Hindawi
Journal of Mathematics
Volume 2021, Article ID 7634728, 8 pages
https://doi.org/10.1155/2021/7634728

Research Article

On Pythagorean Triples and the Primitive Roots Modulo a Prime

Jingzhe Wang

School of Statistics and Mathematics, Inner Mongolia University of Finance and Economics, Hohhot 010070, Inner Mongolia, China

Correspondence should be addressed to Jingzhe Wang; wangjingzhe729@126.com

Received 27 June 2021; Accepted 17 July 2021; Published 30 July 2021

Academic Editor: Wenpeng Zhang

In this paper, we use the elementary methods and the estimates for character sums to study a problem related to primitive roots and the Pythagorean triples and prove the following result: let p be an odd prime large enough. Then, there must exist three primitive roots x, y, and z modulo p such that $x^2 + y^2 = z^2$.

1. Introduction

It is well known that all positive integer solutions of the equation $x^2 + y^2 = z^2$ are $x = t(a^2 - b^2)$, $y = 2tab$, and $z = t(a^2 + b^2)$, where t, a, and b are arbitrary positive integers satisfying $a > b$; a and b have no prime divisors in common, and one of a or b is odd and the other is even. This result can be found in many elementary number theory textbooks, e.g., reference [1] (see Theorems 2–9). We call such a set of solution (x, y, z) as a Pythagorean triple. For example, taking $t = b = 1$ and $a = 2$ or 4, then $(x, y, x) = (3, 4, 5), (15, 8, 17)$ are two Pythagorean triples.

In this paper, we only focus on the solutions of the form

$$(x, y, z) = \left(4a^2 - (2b-1)^2, 4a(2b-1), 4a^2 + (2b-1)^2\right), \tag{1}$$

where a and b are any positive integers.

On the other hand, let p be a fixed odd prime and g be an integer with $(g, p) = 1$. If $g, g^2, \ldots, g^{p-1}$ form a reduced residue system modulo p, then g is called a primitive root modulo p. For other properties of the primitive roots and related results, see references [1–11], which we will not cover here. In this paper, we will consider the following problem.

For any odd prime p and integer $1 < M < p$, whether there is a Pythagorean triple (x, y, z) in (1) with $1 \le a, b \le M$, such that x, y, and z all are the primitive roots modulo p?

If there are, let $C(M, p)$ denotes the number of all such Pythagorean triples (x, y, z) in (1) with $1 \le a, b \le M$. Then, how does $C(M, p)$ depend on p?

We think these problems are interesting, and they depict the distribution properties of the Pythagorean triples in other special integer sets, such as the primitive roots modulo p, D. H. Lehmer numbers, and Lucas and Fibonacci sequences.

In this paper, let us make two simple conclusions about the asymptotic properties of $C(M, p)$ as follows.

Theorem 1. *For any odd prime p, we have the asymptotic formula*

$$C(p, p) = \frac{\phi^3(p-1)}{p-1} + O\left(\frac{\phi^3(p-1)}{p^{3/2}} \cdot 8^{\omega(p-1)}\right), \tag{2}$$

where, as usual, $\phi(n)$ denotes the Euler function and $\omega(n)$ denotes the number of all distinct prime divisors of n.

Theorem 2. *Let p be an odd prime with $p \equiv 1 \bmod 4$. Then, for any integer $1 < M \le p$, we have the asymptotic formula*

$$C(M, p) = \frac{\phi^3(p-1)}{(p-1)^3} \cdot M^2 + O\left(\frac{M^2 \cdot \phi^3(p-1)}{p^{7/2}} \cdot 8^{\omega(p-1)} \cdot \ln^2 p\right) + O\left(\frac{\phi^3(p-1)}{p^2} \cdot 8^{\omega(p-1)} \cdot \ln^2 p\right). \tag{3}$$

It is clear that for any positive number $\varepsilon > 0$, if $M > p^{1/2+\varepsilon}$, then Theorem 2 is nontrivial. That is, the main term is larger than the error terms.

