Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 6(12): 13515–13524.
DOI: 10.3934/math.2021784
Received: 31 January 2021
Accepted: 11 August 2021
Published: 22 September 2021

Research article

On the number of unit solutions of cubic congruence modulo n

Junyong Zhao[1,2,*]

[1] Mathematical College, Sichuan University, Chengdu 610064, China
[2] School of Mathematics and Physics, Nanyang Institute of Technology, Nanyang 473004, China

* **Correspondence:** Email: jyzhao_math@163.com.

Abstract: For any positive integer n, let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$ be the ring of residue classes module n, and let $\mathbb{Z}_n^\times := \{x \in \mathbb{Z}_n | \gcd(x, n) = 1\}$. In 1926, for any fixed $c \in \mathbb{Z}_n$, A. Brauer studied the linear congruence $x_1 + \cdots + x_m \equiv c \pmod n$ with $x_1, \dots, x_m \in \mathbb{Z}_n^\times$ and gave a formula of its number of incongruent solutions. Recently, Taki Eldin extended A. Brauer's result to the quadratic case. In this paper, for any positive integer n, we give an explicit formula for the number of incongruent solutions of the following cubic congruence

$$x_1^3 + \cdots + x_m^3 \equiv 0 \pmod n \quad \text{with } x_1, \dots, x_m \in \mathbb{Z}_n^\times.$$

Keywords: cubic congruence; exponential sums; unit solutions
Mathematics Subject Classification: 11D79, 11L03, 11L03

1. Introduction

For any positive integer n, let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$ be the ring of residue classes modulo n, and let $\mathbb{Z}_n^\times := \{x \in \mathbb{Z}_n | \gcd(x, n) = 1\}$, $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n | x \neq 0\}$ respectively. In 1926, for any fixed $c \in \mathbb{Z}_n$, A. Brauer [2] studied the linear congruence

$$x_1 + \cdots + x_m \equiv c \pmod n, \quad \text{with } x_1, \dots, x_m \in \mathbb{Z}_n^\times,$$

and gave a formula for the number of incongruent solutions. This answered a problem of H. Rademacher [7]. In 2014, Sun and Yang [9] generalized A. Brauer's result by giving an explicit formula for the number of incongruent solutions of general linear congruence

$$k_1x_1 + \cdots + k_mx_m \equiv c \pmod n \quad \text{with } x_1, \dots, x_m \in \mathbb{Z}_n^\times,$$

where $k_1, \dots, k_m, c \in \mathbb{Z}_n$.

Recently, Taki Eldin [8] studied the quadratic case and provided an explicit formula for the number of incongruent solutions of

$$k_1x_1^2 + \cdots + k_mx_m^2 \equiv c \pmod{n} \quad \text{with } x_1, \ldots, x_m \in \mathbb{Z}_n^\times,$$

where $k_1, \ldots, k_m, c \in \mathbb{Z}_n$ with $\gcd(k_1 \cdots k_m, n) = 1$, which extended the result of Yang and Tang [10].

Therefore, it is natural to consider the following cubic congruence:

$$k_1x_1^3 + \cdots + k_mx_m^3 \equiv c \pmod{n}.$$

with $k_1, \ldots, k_m, c \in \mathbb{Z}_n$ such that $\gcd(k_1 \cdots k_m, n) = 1$.

When $n = p$ is a prime number, $k_1 = \cdots = k_m = 1$, S. Chowla, J. Cowles and M. Cowles [3], Hong and Zhu [4] gave a formula of the number of incongruent solutions of the above congruence with $c = 0$ and $c \neq 0$ respectively. In this note, we investigate the following cubic congruence

$$x_1^3 + \cdots + x_m^3 \equiv 0 \pmod{n} \quad \text{with } x_1, \ldots, x_m \in \mathbb{Z}_n^\times. \tag{1.1}$$

Denote by $N_m(n)$ the number of incongruent solutions of (1.1). Li and Ouyang [6], in 2018, presented a relation between $N_m(p^a)$ and $N_m(p^b)$ for some certain integers a and b with $a \geq b$. In this paper, we will give an explicit formula of $N_m(n)$, which couldn't be obtained by the results in [6]. Particularly, we have the first main theorem as follows.

