Some Studies on Quadratic Diophantine Equations

Author: Bangzheng Li
Advisor Teacher:
Affiliated High School of Renmin University of China
Grade 9

Introduction

The integer(or radical) solution to a Quadratic Diophantine Equations is an antique problem, in the ancient time, people began to study the integer solution to the equation $\mathrm{x}^2+\mathrm{y}^2=\mathrm{z}^2$. By studying this problem, Gauss found some theorems, such as quadratic reciprocity law. And Hasse-Minkowski Theorem[5] solved the more general case of the existence of integer solution of a quadratic form.

This article is a generalization to a problem in one exam of The High School Affiliated to Renmin University of China: $x^2+xy+y^2=15z^2$. This article is divided into 2 parts:

1, This article studies the quadratic diophantine equation $x^2+xy+y^2=az^2$ where *x,y,z* are unknowns, and *a* is a given integer. We give an equivalent condition on *a* to the existence(and infinitely) non-trivial solution of that equation. Due to the Hasse-Minkowski Theorem, this section is an effective attempt to these forms.

2, Put $\mathrm{Z}[\mathrm{w}(\mathrm{q})]$ is all algebraic integer in $Q(\sqrt{-q})$ where

$$w(q)=\begin{cases}\dfrac{1+\sqrt{-q}}{2},\ \mathrm{q}\equiv 3(\mathrm{mod}\ 4),\\ \\ \sqrt{\mathrm{-q}},\ \mathrm{q}\equiv 1\text{,}2(\mathrm{mod}\ 4).\end{cases}$$

Through the analogue of $x^2+qy^2=p$, we use the elementary method to find a necessary condition to check whether $\mathrm{Z}[\mathrm{w}(\mathrm{q})]$ is UFD:

$\mathrm{Z}[\mathrm{w}(\mathrm{q})]$ is UFD, then $q+x^2$ is prime for all even $x^2<q(\frac{q}{16}-1)$ and $\frac{q+x^2}{4}$ is prime for all odd $x^2<q(\frac{q}{4}-1)$ (1)

Although we don't prove (1) is an equivalent condition to check whether $\mathrm{Z}[\mathrm{w}(\mathrm{q})]$ is UFD, after calculating in Mathematica, (1) is an equivalent condition for $\mathrm{q}\le 10^8$.

1. Integer Solutions for Bivariate Cubic Equations $x^2+xy+y^2=az^2$

Here the problem of integer solutions for equation in the form of

$$x^2+xy+y^2=az^2 \tag{1.1}$$

is studied. The problem is stated as, which type of integers the variable a should be, so that Equation (1.1) has solutions? And which type of integers of a so that

Equation (1) only has trivial solution $(0,0,0)$?

First it is noticed that, if a has a perfect square factor h^2, then Equation (1.1) could be rewritten as,

$$x^2 + xy + y^2 = \left(\frac{a}{h^2}\right)(hz)^2 \ , \tag{1.2}$$

so that the study for integer solutions of Equation (1.1), is equivalent to the integer solutions of Equation (1.2). Thus, the only case that needs to be studied is when parameter a has no perfect square factors.

In the following discussions, without loss of generality, we assume that parameter a in Equation (1.1) has no perfect square factors.

1.1. When $\mathbf{a = p \equiv 5(\mathrm{mod}\ 6)}$ is prime (1.1) has no non-trivial integer solution

Theorem 1.1: When a is equal to a prime p, and $p \equiv 5(mod\ 6)$, then Equation (1.1) only has a trivial solution $(0,0,0)$.

From now on, $(\frac{a}{p})$stands for the Legendre Symbol in the law of quadratic reciprocity.

Proof.

We have

$$az^2 \equiv 0(\mathrm{mod}\ \ p).$$

Rewrite Equation (1.1) to,

$$x^2 + xy + y^2 \equiv 0(mod\ p) \text{=>} (2x + y)^2 \equiv -3y^2(mod\ p). \tag{1.3}$$

If $y \not\equiv 0(mod\ p)$, then $(y, p) = 1$,

Thus (1.3) becomes,

$$((2x + y)\mathrm{y}^{-1})^2 \equiv -3(mod\ p).$$

Using the law of quadratic reciprocity to get,

$$\left(\frac{-3}{P}\right) = \left(\frac{-1}{\mathrm{p}}\right)\left(\frac{3}{\mathrm{p}}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{P-1}{2}}(-1)^{\frac{P-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right)$$

$$=(-1)^{P-1}\left(\frac{P}{3}\right) = \left(\frac{P}{3}\right)$$

$$=\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

So that -3 is not a quadratic residue modulo p, and we can obtain the contradiction。

Thus

$$y \equiv 0(mod\ p) \text{=>}\ 2x + y \equiv 0(mod\ p) \text{=>}\ 2x \equiv 0(mod\ p) \text{=>}\ x \equiv 0(mod\ p)$$

Suppose (x_0, y_0, z_0) is one non-trivial integer solution for Equation (1.1), and $|\mathrm{z}_0|$

is taken to be the minimum (|Ω| stands for the absolute value of Ω), then $x_0 = x_1 p$ $y_0 = y_1 p$, where x_1, y_1 are all integers.