From our theorems, we may immediately deduce the following two corollaries.

Corollary 1. *Let p be an odd prime large enough. Then, there must exist three primitive roots x, y, and z modulo p such that*

$$x^2 + y^2 = z^2. \tag{4}$$

Corollary 2. *Let $p \equiv 1 \bmod 4$ be a prime large enough. Then, for any integer $p^{1/2+\varepsilon} < M < p$, there must exist three primitive roots x, y, and z modulo p with $1 \le x, y, z \le M^2$ such that*

$$x^2 + y^2 = z^2, \tag{5}$$

where $\varepsilon > 0$ is any fixed positive number.

2. Several Lemmas

To complete the proof of our main result, we need the following four simple lemmas. For the sake of simplicity, we do not repeat some elementary number theory and analytic number theory results, which can be found in references [10, 12, 13]. First, we have the following.

Lemma 1. *Let p be an odd prime. Then, for any integer a with $(a, p) = 1$, we have the identity*

$$\frac{\phi(p-1)}{p-1} \sum_{k \mid p-1} \frac{\mu(k)}{\phi(k)} {\sum_{r=1}^{k}}' e\left(\frac{r \cdot \operatorname{ind}(a)}{k}\right) = \begin{cases} 1, & \text{if } a \text{ is a primitive root mod } p, \\ 0, & \text{if } a \text{ is not a primitive root mod } p, \end{cases} \tag{6}$$

where $e(y) = e^{2\pi i y}$, ${\sum_{r=1}^{k}}'$ denotes the summation over all integers $1 \le r \le k$ such that r is coprime to k, $\mu(n)$ is the Möbius function, and $\operatorname{ind}(a)$ denotes the index of a relative to some fixed primitive root $g \bmod p$.

Proof. See Proposition 2.2 in [13]. □

Lemma 2. *Let p be an odd prime and $\chi_1, \ldots, \chi_r$ be Dirichlet characters modulo p, at least one of which is nonprincipal character. Let $f(x)$ be an integral coefficient polynomial of degree d. Then, for pairwise distinct integers $a_1, \ldots, a_r$, we have the estimate*

$$\sum_{a=1}^{p-1} \chi_1(a + a_1)\chi_2(a + a_2) \ldots \chi_r(a + a_r) e\left(\frac{f(a)}{p}\right) \le (r + d) \cdot p^{1/2}. \tag{7}$$

Proof. This is Lemma 17 in [14]. Some related work can also be found in [15]. □

Lemma 3. *Let p be an odd prime. Then, for any characters χ_1, χ_2, and χ_3 (not all the principal characters) modulo p, we have the estimate*

$$\sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\chi_2(4a)\chi_3\left(4a^2 + 1\right) = O\left(p^{1/2}\right). \tag{8}$$

Proof. If χ_2 is an odd character modulo p, then $\chi_2(-1) = -1$, so we have

$$\begin{aligned} &\sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\chi_2(4a)\chi_3\left(4a^2 + 1\right) \\ &= \sum_{a=1}^{p-1} \chi_1\left(4(-a)^2 - 1\right)\chi_2(-4a)\chi_3\left(4(-a)^2 + 1\right) \\ &= -\sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\chi_2(4a)\chi_3\left(4a^2 + 1\right), \end{aligned} \tag{9}$$

which implies

$$\sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\chi_2(4a)\chi_3\left(4a^2 + 1\right) = 0. \tag{10}$$

