29, 41, 53, and so on. We classify the prime numbers achieving this property as follows.

Theorem 4.3. Let p be a prime number with $p \equiv 2 \pmod{3}$.

1. There are exactly $\frac{1}{8}(p-1)\left(p-2+3(-1)^{\frac{p+1}{2}}\right)$ many monomials of degree p or $2p$;
2. If $p \equiv 5$ or $17 \pmod{24}$, then

$$|S_1| = |S_2| = \frac{1}{2}N(1, 3, p) = \frac{1}{16}(p-1)(p-5).$$

That is, there are exactly $(p-1)(p-5)/16$ many monomials of degree d and so does that of degree $2p$.

Proof.

- (1) It is straightforward from Theorem 2.4 which gives the value of $|S_p|$.
- (2) If $p \equiv 5$ or $17 \pmod{24}$, then -1 is a quadratic residue mod p . Thus, $a + b + c = p \Leftrightarrow (p-a) + (p-b) + (p-c) = 2p$. Here $0 < a, b, c < p \Leftrightarrow 0 < (p-a), (p-b), (p-c) < p$. Thus, there is a one-to-one and onto correspondence between S_1 and S_2 . Then apply Theorem 2.4 again, $|S_1| = |S_2| = \frac{1}{2}N(1, 3, p)$. $\square$

Note that for any monomial $\mathbf{x}^\alpha$, where $\alpha \in S_i$, the exponent for each of the variables x, y, z is non-zero quadratic residue mod p and the total degree is p for $i = 1$ and $2p$ for $i = 2$. The aforementioned results provided the number of such monomials. Next, we show that these types of monomials have an interesting formal partial derivative. Let $\mathbf{x}^\alpha$ be a monomial in the polynomial ring $(\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$, the formal partial derivative of $\mathbf{x}^\alpha$ with respect to x_i is $\frac{\partial \mathbf{x}^\alpha}{\partial x_i}$.

Theorem 4.4. Let p be an odd prime number with $p \equiv 2 \pmod{3}$ and $R = (\mathbb{Z}/p\mathbb{Z})[x, y, z]$.

1. Let $\mathbf{x}^\alpha$ be a monomial in R with $\alpha \in S_p$. Then

$$x \frac{\partial \mathbf{x}^\alpha}{\partial x} + y \frac{\partial \mathbf{x}^\alpha}{\partial y} + z \frac{\partial \mathbf{x}^\alpha}{\partial z} = 0.$$

2. A polynomial $f(x)$ in R satisfying $x \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y} + z \frac{\partial f}{\partial z} = 0$ if all of the monomial terms of $f(x, y, z)$ are of degree p or $2p$.

Proof.

- (1) The left hand side expression equals 0 if and only if the coefficients of all the three monomials are divisible by p . Let $\mathbf{x}^a = x^a y^b z^c$, where $(a, b, c) \in S_p$. Then $a + b + c = p$ or $a + b + c = 2p$. Then

$$x \frac{\partial \mathbf{x}^a}{\partial x} + y \frac{\partial \mathbf{x}^a}{\partial y} + z \frac{\partial \mathbf{x}^a}{\partial z} = x(ax^{a-1}y^b z^c) + y(bx^a y^{b-1} z^c) + z(cx^a y^b z^{c-1}) = (a + b + c)x^a y^b z^c = 0 \text{ in } R,$$

since $a + b + c = p$ or $2p$ which means $a + b + c = 0$ in R .

- (2) This is immediately from (1). □

5 Conclusions and future directions

In this paper, we have made connections between the number of solutions of certain Diophantine equations modulo a prime number p and the number of 3Q-partitions of 0 in the ring $\mathbb{Z}/p\mathbb{Z}$. We classified two types of 3Q-partitions of 0 and provided the number of each type of partitions. Many questions remain open. In the theory of partitions of positive integers, researchers have worked on restricted partitions with a given number of parts, with distinct parts, or with a given maximal value of all the parts, etc. Other questions involve concepts such as conjugate and self-conjugate partitions. We are interested in studying similar problems for our partition problems. We also plan to study similar Diophantine equations mod p involving more than three variables and generalize the results.

