Mathematics

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

AIMS Mathematics, 7(1): 957–966.
DOI:10.3934/math.2022057
Received: 06 July 2021
Accepted: 18 September 2021
Published: 19 October 2021

Research article

Pythagorean triples and quadratic residues modulo an odd prime

Jiayuan Hu[1,*] **and Yu Zhan**[2]

[1] Department of Mathematics and Computer Science, Hetao College, Bayannur 015000, China

[2] Department of Civil Engineering, Hetao College, Bayannur 015000, China

* **Correspondence:** Email: hujiayuan1986@163.com.

Abstract: In this article, we use the elementary methods and the estimate for character sums to study a problem related to quadratic residues and the Pythagorean triples, and prove the following result. Let p be an odd prime large enough. Then for any positive number $0 < \epsilon < 1$, there must exist three quadratic residues x, y and z modulo p with $1 \leq x,\ y,\ z \leq p^{1+\epsilon}$ such that the equation $x^2 + y^2 = z^2$.

Keywords: quadratic residue; Pythagorean triples; the estimate for character sums; asymptotic formula
Mathematics Subject Classification: 11A15, 11D09

1. Introduction

For any three positive integers x, y and z, if they satisfy the equation $x^2 + y^2 = z^2$, then we call (x, y, z) is a Pythagorean triple. In other words, with these three integers as sides, we can form a right triangle. So sometimes, we call (x, y, z) as a set of Pythagorean numbers. For example, $(x, y, x) = (3, 4, 5)$, $(5, 12, 13)$ are two Pythagorean triples. It is well known that all positive integer solutions of the equation $x^2 + y^2 = z^2$ are $x = t\left(a^2 - b^2\right)$, $y = 2tab$, $z = t\left(a^2 + b^2\right)$, where t, a and b, are arbitrary positive integers such that $a > b$, a and b have no prime divisors in common, and one of a or b is odd, the other even. This result can be found in many elementary number theory textbooks, e.g. [3, Theorems 2–9], the proof will not be repeated here.

On the other hand, let p be a fixed odd prime, and a is an integer with $(a, p) = 1$. If the congruence equation $x^2 \equiv a \bmod p$ has the solution, then we call a is a quadratic residue modulo p. Otherwise, we call a is a quadratic non-residue modulo p. For the various properties of quadratic residues modulo p, refer to [1]. It is worth mentioning that Legendre has made an important contribution to the research in this field, and he firstly introduced the characteristic function of quadratic residue, called Legendre's symbol. Let $p \geq 3$ be a prime. For any integer n, the Legendre's symbol $\left(\frac{n}{p}\right)$ modulo p is defined as following.

$$\left(\frac{n}{p}\right)=\begin{cases}1 & \text{if } (n,p)=1 \text{ and } n \text{ is a quadratic residue modulo } p,\\ -1 & \text{if } (n,p)=1 \text{ and } n \text{ is a quadratic non-residue modulo } p,\\ 0 & \text{if } p \mid n.\end{cases}$$

In fact, this function occupies a very important position in elementary number theory and analytic number theory, many classical number theory problems are closely related to it. For example, if p is an odd prime with $p \equiv 1 \bmod 4$, then one has the identity (See [3, Theorems 4–11]).

$$p=\left(\frac{1}{2}\sum_{a=1}^{p-1}\left(\frac{a+r\overline{a}}{p}\right)\right)^2+\left(\frac{1}{2}\sum_{b=1}^{p-1}\left(\frac{b+s\overline{b}}{p}\right)\right)^2,$$

where r and s are any integers with $\left(\frac{r}{p}\right)\cdot\left(\frac{s}{p}\right)=-1$, and $a\overline{a}\equiv 1 \bmod p$.

Of course, the smallest quadratic non-residue, the formula for class number in the quadratic field, and the prime distribution are all closely related to Legendre's symbol modulo p.

In addition, Legendre's symbol has many important properties, such as the quadratic reciprocity law. That is, for any two odd primes p and q with $p \neq q$, we have the identity (see [1, Theorem 9.8]).

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

The main reason why this paper mentioned Pythagorean numbers and quadratic residues is related to a conjecture proposed by Professor Z. W. Sun. In 2015, Z. W. Sun [12] proposed the following conjecture and checked with mathematical software.