If χ_2 is an even character modulo p, then there is a character ψ modulo p such that $\chi_2 = \psi^2$. Now, from the properties of the Legendre symbol modulo p and Lemma 2, we have the estimate

$$\begin{aligned} &\sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\chi_2(4a)\chi_3\left(4a^2 + 1\right) \\ &= \chi_2(4) \sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\psi^2(a)\chi_3\left(4a^2 + 1\right) \\ &= \chi_2(4) \sum_{a=1}^{p-1} \left(1 + \left(\frac{a}{p}\right)\right)\chi_1(4a - 1)\psi(a)\chi_3(4a + 1) \\ &= \chi_2(4) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\chi_1(4a - 1)\psi(a)\chi_3(4a + 1) + \chi_2(4) \\ &\quad \sum_{a=1}^{p-1} \chi_1(4a - 1)\psi(a)\chi_3(4a + 1) = O\left(p^{1/2}\right). \end{aligned} \tag{11}$$

If χ_1 and χ_3 are the principal character modulo p, then χ_2 is not the principal character modulo p. In this case, we have

$$\begin{aligned} &\sum_{a=1}^{p-1} \chi_1\left(4a^2 - 1\right)\chi_2(4a)\chi_3\left(4a^2 + 1\right) \\ &= \sum_{a=1}^{p-1} \chi_2(4a) + O(1) = O(1). \end{aligned} \tag{12}$$

Combining (10)–(12), we may immediately deduce Lemma 3. □

Lemma 4. *Let p be an odd prime with $p \equiv 1 \bmod 4$ and $1 < M < p$ be an integer. Then, for any characters χ_1, χ_2, and χ_3 (not all the principal characters) modulo p, we have the estimate*

$$\sum_{a=1}^{M}\sum_{b=1}^{M}\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right) = O\left(\frac{M^2}{\sqrt{p}}\cdot \ln^2 p\right)+O(p\cdot \ln p). \tag{13}$$

Proof. For any integer n, from the trigonometric identity

$$\sum_{a=0}^{p-1} e\left(\frac{na}{p}\right) = \begin{cases} p, & \text{if } p\mid n, \\ 0, & \text{if } p\nmid n, \end{cases} \tag{14}$$

we have

$$\begin{aligned}
&\sum_{a=1}^{M}\sum_{b=1}^{M}\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)\\
&=\frac{1}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} e\left(\frac{r(a-c)}{p}\right)e\left(\frac{s(b-d)}{p}\right)\\
&\quad\times\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)\\
&=\frac{M^2}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)\\
&\quad+\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\times\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)e\left(\frac{r(a-c)}{p}\right)\\
&\quad+\frac{M}{p^2}\sum_{s=1}^{p-1}\sum_{d=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\times\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)e\left(\frac{s(b-d)}{p}\right)\\
&\quad+\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M} e\left(\frac{r(a-c)}{p}\right)e\left(\frac{s(b-d)}{p}\right)\\
&\quad\times\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)\equiv W_1+W_2+W_3+W_4.
\end{aligned} \tag{15}$$

From the properties of the reduced residue system, complete residue system modulo p, and Lemma 3, we have

$$
\begin{aligned}
W_1 &= \frac{M^2}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)\\
&= \frac{M^2}{p^2}\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)-\frac{M^2}{p^2}\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(-4a)\chi_3\left(4a^2+1\right)\\
&= \frac{M^2}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-b^2\right)\chi_2(4ab)\chi_3\left(4a^2+b^2\right)+O\left(p^{1/2}\right)\\
&= \frac{M^2}{p^2}\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)\sum_{b=1}^{p-1}\chi_1\left(b^2\right)\chi_2\left(b^2\right)\chi_3\left(b^2\right)+O\left(p^{1/2}\right)\\
&= O\left(\frac{M^2}{p}\cdot\left|\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)\right|\right)+O\left(p^{1/2}\right)\\
&= O\left(\frac{M^2}{\sqrt{p}}\right)+O\left(p^{1/2}\right).
\end{aligned}
\tag{16}
$$