In Section 4, we counted the number of certain monomials of degree p or $2p$ in the polynomial ring $(\mathbb{Z}/p\mathbb{Z})[x, y, z]$. We provided exact formulas for the number of each type of monomials when $p \equiv 5$ or $17 \pmod{24}$. It remains open to count such monomials for $p \equiv 11$ or $23 \pmod{24}$. Let $R_p = \{\text{all monomials of degree } p\}$ and $R_{2p} = \{\text{all monomials of degree } 2p\}$. It is known from [20] that R_p and R_{2p} are vector spaces over $\mathbb{Z}/p\mathbb{Z}$ and the dimensions of these two spaces are given by

$$\dim(R_p) = \binom{p+2}{2} = \frac{(p+2)(p+1)}{2}, \quad \dim(R_{2p}) = \binom{2p+2}{2} = (p+1)(2p+1).$$

The set of monomials we have studied is a subset of $R_p \cup R_{2p}$. It is natural to study other types of monomials and the enumeration of them.

A homogeneous ideal of the ring $(\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$ is an ideal generated by homogeneous polynomials. These ideals are important algebraic structures in the study of projective varieties in algebraic geometry. We would like to seek further connections and applications in this area.

Acknowledgement: The authors would like to thank the referees for helpful and detailed comments, which have significantly contributed to improving the presentation of this paper.

Funding information: This work was supported by the Fundamental Research Funds for the Central Universities, CHD (300102121102).

Conflict of interest: Authors state no conflict of interest.

References

- [1] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), no. 3, 443–551.
- [2] J. Ax, *Solving Diophantine problems modulo every prime*, Ann. Math. **85** (1967), no. 2, 161–183.
- [3] M. Murata, *Primitive solutions of nonscalar quadratic Diophantine equations*, J. Number Theory **201** (2019), 398–435.
- [4] G. Gao and Z. Liu, *Small prime solution to diagonal Diophantine equations*, Int. J. Number Theory **16** (2020), no. 3, 447–460.

- [5] S. Li, *On a Diophantine equation with prime numbers*, Int. J. Number Theory **15** (2019), no. 8, 1601–1616.
- [6] T. Ching and K. Tsang, *Small prime solutions to linear equations in three variables*, Acta Arith. **178** (2017), no. 1, 57–76.
- [7] N. D. Elkies, *On $A^4 + B^4 + C^4 = D^4$* , Math. Comp. **51** (1988), no. 184, 825–835.
- [8] W. Zhang and X. Wang, *On a kind of character sums and their recurrence properties*, Acta Arith. **185** (2018), no. 4, 347–355.
- [9] S. Shen and W. Zhang, *On the quartic Gauss sums and their recurrence property*, Adv. Differ. Equ. **2017** (2017), 43.
- [10] W. Zhang and J. Hu, *The number of solutions of the diagonal cubic congruence equation mod p* , Math. Rep. **20** (2018), no. 70, 73–80.
- [11] G. Andrews, *The Theory of Partitions*, Cambridge University Press, Cambridge, 1998.
- [12] B. Kim, *On the number of partitions of n into k different parts*, J. Number Theory **132** (2012), no. 6, 1306–1313.
- [13] J. Melenk and I. Babuska, *The partition of unity finite element method: basic theory and applications*, Comput. Meth. Appl. Mech. Eng. **139** (1996), 289–314.
- [14] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- [15] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349–389.
- [16] B. C. Berndt and R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 107–129.
- [17] W. Zhang and H. Li, *Elementary Number Theory*, Shaanxi Normal University Press, Shaanxi, 2008.
- [18] W. Zhang and H. Liu, *On the general Gauss sums and their fourth power mean*, Osaka J. Math. **42** (2005), 189–199.
- [19] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, France, 1993.
- [20] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, 2nd ed., Springer Science+Business Media, Inc., New York, NY, USA, 2005.