Conjecture. For any prime $p > 50$, there must exist a Pythagorean triple (x, y, z) with $1 \leq x, y, z \leq p-1$ such that

$$\left(\frac{x}{p}\right)=\left(\frac{y}{p}\right)=\left(\frac{z}{p}\right)=1.$$

About this problem,it seems that there is still no one made any substantial progress up to now. At least we do not see it in the existing literature. This problem is very interesting, it is actually dealing with the quadratic residue problem in some special set of integers. Although we can not prove this conjecture at present, we can get some results that are conducive to the correctness of the conjecture. For convenience, we only consider the Pythagorean triples in the following special form:

$$(x,y,z)=\left(4a^2-(2b-1)^2, 4a(2b-1), 4a^2+(2b-1)^2\right), \tag{1.1}$$

where a and b are any positive integers.

Now we let $i,\ j,\ k=\pm 1$. A natural problem is that for any odd prime p and integer $1 < M < p$, whether there is a Pythagorean triple (x, y, z) in (1.1) with $1 \leq a,\ b \leq M$, such that

$$\left(\frac{x}{p}\right)=i,\ \left(\frac{y}{p}\right)=j \text{ and } \left(\frac{z}{p}\right)=k.$$

If there is such a Pythagorean triple (x, y, z), let $W(M, p, i, j, k)$ denote the number of all such Pythagorean triples (x, y, z) in (1.1) with $1 \leq a,\ b \leq M$. Then how about the asymptotic properties of $W(M, p, i, j, k)$?

In this paper, we will use the elementary and analytic methods, and the estimate for character sums to study this problem, and obtain a sharp asymptotic formula for $W(M, p, i, j, k)$. That is, we will prove the following:

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

$$W(p, p, i, j, k) = \frac{1}{8} \cdot p^2 + O\left(p^{\frac{3}{2}}\right).$$

Theorem 2. Let p be an odd prime. Then for any integer $1 < M \leq p$, we have the asymptotic formula

$$W(M, p, i, j, k) = \frac{1}{8} \cdot M^2 + O\left(M \cdot p^{\frac{1}{2}} \cdot \ln^2 p\right).$$

Taking $i = j = k = 1$, from our theorems we may immediately deduce the following two corollaries.

Corollary 1. Let p be a prime large enough. Then for any positive number $\epsilon > 0$, there must exist three quadratic residues x, y and z modulo p with $1 \leq x,\ y,\ z \leq p^{1+\epsilon}$ satisfying the equation

$$x^2 + y^2 = z^2.$$

Corollary 2. Let p be a prime large enough. Then there must exist three elements x, y and z in the finite field $\mathbb{F}_p$ satisfying the equation

$$x^4 + y^4 = z^4.$$

Some notes It is clear that our conclusions can also be extended to any k-th residue modulo p, where $k \geq 2$ and $k \mid (p-1)$. That is, let p be an odd prime, k be any fixed positive integer with $k \mid (p-1)$. For any positive number $1 \leq M \leq p-1$, let $H(M, p)$ denotes the number of all solutions in (1.1) with $1 \leq a,\ b \leq M$ such that $x,\ y,\ z$ are k-th residues modulo p. Then we have the asymptotic formula

$$H(M, p) = \frac{1}{k^3} \cdot M^2 + O\left(M \cdot p^{\frac{1}{2}} \cdot \ln^2 p\right).$$

For any positive number $0 < \epsilon < 1$, there must exist three k-th residues x, y and z modulo p with $1 \leq x,\ y,\ z \leq p^{1+\epsilon}$ such that the equation

$$x^2 + y^2 = z^2.$$

2. Several lemmas

To complete the proofs of our main results, we need following three simple lemmas. For the sake of simplicity, we do not repeat some elementary results of number theory and analytic number theory, which can be found in references [1–3]. Some papers related to character sums and exponential sums can also be found in [4–8], we do not want to repeat that here. Firstly, we have the following lemma.

Lemma 1. Let p be an odd prime, χ a d-th character modulo p, and $f(x)$ an integral coefficient polynomial, which is not a perfect d-th power. Then for any integer n, we have the estimate

$$\sum_{a=0}^{p-1} \chi\left(f(a)\right) e\left(\frac{an}{p}\right) \leq s \cdot p^{\frac{1}{2}},$$

where $e(x) = e^{2\pi i x}$ and s is the number of all distinct integer roots of $f(x)$.