Note that if $p\equiv 1\bmod 4$, then there exist two integers u_0 and $-u_0$ such that the congruence $4x^2\equiv -1\bmod p$. So we have

$$
4a^2+1\equiv 4a^2-4u_0^2\equiv 4(a-u_0)(a+u_0)\bmod p. \tag{17}
$$

From the estimate

$$
\sum_{c=1}^{M} e\left(\frac{-rc}{p}\right)=O\left(\frac{1}{|\sin(\pi r/p)|}\right), \tag{18}
$$

the method of proving (16), and the properties of Gauss sums, we have

$$
\begin{aligned}
W_2 &= \frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\times\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)e\left(\frac{r(a-c)}{p}\right)\\
&= \frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-b^2\right)\times\chi_2(4ab)\chi_3\left(4a^2+b^2\right)e\left(\frac{r(a-c)}{p}\right)\\
&\quad-\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(-4a)\chi_3\left(4a^2+1\right)e\left(\frac{r(a-c)}{p}\right)\\
&= \frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)\times\sum_{b=1}^{p-1}\chi_1\left(b^2\right)\chi_2\left(b^2\right)\chi_3\left(b^2\right)e\left(\frac{rab}{p}\right)\sum_{c=1}^{M}e\left(\frac{-rc}{p}\right)\\
&\quad-\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(-4a)\chi_3\left(4a^2+1\right)e\left(\frac{r(a-c)}{p}\right)\\
&\ll \frac{M\left|\tau\left(\chi_1^2\chi_2^2\chi_3^2\right)\right|}{p^2}\sum_{r=1}^{p-1}\left|\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)\overline{\chi_1}^2(a)\overline{\chi_2}^2(a)\overline{\chi_3}^2(a)\right|\\
&\quad\times\frac{1}{|\sin(\pi r/p)|}+\frac{M}{p^2}\cdot p^{1/2}\cdot\sum_{r=1}^{p-1}\frac{1}{|\sin(\pi r/p)|}\\
&\ll \frac{M\cdot\ln p}{\sqrt{p}}\cdot\left|\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\overline{\chi_1\chi_2}^2\overline{\chi_3}^2(4a)\chi_3\left(4a^2+1\right)\right|+\frac{M}{\sqrt{p}}\cdot\ln p\ll M\cdot\ln p,
\end{aligned}
\tag{19}
$$

where $\tau(\chi) = \sum_{a=1}^{p-1}\chi(a)e(a/p)$ denotes the classical Gauss sums and $|\tau(\chi)| \le \sqrt{p}$.

$$\begin{aligned} W_3 &= \frac{M}{p^2}\sum_{s=1}^{p-1}\sum_{d=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\left(4a^2-(2b-1)^2\right)\times\chi_2(4a(2b-1))\chi_3\left(4a^2+(2b-1)^2\right)e\left(\frac{s(b-d)}{p}\right) \\ &= \frac{M}{p^2}\sum_{s=1}^{p-1}\sum_{d=1}^{M}\sum_{a=1}^{p-1}\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)e\left(\frac{-s\ d}{p}\right)\times\sum_{b=1}^{p-1}\chi_1^2(2b-1)\chi_2^2(2b-1)\chi_3^2(2b-1)e\left(\frac{\overline{2}s(2b-1+1)}{p}\right) \\ &\ll \frac{M}{p^{3/2}}\sum_{s=1}^{p-1}\frac{1}{|\sin(\pi s/p)|}\cdot\left|\sum_{b=1}^{p-1}\chi_1^2(b)\chi_2^2(b)\chi_3^2(b)e\left(\frac{\overline{2}sb}{p}\right)\right| \ll M\cdot\ \ln\ p, \end{aligned} \tag{20}$$