Theorem 1.1. *Let p be a prime number and m be a positive integer. Then each of the following holds.*

(1). If $p \equiv 1 \pmod 3$, then

$$N_1(p) = 0, \;\; N_2(p) = 3(p-1), \;\; N_3(p) = p^2 + (c-9)p + (8-c),$$

and

$$N_m(p) + 3N_{m-1}(p) - 3(p-1)N_{m-2}(p) - (pc + 3p - 1)N_{m-3}(p) = (p-1)^{m-3}(p^2 - 3p - c),$$

for all $m \geq 4$, where c is uniquely determined by

$$4p = c^2 + 27d^2, \quad c \equiv 1 \pmod 3.$$

(2). If $p \not\equiv 1 \pmod 3$, then

$$N_m(p) = \frac{(p-1)^m + (-1)^{m+1}}{p} + (-1)^m.$$

For every nonzero integer n, let $rad(n)$ be the *radical* of n, i.e., the product of distinct prime divisors of n. As usual, for any prime number p, let $v_p(n)$ be the *p-adic valuation* of n, i.e., $p^{v_p(n)} \mid n$ and $p^{v_p(n)+1} \nmid n$. For any $a \in \mathbb{Z}$, let $\langle a \rangle_n$ be the unique element in $\mathbb{Z}_n$ such that $a \equiv \langle a \rangle_n \pmod{n}$. Now, we can state our second main Theorem.

Theorem 1.2. *Let n and m be positive integers and let $\xi := \exp(\frac{2\pi i}{9})$. Then*

$$N_m(n) = \delta_m(n) \frac{n^{m-1}}{(rad(n))^{m-1}} \prod_{p \mid n} N_m(p),$$

where

$$\delta_m(n) = \begin{cases} 1, & \text{if } v_3(n) \le 1, \\ \frac{9N'_m(9)}{2^m+2(-1)^m}, & \text{if } v_3(n) \ge 2, \end{cases}$$

$$N'_m(9) = \begin{cases} \frac{1}{9}\sum\limits_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9}{2}})^{9-j}(1+\xi^j)^m, & \text{if } \langle m\rangle_9 \text{ is even}, \\ \frac{1}{9}\sum\limits_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9+9}{2}})^{9-j}(1+\xi^j)^m, & \text{if } \langle m\rangle_9 \text{ is odd and } m \ge 10, \\ 0, & \text{otherwise}, \end{cases}$$

$N_m(p)$ was obtained in Theorem 1.1.

The paper is organized as follows: Section 2 provides some notations and lemmas which will be used in the sequel. In Section 3, we give the proofs of Theorem 1.1 and Theorem 1.2.

2. Preliminaries

Throughout, p denotes a prime number. For any finite set A, denote by $|A|$ the cardinality of A. For any $a \in \mathbb{Z}$, let

$$T_a := \sum_{x\in\mathbb{Z}_p^*} \exp\Big(\frac{2\pi i a x^3}{p}\Big).$$

Next, we give some lemmas which are needed in the proofs of Theorem 1.1 and Theorem 1.2. We begin with the following famous result.

Lemma 2.1. ([1]) *(Chinese Remainder Theorem) Let $f(x_1,\ldots,x_m) \in \mathbb{Z}[x]$. If $n_1,\ldots,n_r$ are pairwise relatively prime positive integers, let N_i be the number of zeros of*

$$f(x_1,\ldots,x_m) \equiv 0 \pmod{n_i},$$

and N be the number of zeros of

$$f(x_1,\ldots,x_m) \equiv 0 \pmod{n_1\cdots n_r},$$

then $N = N_1\cdots N_r$.

The following classical result was obtained by Gauss.