Proof. For this see [9]. Some related work can also be found in [10, 11].

Lemma 2. Let p be an odd prime, $\chi_2 = \left(\frac{*}{p}\right)$ denotes the Legendre's symbol modulo p. Then we have the estimate

$$\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_2\left(4a^2+(2b-1)^2\right) = O\left(p^{\frac{3}{2}}\right).$$

Proof. From the properties of the complete residue system modulo p and Lemma 1 we have

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_2\left(4a^2+(2b-1)^2\right)\\
= &\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\chi_2\left(4a(2b-1)\right)\chi_2\left(4a^2+(2b-1)^2\right)\\
&-\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2\left(-4a\right)\chi_2\left(4a^2+1\right)\\
= &\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-b^2\right)\chi_2\left(4ab\right)\chi_2\left(4a^2+b^2\right)\\
&-\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(-4a)\chi_2\left(4a^2+1\right)\\
= &(p-1)\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2\left(4a\right)\chi_2\left(4a^2+1\right)\\
&-\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(-4a)\chi_2\left(4a^2+1\right) = O\left(p^{\frac{3}{2}}\right).
\end{aligned}$$

This proves Lemma 2.

Lemma 3. Let p be an odd prime and M an integer with $1 < M < p$. Then we have the estimate

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

Proof. For any integer n, from the trigonometric identity

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

we have

$$\sum_{a=1}^{M}\sum_{b=1}^{M}\chi_2\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)$$

$$
\begin{aligned}
&= \frac{1}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} e\left(\frac{r(a-c)}{p}\right) e\left(\frac{s(b-d)}{p}\right)\\
&\quad \times\chi_2\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)\\
&= \frac{M^2}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)\\
&\quad +\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\\
&\quad \times\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right) e\left(\frac{r(a-c)}{p}\right)\\
&\quad +\frac{M}{p^2}\sum_{s=1}^{p-1}\sum_{d=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\\
&\quad \times\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right) e\left(\frac{s(b-d)}{p}\right)\\
&\quad +\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M} e\left(\frac{r(a-c)}{p}\right) e\left(\frac{s(b-d)}{p}\right)\\
&\quad \times\chi_2\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)\\
&= U_1+U_2+U_3+U_4. \qquad (2.1)
\end{aligned}
$$

From Lemma 2 we have

$$
\begin{aligned}
U_1 &= \frac{M^2}{p^2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)\\
&= O\left(\frac{M^2}{p^2}\cdot p^{\frac{3}{2}}\right) = O\left(\frac{M^2}{\sqrt{p}}\right). \qquad (2.2)
\end{aligned}
$$

From the estimate

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

the method of proving (2.2) and the properties of Gauss sums we have

$$
\begin{aligned}
U_2 = \frac{M}{p^2}&\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\\
&\times\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right) e\left(\frac{r(a-c)}{p}\right)\\
= \ &\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-b^2\right)\\
&\times\chi_2(4ab)\chi_2\left(4a^2+b^2\right) e\left(\frac{r(a-c)}{p}\right)
\end{aligned}
$$

$$
\begin{aligned}
& -\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(-4a)\chi_2\left(4a^2+1\right)e\left(\frac{r(a-c)}{p}\right)\\
= \;& \frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(4a)\chi_2\left(4a^2+1\right)\\
& \times\sum_{b=1}^{p-1}\chi_2\left(b^2\right)\chi_2(b^2)\chi_2\left(b^2\right)e\left(\frac{rab}{p}\right)\sum_{c=1}^{M}e\left(\frac{-rc}{p}\right)\\
& -\frac{M}{p^2}\sum_{r=1}^{p-1}\sum_{c=1}^{M}\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(-4a)\chi_2\left(4a^2+1\right)e\left(\frac{r(a-c)}{p}\right)\\
\ll \;& \frac{M}{p^2}\sum_{r=1}^{p-1}\left|\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(4a)\chi_2\left(4a^2+1\right)\right|\cdot\frac{1}{\left|\sin\left(\frac{\pi r}{p}\right)\right|}\\
& +\frac{M}{p^2}\sum_{r=1}^{p-1}\left|\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(4a)\chi_2\left(4a^2+1\right)e\left(\frac{ra}{p}\right)\right|\cdot\frac{1}{\left|\sin\left(\frac{\pi r}{p}\right)\right|}\\
\ll \;& \frac{M}{\sqrt{p}}\sum_{r=1}^{p-1}\frac{1}{r}\ll\frac{M}{\sqrt{p}}\cdot\ln p. \qquad (2.3)
\end{aligned}
$$