and

$$\begin{aligned} W_4 &= \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{r(a-c)}{p}\right)e\left(\frac{s(b-d)}{p}\right) \\ &\quad\times\chi_1\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_3\left(4a^2+(2b-1)^2\right) \\ &\quad-\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{r(a-c)}{p}\right)e\left(\frac{-s\ d}{p}\right) \\ &\quad\times\chi_1\left(4a^2-1\right)\chi_2(-4a)\chi_3\left(4a^2+1\right) \\ &= \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{r(a-c)}{p}\right)e\left(\frac{\overline{2}s(b+1-2\ d)}{p}\right) \\ &\quad\times\chi_1\left(4a^2-b^2\right)\chi_2(4ab)\chi_3\left(4a^2+b^2\right)+O\left(p^{1/2}\cdot\ \ln^2\ p\right) \\ &= \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{r(ab-c)}{p}\right)e\left(\frac{\overline{2}s(b+1-2\ d)}{p}\right) \\ &\quad\times\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)\chi_1^2(b)\chi_2^2(b)\chi_3^2(b)+O\left(p^{1/2}\cdot\ \ln^2\ p\right) \\ &= \frac{\tau\left(\chi_1^2\chi_2^2\chi_3^2\right)}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{-rc}{p}\right)e\left(\frac{\overline{2}s(1-2\ d)}{p}\right) \\ &\quad\times\chi_1\left(4a^2-1\right)\chi_2(4a)\chi_3\left(4a^2+1\right)\overline{\chi}_1^2(ra+\overline{2}s)\overline{\chi}_2^2(ra+\overline{2}s) \\ &\quad\times\overline{\chi}_3^2(ra+\overline{2}s)+O\left(p^{1/2}\cdot\ \ln^2\ p\right) \\ &= O\left(\frac{p}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\frac{1}{|\sin(\pi r/p)|}\cdot\frac{1}{|\sin(\pi s/p)|}\right)=O\left(p\cdot\ \ln^2\ p\right), \end{aligned} \tag{21}$$

where $\overline{a}$ denotes the solution of the congruence equation $ax \equiv 1 \bmod p$.

Similarly, we also have

Combining (15), (16), and (19)–(21), we have the estimate

$$\sum_{a=1}^{M}\sum_{b=1}^{M}\chi_1\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_3\left(4a^2+(2b-1)^2\right)$$
$$=O\left(\frac{M^2}{\sqrt{p}}\cdot\ \ln^2\ p\right)+O\left(p\cdot\ \ln^2\ p\right). \tag{22}$$

This proves Lemma 4. □

3. Proofs of the Theorems

In this section, we shall complete the proofs of our main results. First, we prove Theorem 1. From the definition of $C(p,p)$, Lemma 1, and the properties of the complete residue system modulo p, we have the identity

$$\begin{aligned}
C(p,p)&=\frac{\phi^3(p-1)}{(p-\ 1)^3}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{r=1}^{h}{}'e\left(\frac{r\cdot\mathrm{ind}\left(4a^2-(2b-1)^2\right)}{h}\right)\\
&\quad\times\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{t=1}^{k}{}'e\left(\frac{t\cdot\mathrm{ind}\left(4a(2b-1)\right)}{k}\right)\\
&\quad\times\sum_{s|p-1}\frac{\mu(s)}{\phi(s)}\sum_{u=1}^{s}{}'e\left(\frac{u\cdot\mathrm{ind}\left(4a^2+(2b-1)^2\right)}{s}\right)\\
&=\frac{\phi^3(p-1)}{(p-\ 1)^3}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{s|p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\quad\times\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{r,h}\left(4a^2-(2b-1)^2\right)\chi_{t,k}\left(4a(2b-1)\right)\chi_{u,s}\left(4a^2+(2b-1)^2\right)\\
&=\frac{\phi^3(p-1)}{(p-\ 1)^3}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{s|p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\quad\times\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\chi_{r,h}\left(4a^2-(2b-1)^2\right)\chi_{t,k}\left(4a(2b-1)\right)\chi_{u,s}\left(4a^2+(2b-1)^2\right)\\
&\quad-\frac{\phi^3(p-1)}{(p-\ 1)^3}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{s|p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\quad\times\sum_{a=1}^{p-1}\chi_{r,h}\left(4a^2-1\right)\chi_{t,k}(-4a)\chi_{u,s}\left(4a^2+1\right)\\
&=\frac{\phi^3(p-1)}{(p-\ 1)^3}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{s|p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\quad\times\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{r,h}\left(4a^2-b^2\right)\chi_{t,k}(4ab)\chi_{u,s}\left(4a^2+b^2\right)\\
&\quad-\frac{\phi^3(p-1)}{(p-\ 1)^3}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{s|p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\quad\times\sum_{a=1}^{p-1}\chi_{r,h}\left(4a^2-1\right)\chi_{t,k}(-4a)\chi_{u,s}\left(4a^2+1\right),
\end{aligned} \tag{23}$$