Lemma 2.2. ([3]) *Let g be a primitive root modulo p. Then T_1+1, T_g+1, $T_{g^2}+1$ are the roots of equation*

$$x^3 - 3px - pc = 0,$$

where c is uniquely determined by

$$4p = c^2 + 27d^2, \quad c \equiv 1 \pmod 3).$$

Lemma 2.3. *Let g be a primitive root modulo p, and let $S = \{1, g, g^2\}$. Then for any $a \in \mathbb{Z}_p^*$, there exists a unique $b \in S$ such that*

$$T_a = T_b.$$

Proof. Since g is a primitive root modulo p, for any $a \in \mathbb{Z}_p^*$, one has $a \equiv g^c \pmod p$ for some integer c with $1 \le c \le p-1$. Let $c = 3q + r$ with $q, r \in \mathbb{Z}$ and $0 \le r \le 2$. It then follows that

$$\begin{aligned} T_a &= \sum_{x \in \mathbb{Z}_p^*} \exp\Big(\frac{2\pi i a x^3}{p}\Big) \\ &= \sum_{x \in \mathbb{Z}_p^*} \exp\Big(\frac{2\pi i g^c x^3}{p}\Big) \\ &= \sum_{x \in \mathbb{Z}_p^*} \exp\Big(\frac{2\pi i a g^r (g^q x)^3}{p}\Big) \\ &= \sum_{x \in \mathbb{Z}_p^*} \exp\Big(\frac{2\pi i a g^r x^3}{p}\Big) \\ &= T_{g^r} \end{aligned}$$

as desired. So Lemma 2.3 is proved. □

Lemma 2.4. ([1]) *For any $a \in \mathbb{Z}_p$, we have*

$$\sum_{b \in \mathbb{Z}_p} \exp\Big(\frac{2\pi i a b}{p}\Big) = \begin{cases} p, & \text{if } p \mid a, \\ 0, & \text{if } p \nmid a. \end{cases}$$

Lemma 2.5. ([5]) *Let $a \in \mathbb{Z}_p^*$. Then $x^3 \equiv a \pmod p$ is solvable if and only if $a^{\frac{p-1}{d}} \equiv 1 \pmod p$, where $d = \gcd(3, p-1)$.*

For any positive integer m, let

$$A_m(p) := \{(x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m | x_1^3 + \cdots + x_m^3 \equiv 0 \pmod p\}.$$

We have the following lemma.

Lemma 2.6. *Suppose $p \not\equiv 1 \pmod 3$. Then for any positive integer m, we have*

$$|A_m(p)| = p^{m-1}.$$

Proof. Let $f : \mathbb{Z}_p \mapsto \mathbb{Z}_p$ be a map satisfying that $f(a) = \langle a^3 \rangle_p$ for any $a \in \mathbb{Z}_p$. We claim that f is bijective. In fact, by Lemma 2.5, it is easy to see that f is subjective. Moreover, since $|\mathbb{Z}_p|$ is finite, one has that f is also injective. So the claim is true.

Therefore, we deduce that

$$\begin{aligned} |A_m(p)| &= \Big|\{(x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m | x_1^3 + \cdots + x_m^3 \equiv 0 \pmod p\}\Big| \\ &= \Big|\{(x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m | x_1 + \cdots + x_m \equiv 0 \pmod p\}\Big| \\ &= p^{m-1} \end{aligned}$$

as expected. □

Lemma 2.7. *Let* $\xi := \exp(\frac{2\pi i}{9})$ *and let* $N'_m(9)$ *be the number of solutions of congruence*

$$x_1 + \cdots + x_m \equiv 0 \pmod 9 \text{ with } x_1, \ldots, x_m \in \{-1, 1\}. \tag{2.1}$$

Then

$$N'_m(9) = \begin{cases} \frac{1}{9}\sum_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9}{2}})^{9-j}(1+\xi^j)^m, & \text{if } \langle m\rangle_9 \text{ is even,} \\ \frac{1}{9}\sum_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9+9}{2}})^{9-j}(1+\xi^j)^m, & \text{if } \langle m\rangle_9 \text{ is odd and } m \geq 10, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let S_1 and S_{-1} be the number of terms of Eq (2.1) for which $x_i = 1$ and $x_i = -1$ $(1 \leq i \leq m)$ respectively. Then the Eq (2.1) has a solution if and only if $S_1 \equiv S_{-1} \pmod 9$. We distinguish two cases as follows.