Similarly, we also have the estimate

$$
\begin{aligned}
U_3 = \frac{M}{p^2}&\sum_{s=1}^{p-1}\sum_{d=1}^{M}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_2\left(4a^2-(2b-1)^2\right)\\
&\times\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)e\left(\frac{s(b-d)}{p}\right)\\
= \;& \frac{M}{p^2}\sum_{s=1}^{p-1}\sum_{d=1}^{M}\sum_{a=1}^{p-1}\chi_2\left(4a^2-1\right)\chi_2(4a)\chi_2\left(4a^2+1\right)e\left(\frac{-sd}{p}\right)\\
&\times\sum_{b=1}^{p-1}\chi_2^2(2b-1)\chi_2^2(2b-1)\chi_2^2(2b-1)e\left(\frac{\overline{2}s(2b-1+1)}{p}\right)\\
\ll \;& \frac{M}{p^{\frac{3}{2}}}\sum_{s=1}^{p-1}\frac{1}{\left|\sin\left(\frac{\pi s}{p}\right)\right|}\ll\frac{M}{\sqrt{p}}\cdot\ln p \qquad (2.4)
\end{aligned}
$$

and

$$
\begin{aligned}
U_4 = \frac{1}{p^2}&\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{r(a-c)}{p}\right)e\left(\frac{s(b-d)}{p}\right)\\
&\times\chi_2\left(4a^2-(2b-1)^2\right)\chi_2(4a(2b-1))\chi_2\left(4a^2+(2b-1)^2\right)\\
&-\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M}e\left(\frac{r(a-c)}{p}\right)e\left(\frac{-sd}{p}\right)
\end{aligned}
$$

$$
\begin{aligned}
& \times\chi_2\left(4a^2-1\right)\chi_2(-4a)\chi_2\left(4a^2+1\right) \\
= \; & \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M} e\left(\frac{r(a-c)}{p}\right)e\left(\frac{\overline{2}s(b+1-2d)}{p}\right) \\
& \times\chi_2\left(4a^2-b^2\right)\chi_2(4ab)\chi_2\left(4a^2+b^2\right)+O\left(p^{\frac{1}{2}}\cdot\ln^2 p\right) \\
= \; & \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M} e\left(\frac{r(ab-c)}{p}\right)e\left(\frac{\overline{2}s(b+1-2d)}{p}\right) \\
& \times\chi_2\left(4a^2-1\right)\chi_2(4a)\chi_2\left(4a^2+1\right)\chi_2^2(b)\chi_2^2(b)\chi_2^2(b)+O\left(p^{\frac{1}{2}}\cdot\ln^2 p\right) \\
= \; & \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\sum_{a=1}^{p-1}\sum_{c=1}^{M}\sum_{d=1}^{M} e\left(\frac{-rc}{p}\right)e\left(\frac{\overline{2}s(1-2d)}{p}\right) \\
& \times\chi_2\left(4a^2-1\right)\chi_2(4a)\chi_2\left(4a^2+1\right)\sum_{b=1}^{p-1} e\left(\frac{b(ra+\overline{2}s)}{p}\right)+O\left(p^{\frac{1}{2}}\cdot\ln^2 p\right) \\
= \; & O\left(\frac{\sqrt{p}}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\left|\sin\left(\frac{\pi r}{p}\right)\right|}\cdot\frac{1}{\left|\sin\left(\frac{\pi s}{p}\right)\right|}\right)+O\left(\sqrt{p}\cdot M\cdot\ln p\right) \\
= \; & O\left(p^{\frac{1}{2}}\cdot\ln^2 p\right)+O\left(M\cdot p^{\frac{1}{2}}\cdot\ln p\right). \qquad (2.5)
\end{aligned}
$$

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

Combining (2.1)–(2.5) we have the estimate

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

This proves Lemma 3.