where $\chi_{t,k}(a) = e(t \cdot \mathrm{ind}(a)/k)$ denotes a Dirichlet character modulo p.

If $\chi_{r,h} = \chi_{t,k} = \chi_{u,s} = \chi_0$ is the principal character modulo p, then we have

$$\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_0\left(4a^2-b^2\right)\chi_0(4ab)\chi_0\left(4a^2+b^2\right) = (p-1)^2 + O(p). \tag{24}$$

If one of $\chi_{r,h}$, $\chi_{t,k}$, or $\chi_{u,s}$ is a nonprincipal character modulo p, then from Lemma 3 and the properties of the reduced residue system modulo p, we have

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{r,h}\left(4a^2-b^2\right)\chi_{t,k}(4ab)\chi_{u,s}\left(4a^2+b^2\right)\\
&\quad=\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{r,h}\left(4(ab)^2-b^2\right)\chi_{t,k}(4(ab)b)\chi_{u,s}\left(4(ab)^2+b^2\right)\\
&\quad=\sum_{a=1}^{p-1}\chi_{r,h}\left(4a^2-1\right)\chi_{t,k}(4a)\chi_{u,s}\left(4a^2+1\right)\sum_{b=1}^{p-1}\chi_{r,h}^2(b)\chi_{t,k}^2(b)\chi_{u,s}^2(b)\\
&\quad=O\left(p\cdot\left|\sum_{a=1}^{p-1}\chi_{r,h}\left(4a^2-1\right)\chi_{t,k}(4a)\chi_{u,s}\left(4a^2+1\right)\right|\right)=O\left(p^{3/2}\right).
\end{aligned} \tag{25}$$

Note that the estimate

$$\sum_{k\mid p-1}\left|\frac{\mu(k)}{\phi(k)}\right|\sum_{t=1}^{k}{}'1 = \sum_{k\mid p-1}|\mu(k)| = 2^{\omega(p-1)}, \tag{26}$$

where $\omega(n)$ denotes the number of all distinct prime divisors of n.

From (24) and (25), we have

$$\begin{aligned}
&\frac{\phi^3(p-1)}{(p-1)^3}\sum_{h\mid p-1}\frac{\mu(h)}{\phi(h)}\sum_{k\mid p-1}\frac{\mu(k)}{\phi(k)}\sum_{s\mid p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\qquad\times\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{r,h}\left(4a^2-b^2\right)\chi_{t,k}(4ab)\chi_{u,s}\left(4a^2+b^2\right)\\
&\quad=\frac{\phi^3(p-1)}{p-1}+O\left(\frac{\phi^3(p-1)}{(p-1)^3}\cdot p^{3/2}\cdot\left(\sum_{k\mid p-1}\left|\frac{\mu(k)}{\phi(k)}\right|\sum_{t=1}^{k}{}'1\right)^3\right)\\
&\quad=\frac{\phi^3(p-1)}{p-1}+O\left(\frac{\phi^3(p-1)}{(p-1)^3}\cdot p^{3/2}\cdot 8^{\omega(p-1)}\right).
\end{aligned} \tag{27}$$

$$\begin{aligned}
&\frac{\phi^3(p-1)}{(p-1)^3}\sum_{h\mid p-1}\frac{\mu(h)}{\phi(h)}\sum_{k\mid p-1}\frac{\mu(k)}{\phi(k)}\sum_{s\mid p-1}\frac{\mu(s)}{\phi(s)}\sum_{r=1}^{h}{}'\sum_{t=1}^{k}{}'\sum_{u=1}^{s}{}'\\
&\qquad\times\sum_{a=1}^{p-1}\chi_{r,h}\left(4a^2-1\right)\chi_{t,k}(-4a)\chi_{u,s}\left(4a^2+1\right)\\
&\quad=O\left(\frac{\phi^3(p-1)}{(p-1)^3}\cdot p\cdot 8^{\omega(p-1)}\right).
\end{aligned} \tag{28}$$