Case 1. Let $\langle m\rangle_9$ be even.

The congruence (2.1) has a solution if and only if

$$S_1 \in \{\frac{\langle m\rangle_9}{2}, \frac{\langle m\rangle_9}{2}+9, \frac{\langle m\rangle_9}{2}+18, \ldots, m-\frac{\langle m\rangle_9}{2}\}.$$

Therefore, one gets

$$N'_m(9) = \binom{m}{\frac{\langle m\rangle_9}{2}} + \binom{m}{\frac{\langle m\rangle_9}{2}+9} + \binom{m}{\frac{\langle m\rangle_9}{2}+18} + \cdots + \binom{m}{m-\frac{\langle m\rangle_9}{2}}. \tag{2.2}$$

Since $\xi = \exp(\frac{2\pi i}{9})$, we easily obtain the well-known fact:

$$\xi^9 = 1,\ 1 + \xi^j + (\xi^j)^2 + \cdots + (\xi^j)^8 = 0 \text{ with } (j = 1\ldots, 8). \tag{2.3}$$

By (2.3) and computing directly, one gets the following identity:

$$\frac{1}{9}\sum_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9}{2}})^{9-j}(1+\xi^j)^m = \binom{m}{\frac{\langle m\rangle_9}{2}} + \binom{m}{\frac{\langle m\rangle_9}{2}+9} + \binom{m}{\frac{\langle m\rangle_9}{2}+18} + \cdots + \binom{m}{m-\frac{\langle m\rangle_9}{2}}. \tag{2.4}$$

By (2.2) and (2.4), we have

$$N'_m(9) = \frac{1}{9}\sum_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9}{2}})^{9-j}(1+\xi^j)^m. \tag{2.5}$$

Case 2. Let $\langle m\rangle_9$ be odd.

Obviously, the congruence (2.1) has no solution if $m = 1, 3, 5, 7$. So we suppose that $m \geq 10$.

The Eq (2.1) has a solution if and only if

$$S_1 \in \{\frac{\langle m\rangle_9+9}{2}, \frac{\langle m\rangle_9+9}{2}+9, \frac{\langle m\rangle_9+9}{2}+18, \ldots, m-\frac{\langle m\rangle_9+9}{2}\}.$$

From an argument which is similar to that in Case 1, we get

$$N'_m(9) = \frac{1}{9}\sum_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9+9}{2}})^{9-j}(1+\xi^j)^m. \tag{2.6}$$

From the above discussion, we can conclude that

$$N'_m(9)=\begin{cases}\frac{1}{9}\sum\limits_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9}{2}})^{9-j}(1+\xi^j)^m, & \textit{if } \langle m\rangle_9 \textit{ is even},\\ \frac{1}{9}\sum\limits_{j=1}^{9}(\xi^{\frac{\langle m\rangle_9+9}{2}})^{9-j}(1+\xi^j)^m, & \textit{if } \langle m\rangle_9 \textit{ is odd and } m\geq 10,\\ 0, & \textit{otherwise}.\end{cases}$$

This finishes the proof of Lemma 2.7. □

3. Proof of Theorem 1.1 and Theorem 1.2

In this section, we give the proofs of Theorem 1.1 and Theorem 1.2.

Proof of Theorem 1.1. We divide the proof into two cases.