Some notes: If we take $M = p$ in Lemma 3, then the estimate is significantly weaker than Lemma 2. This is because when $M < p$, we can not directly apply the properties of the complete (or reduced) residue system modulo p. And to do that, we use trigonometric sums to convert the sums $1 \le a \le M$ to $1 \le a \le p$. In this way, some extra error terms are generated in the conversion process.

3. Proofs of the theorems

Now we prove Theorem 1. If $i = \pm 1$, then for integer x with $(x, p) = 1$, note that

$$
\left(\frac{x}{p}\right)=i \text{ if and only if } \frac{1}{2}\left(1+i\left(\frac{x}{p}\right)\right)=1.
$$

So from the definition of $W(p, p, i, j, k)$ and the properties of Legendre's symbol modulo p we have the estimate

$$
W(p,p,i,j,k) \;=\; \frac{1}{8}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(1+i\left(\frac{4a^2-(2b-1)^2}{p}\right)\right)\left(1+j\left(\frac{4a(2b-1)}{p}\right)\right)
$$

$$\times\left(1+k\left(\frac{4a^2+(2b-1)^2}{p}\right)\right)+O(p), \tag{3.1}$$

where the big-O term $O(p)$ comes from $p \mid \left(4a^2-(2b-1)^2\right)$ and $p \mid \left(4a^2+(2b-1)^2\right)$.

For any integer c with $(c,p)=1$, note that the identity

$$\sum_{a=0}^{p-1}\left(\frac{a^2+c}{p}\right)=\chi_2(c)+\sum_{a=1}^{p-1}(1+\chi_2(a))\chi_2(a+c)=\sum_{a=1}^{p-1}\chi_2(1+ca)=-1.$$

From the properties of the complete residue system modulo p and Lemma 2 we have

$$\begin{aligned}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{4a^2-(2b-1)^2}{p}\right)&=\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\left(\frac{4a^2-b^2}{p}\right)-\sum_{a=1}^{p-1}\left(\frac{4a^2-1}{p}\right)\\ =\ (p-1)\sum_{a=1}^{p-1}\left(\frac{a^2-1}{p}\right)+p-1-\sum_{a=1}^{p-1}\left(\frac{a^2-1}{p}\right)&=O(p). \end{aligned}\tag{3.2}$$

$$\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{4a(2b-1)}{p}\right)=O(1). \tag{3.3}$$

$$\begin{aligned}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{4a^2+(2b-1)^2}{p}\right)&=\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\left(\frac{4a^2+b^2}{p}\right)-\sum_{a=1}^{p-1}\left(\frac{4a^2+1}{p}\right)\\ =\ (p-1)\sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)+p-1-\sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)&=O(p). \end{aligned}\tag{3.4}$$

From Lemma 1 we also have

$$\begin{aligned}&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{4a^2-(2b-1)^2}{p}\right)\left(\frac{4a(2b-1)}{p}\right)\\ =\ &\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{a^2-b^2}{p}\right)\left(\frac{2ab}{p}\right)-\sum_{a=1}^{p-1}\left(\frac{4a^2-1}{p}\right)\left(\frac{-4a}{p}\right)\\ =\ &(p-1)\sum_{a=1}^{p-1}\left(\frac{a^2-1}{p}\right)\left(\frac{2a}{p}\right)-\sum_{a=1}^{p-1}\left(\frac{a^2-1}{p}\right)\left(\frac{-2a}{p}\right)=O\left(p^{\frac{3}{2}}\right).\end{aligned}\tag{3.5}$$

$$\begin{aligned}&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{4a^2+(2b-1)^2}{p}\right)\left(\frac{4a(2b-1)}{p}\right)\\ =\ &\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{a^2+b^2}{p}\right)\left(\frac{2ab}{p}\right)-\sum_{a=1}^{p-1}\left(\frac{4a^2+1}{p}\right)\left(\frac{-4a}{p}\right)\end{aligned}$$

$$= (p-1)\sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)\left(\frac{2a}{p}\right) - \sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)\left(\frac{-2a}{p}\right) = O\left(p^{\frac{3}{2}}\right). \tag{3.6}$$

$$\begin{aligned}&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{4a^2+(2b-1)^2}{p}\right)\left(\frac{4a^2-(2b-1)^2}{p}\right)\\ = &\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\left(\frac{a^2+b^2}{p}\right)\left(\frac{a^2-b^2}{p}\right) - \sum_{a=1}^{p-1}\left(\frac{4a^2+1}{p}\right)\left(\frac{4a^2-1}{p}\right)\\ = &(p-2)\sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)\left(\frac{a^2-1}{p}\right) + (p-1) = O\left(p^{\frac{3}{2}}\right).\end{aligned} \tag{3.7}$$