Combining (23), (27), and (28), we have the asymptotic formula

$$C(p,p)=\frac{\phi^3(p-1)}{p-1}+O\left(\frac{\phi^3(p-1)}{p^{3/2}}\cdot 8^{\omega(p-1)}\right). \quad (29)$$

This proves Theorem 1.

Similarly, from Lemma 4 and the method of proving Theorem 1, we can also deduce Theorem 2. Details are not given in this study.

4. Conclusion

The main results of this paper are two theorems, which are closely related to Pythagorean triples and primitive roots modulo an odd prime p. It describes that when the prime p is large enough, then there must exist three primitive roots x, y, and z modulo p such that $x^2+y^2=z^2$. At the same time, we also give a sharp asymptotic formula for the counting function of all such solutions (x,y,z). Of course, our conclusion can also be generalized to other special integer sets, such as D. H. Lehmer numbers and k-th residue modulo p.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

Authors' Contributions

The author contributed to the work and read and approved the final manuscript.

Acknowledgments

This work was supported by the NSF of China (11862018) and NSF of Inner Mongolia of China (2017BS0101).

References

[1] W. P. Zhang and H. L. Li, *Elementary Number Theory*, Shaanxi Normal University Press, Xi'an, Shaanxi, China, 2013.

[2] Q. Sun, "On primitive roots in a finite field," *Journal of Sichuan University*, vol. 25, pp. 133–139, 1988.

[3] T. Tian and W. Qi, "Primitive normal element and its inverse in finite fields," *Acta Mathematica Sinica*, vol. 49, pp. 657–668, 2006.

[4] J. P. Wang, "On Golomb's conjecture," *Science in China*, vol. 9, pp. 927–935, 1987.

[5] T. T. Wang and X. N. Wang, "On the Golomb's conjecture and Lehmer's numbers," *Open Mathematics*, vol. 15, pp. 1003–1009, 2017.

[6] W. P. Zhang, "On a problem related to Golomb's conjectures," *Journal of Systems Science and Complexity*, vol. 16, pp. 13–18, 2003.

[7] S. Cohen and W. P. Zhang, "Sums of two exact powers," *Finite Fields and Their Applications*, vol. 8, no. 4, pp. 471–477, 2002.

[8] S. D. Cohen, "Pairs of primitive roots," *Mathematika*, vol. 32, no. 2, pp. 276–285, 1985.

[9] S. D. Cohen and T. Trudgian, "Lehmer numbers and primitive roots modulo a prime," *Journal of Number Theory*, vol. 203, pp. 68–79, 2019.

[10] Y. Y. Liu and W. P. Zhang, "The linear recurrence formula of the hybrid power mean involving the cubic Gauss sums and two-term exponential sums," *Journal of Shaanxi Normal University*, vol. 45, pp. 14–17, 2017.

[11] Y. W. Hou and W. P. Zhang, "One kind high dimensional Kloosterman sums and its upper bound estimate," *Journal of Shaanxi Normal University (Natural Science Edition)*, vol. 46, pp. 28–31, 2018.

[12] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, NY, USA, 1976.

[13] W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientifc Publishers, Warsaw, Poland, 1986.

[14] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, "On the hidden shifted power problem," *SIAM Journal on Computing*, vol. 41, no. 6, pp. 1524–1557, 2012.

[15] K. Gong and C. Jia, "Shifted character sums with multiplicative coefficients," *Journal of Number Theory*, vol. 153, pp. 364–371, 2015.