Case 1. Let $p\equiv 1 \pmod 3$. By Lemma 2.3 and Lemma 2.4, we deduce that

$$\begin{aligned}N_m(p)&=\frac{1}{p}\sum_{(x_1,\ldots,x_m)\in(\mathbb{Z}_p^*)^m}\sum_{a=0}^{p-1}\exp\Big(\frac{2\pi ia(x_1^3+\cdots+x_m^3)}{p}\Big)\\&=\frac{(p-1)^m}{p}+\frac{1}{p}\sum_{a=1}^{p-1}\sum_{(x_1,\ldots,x_m)\in(\mathbb{Z}_p^*)^m}\exp\Big(\frac{2\pi ia(x_1^3+\cdots+x_m^3)}{p}\Big)\\&=\frac{(p-1)^m}{p}+\frac{1}{p}\sum_{a=1}^{p-1}\Big(\sum_{x\in\mathbb{Z}_p^*}\exp\Big(\frac{2\pi iax^3}{p}\Big)\Big)^m\\&=\frac{(p-1)^m}{p}+\frac{1}{p}\Big(\frac{p-1}{3}T_1^m+\frac{p-1}{3}T_g^m+\frac{p-1}{3}T_{g^2}^m\Big).\end{aligned}\tag{3.1}$$

By Lemma 2.2, T_1, T_g, T_{g^2} are roots of equation

$$x^3+3x^2-3(p-1)x-(pc+3p-1)=0,\tag{3.2}$$

where c is uniquely determined by

$$4p=c^2+27d^2,\quad c\equiv 1 \pmod 3.$$

It then follows from (3.2) that

$$\begin{aligned}T_1+T_g+T_{g^2}&=-3,\\T_1T_g+T_1T_{g^2}+T_gT_{g^2}&=3-3p,\\T_1T_gT_{g^2}&=pc+3p-1.\end{aligned}\tag{3.3}$$

Clearly, $N_1(p)=0$. Moreover, using (3.1) and (3.3), we get that

$$
\begin{aligned}
N_2(p) &= \frac{(p-1)^2}{p} + \frac{p-1}{3p}(T_1^2 + T_g^2 + T_{g^2}^2)\\
&= \frac{(p-1)^2}{p} + \frac{p-1}{3p}((T_1 + T_g + T_{g^2})^2 - 2(T_1T_g + T_1T_{g^2} + T_gT_{g^2}))\\
&= 3(p-1),
\end{aligned}
$$

and

$$
\begin{aligned}
N_3(p) =&\frac{(p-1)^3}{p} + \frac{p-1}{3p}(T_1^3 + T_g^3 + T_{g^2}^3)\\
=&\frac{(p-1)^3}{p} + \frac{p-1}{6p}(3(T_1 + T_g + T_{g^2})(T_1^2 + T_g^2 + T_{g^2}^2) + 6T_1T_gT_{g^2} - (T_1 + T_g + T_{g^2})^3)\\
=&p^2 + (c-9)p + (8-c).
\end{aligned}
$$

Now, let m be any integer with $m \geq 4$. Then for any $a \in \{1, g, g^2\}$, we have

$$T_a^m + 3T_a^{m-1} - 3(p-1)T_a^{m-2} - (pc + 3p - 1)T_a^{m-3} = 0 \tag{3.4}$$

by (3.2). It then follows from (3.1) and (3.4) that

$$
\begin{aligned}
&N_m(p) - \frac{(p-1)^m}{p} + 3(N_{m-1}(p) - \frac{(p-1)^{m-1}}{p})\\
&- 3(p-1)(N_{m-2}(p) - \frac{(p-1)^{m-2}}{p}) - (pc + 3p - 1)(N_{m-3}(p) - \frac{(p-1)^{m-3}}{p}) = 0,
\end{aligned}
$$

which is equivalent to

$$N_m(p) + 3N_{m-1}(p) - 3(p-1)N_{m-2}(p) - (pc + 3p - 1)N_{m-3}(p) = (p-1)^{m-3}(p^2 - 3p - c).$$

So Theorem 1.1 is proved in this case.