Now combining (3.1)–(3.7) and Lemma 2 we have the asymptotic formula

$$W(p,p,i,j,k) = \frac{1}{8}\cdot p^2 + O\left(p^{\frac{3}{2}}\right).$$

This proves Theorem 1.

Now we prove Theorem 2. In fact from the definition of $W(M,p,i,j,k)$ we also have

$$\begin{aligned}W(M,p,i,j,k) &= \frac{1}{8}\sum_{a=1}^{M}\sum_{b=1}^{M}\left(1+i\left(\frac{4a^2-(2b-1)^2}{p}\right)\right)\left(1+j\left(\frac{4a(2b-1)}{p}\right)\right)\\ &\quad\times\left(1+k\left(\frac{4a^2+(2b-1)^2}{p}\right)\right) + O(M).\end{aligned} \tag{3.8}$$

From Lemma 3 and the methods of proving Theorem 1 we can easily deduce the asymptotic formula

$$W(M,p,i,j,k) = \frac{1}{8}\cdot M^2 + O\left(M\cdot p^{\frac{1}{2}}\cdot \ln^2 p\right).$$

This proves Theorem 2. In order to save the space, details are omitted here.

4. Conclusions

The main results of this paper are two theorems, which are closely related to Pythagorean triples and quadratic residues modulo an odd prime p. It describes that when prime p is large enough, then there must exist three quadratic residues x, y and z modulo p such that the equation $x^2+y^2=z^2$. 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, etc.

Acknowledgments

This work is supported by the N. S. F. (12161031) of China, the N. S. F. (2021MS01003) of Inner Mongolia (CN) and the Number Theory Research Center of Hetao College. The authors would like to thank the referees for their very helpful and detailed comments.

Conflict of interest

The authors declare that there are no conflict of interest regarding the publication of this paper.

References

1. T. M. Apostol, *Introduction to Analytic Number Theory*, New York: Springer-Verlag, 1979.
2. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, New York: Springer-Verlag, 1982.
3. W. P. Zhang, H. L. Li, *Elementary Number Theory*, Xi'an: Shaanxi Normal University Press, 2013.
4. Y. W. Hou, W. P. Zhang, One kind high dimensional Kloosterman sums and its upper bound estimate, *J. Shaanxi Norm. Univ., Nat. Sci. Ed.,* **46** (2018), 28–31. doi: 10.15983/j.cnki.jsnu.2018.05.155.
5. A. Granville, K. Soundararajan, Large character sums: Pretentious characters and the Pólya-Vinogradov theorem, *J. Amer. Math. Soc.,* **20** (2007), 357–384. doi: 10.1090/S0894-0347-06-00536-4.
6. W. P. Zhang, Y. Yi, On Dirichlet characters of polynomials, *Bull. London Math. Soc.,* **34** (2002), 469–473. doi: 10.1112/S0024609302001030.
7. W. P. Zhang, W. L. Yao, A note on the Dirichlet characters of polynomials, *J. Acta Arithmetica,* **115** (2004), 225–229. doi: 10.4064/aa115-3-3.
8. A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.,* **34** (1948), 204–207. doi: 10.1073/pnas.34.5.204.
9. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: measure of pseudorandomness, the Legendre symbol, *Acta Arithmetica,* **82** (1997), 365–377.
10. K. Gong, C. H. Jia, Shifted character sums with multiplicative coefficients, *J. Number Theory,* **153** (2015), 364–371. doi: 10.1016/j.jnt.2015.01.015.
11. J. Bourgain, M. Z. Garaev, S. V. Konyagin, I. E. Shparlinski, On the hidden shifted power problem, *SIAM J. Comput.,* **41** (2012), 1524–1557. doi: 10.1137/110850414.
12. Z. W. Sun, Sequence A260911 at OEIS, 2015. Available from: http://oeis.org/A260911.