Case 2. Let $p \not\equiv 1 \pmod 3$. For any integer i with $1 \leq i \leq m$, define

$$A_{m,i}(p) := \{(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_m) \in (\mathbb{Z}_p)^m | x_1^3 + \cdots + x_m^3 \equiv 0 \pmod p\}.$$

Then using principle of cross-classification, we derive that

$$
\begin{aligned}
N_m(p) =&\Big|A_m(p) \setminus \bigcup_{i=1}^{m} A_{m,i}(p)\Big|\\
=&|A_m(p)| + \sum_{t=1}^{m}(-1)^t \sum_{1\leq i_1<\cdots<i_t\leq m} \Big|\bigcap_{j=1}^{t} A_{m,i_j}(p)\Big|.
\end{aligned} \tag{3.5}
$$

Let t be an integer with $1 \leq t \leq m-1$. Then for any integer t-tuple $(i_1, \dots, i_t)$ with $1 \leq i_1 < \cdots < i_t \leq m$, it is obvious that

$$\Big|\bigcap_{j=1}^{t} A_{m,i_j}(p)\Big| = |A_{m-t}(p)|. \tag{3.6}$$

Thus by Lemma 2.5, (3.5) and (3.6), one gets that

$$\begin{aligned} N_m(p) =& p^{m-1} + \sum_{t=1}^{m-1}(-1)^t\binom{m}{t}p^{m-t-1} + (-1)^m \\ =& \frac{1}{p}\sum_{t=0}^{m-1}(-1)^t\binom{m}{t}p^{m-t} + (-1)^m \\ =& \frac{(p-1)^m + (-1)^{m+1}}{p} + (-1)^m. \end{aligned}$$

This finishes the proof of Theorem 1.1. □

Now, we begin the proof of Theorem 1.2.

Proof of Theorem 1.2. Let n have the prime decomposition

$$n = \prod_{p|n} p^{v_p(n)}.$$

By Lemma 2.1, one has the product formla

$$N_m(n) = \prod_{p|n} N_m(p^{v_p(n)}). \tag{3.7}$$

So to compute $N_m(n)$, it is enough to study the prime power case $N_m(p^{v_p(n)})$ with $p|n$.

Now, we consider the following two cases with $p|n$.

Case 1. For any $p|n$ it holds either $p \neq 3$ or $p = 3,\ v_3(n) = 1$.

If $p \neq 3$, by Theorem B(1) of [6], we have

$$N_m(p^{v_p(n)}) = p^{(m-1)(v_p(n)-1)}N_m(p),$$

where $N_m(p)$ has been studied in Theorem 1.1.

If $p = 3$ and $v_3(n) = 1$, one has

$$N_m(3^{v_3(n)}) = N_m(3) = 3^{(m-1)(v_3(n)-1)}N_m(3).$$

Hence, for $p \neq 3$ or $p = 3,\ v_3(n) = 1$, we get

$$N_m(p^{v_p(n)}) = p^{(m-1)(v_p(n)-1)}N_m(p). \tag{3.8}$$

It then follows from (3.7) and (3.8) that

$$\begin{aligned} N_m(n) &= \prod_{p|n} N_m(p^{v_p(n)}) \\ &= \prod_{p|n} p^{(m-1)(v_p(n)-1)}N_m(p) \\ &= \prod_{p|n} \frac{p^{(m-1)v_p(n)}}{p^{m-1}}N_m(p) \end{aligned}$$

$$= \frac{n^{m-1}}{(rad(n))^{m-1}} \prod_{p|n} N_m(p)$$

as expected.

Case 2. $p = 3$ and $v_3(n) \geq 2$.

By Theorem B(1) in [6], one has

$$N_m(3^{v_3(n)}) = 3^{(m-1)(v_3(n)-2)} N_m(9). \tag{3.9}$$

Since $x^3 \equiv 1 \pmod 9$ for $x \in \{1, 4, 7\}$ and $x^3 \equiv -1 \pmod 9$ for $x \in \{2, 5, 8\}$, one gets that

$$N_m(9) = 3^m N'_m(9). \tag{3.10}$$

Therefore, by (3.7)–(3.10), we have

$$\begin{aligned} N_m(n) &= \prod_{p|n} N_m(p^{v_p(n)}) \\ &= 3^{(m-1)(v_3(n)-2)} N_m(9) \prod_{\substack{p|n \\ p\neq 3}} N_m(p^{v_p(n)}) \\ &= 3^{(m-1)(v_3(n)-2)+m} N'_m(9) \prod_{\substack{p|n \\ p\neq 3}} p^{(m-1)(v_p(n)-1)} N_m(p) \\ &= \frac{(3^{v_3(n)})^{m-1}}{3^{m-2}} N'_m(9) \prod_{\substack{p|n \\ p\neq 3}} \frac{(p^{v_p(n)})^{m-1}}{p^{m-1}} N_m(p) \\ &= \frac{3N'_m(9)}{N_m(3)} \frac{n^{m-1}}{(rad(n))^{m-1}} \prod_{p|n} N_m(p). \end{aligned}$$

By Theorem 1.1, we have

$$N_m(3) = \frac{2^m + 2(-1)^m}{3}.$$

Hence, we get

$$N_m(n) = \frac{9N'_m(9)}{2^m + 2(-1)^m} \frac{n^{m-1}}{(rad(n))^{m-1}} \prod_{p|n} N_m(p).$$

From the above discussion of Case 1 and Case 2, we can conclude that

$$N_m(n) = \delta_m(n) \frac{n^{m-1}}{(rad(n))^{m-1}} \prod_{p|n} N_m(p),$$

where

$$\delta_m(n) = \begin{cases} 1, & if\ v_3(n) \leq 1, \\ \frac{9N'_m(9)}{2^m+2(-1)^m}, & if\ v_3(n) \geq 2, \end{cases}$$

$N'_m(9)$ and $N_m(p)$ were obtained in Lemma 2.7 and Theorem 1.1, respectively.

This finishes the proof of Theorem 1.2. □

4. Conclusions

In this paper, we present an explicit formula of the number of unit solutions of diagonal cubic form over $\mathbb{Z}_n$, by using the method of exponential sums. As future directions, one can find the formula of the number of unit solutions of $x_1^3 + \cdots + x_n^3 \equiv c \pmod{n}$ over $\mathbb{Z}_n$ with $c \not\equiv 0 \pmod{n}$.

Conflict of interest

We declare that we have no conflict of interest.

References

1. T. M. Apostol, *Introduction to analytic number theory*, New York: Springer, 1976.
2. A. Brauer, Lösung der Aufgabe 30, *Jahresber. Dtsch. Math.-Ver.*, **35** (1926), 92–94.
3. S. Chowla, J. Cowles, M. Cowles, On the number of zeros of diagonal cubic forms, *J. Number Theory*, **9** (1977), 502–506.
4. S. F. Hong, C. X. Zhu, On the number of zeros of diagonal cubic forms over finite fields, *Forum Math.*, **33** (2021), 697–708.
5. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, 2 Eds., Graduate Texts in Mathematics, New York: Springer-Verlag, 1990.
6. S. Li, Y. Ouyang, Counting the solutions of $\lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} \equiv c \bmod n$, *J. Number Theroy*, **187** (2018), 41–65.
7. H. Rademacher, Aufgabe 30, *Jahresber. Dtsch. Math.-Ver.*, **34** (1925), 158.
8. R. F. Taki Eldin, On the number of incongruent solutions to a quadratic congruence over algebraic integers, *Int. J. Number Theory*, **15** (2019), 105–130.
9. C. Sun, Q. Yang, On the sumset of atoms in cyclic groups, *Int. J. Number Theory*, **10** (2014), 1355–1363.
10. Q. Yang, M. Tang, On the addition of squares of units and nonunits modulo n, *J. Number Theory*, **155** (2015), 1–12.