Equation (1.1) could be rewritten as,

$$({x_1}^2 + x_1 y_1 + {y_1}^2)\mathrm{p}^2 = p{z_0}^2. \tag{1.4}$$

Divided by p from both sides, to get

$$({x_1}^2 + x_1 y_1 + {y_1}^2)\mathrm{p} = {z_0}^2. \tag{1.5}$$

In Equation (1.5)，we have $\mathrm{p} \mid \mathrm{z}_0$.

Let $\mathrm{z}_0 = \mathrm{z}_1\mathrm{p}$，then (1.5) becomes

$$({x_1}^2 + x_1 y_1 + {y_1}^2) = p{z_1}^2. \tag{1.6}$$

Since $a = p$, (1.6) becomes

$$({x_1}^2 + x_1 y_1 + {y_1}^2) = a{z_1}^2. \tag{1.7}$$

Thus (x_1, y_1, z_1) is also a non-trivial solution for Equation (1.1), and $|z_1| < |z_0|$, contradiction. So that Equation (1.1) only has trivial solution (0,0,0) when a is a prime p, and $p \equiv 5(\mathrm{mod}\ 6)$.

1.2 When $a = p$ and p is prime， $p \equiv 1(\mathrm{mod}\ 6)$，Equation（1.1）has non-trivial integer solutions.

Lemma 1.1: If prime number $\boldsymbol{p}$ satisfies $p \equiv 1(\mathrm{mod}\ 6)$, then there exists integer m, n, such that $\mathrm{m}^2 + 3\mathrm{n}^2 = \mathrm{p}$.

Proof.

By the law of quadratic reciprocity,

$$\left(-\frac{3}{P}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{P-1}{2}}(-1)^{\frac{P-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right)$$

$$=(-1)^{P-1}\left(\frac{P}{3}\right) = \left(\frac{P}{3}\right)$$

$$=\left(\frac{1}{3}\right) = 1$$

so that -3 is a quadratic residue modulo p，i.e., there exists integer m，0<m<p，such that

$$m^2 \equiv -3(\mathrm{mod\,p}). \tag{1.8}$$

Since $\left(\frac{1}{P}\right) = 1$, 1 is a quadratic residue modulo p, i.e. there exists integer n，0<n<p，and $\mathrm{n}^2 \equiv 1(\mathrm{mod\,p})$

$$\Rightarrow \quad 3n^2 \equiv 3(\mathrm{mod\,p}). \tag{1.9}$$

Combining Equation (1.8) and (1.9) to get

$$\mathrm{m}^2 + 3\mathrm{n}^2 = 0\ (\mathrm{mod\,p}). \tag{1.10}$$

Thus

$$\mathrm{m}^2 + 3\mathrm{n}^2 = \mathrm{Kp}. \tag{1.11}$$

where K is a positive integer.

Next we prove that K<p.
In fact, choose n=1，so that Equation (1.9) stands.
Then we have,
$m^2 + 3n^2 \leq (p-1)^2 + 3 = p^2 - 2p + 4 < p^2$.
So that there exist positive integer *m，n* so that（1.11）stands，and K<p.
Suppose that K>1

Choose two integers u，v, such that $|u|, |v| \leq \frac{K}{2}$， and $u \equiv m(\mathrm{mod}\,K)$，$v \equiv n(\mathrm{mod}\,K)$
Since p is prime, K ∤ p, and from the following equation

$$u^2 + 3v^2 = m^2 + 3n^2 = 0\text{（mod K）}, \tag{1.12}$$

thus if we set

$$u^2 + 3v^2 = rK. \tag{1.13}$$

where r is a positive integer, next we prove that if $|u|, |v|$ are both equal to $\frac{K}{2}$, then K ＝1.
we have

$$m^2 + 3n^2 \equiv 0(\mathrm{mod}\,K^2). \tag{1.14}$$

Or we can write (1.14) as

$$m^2 + 3n^2 = \alpha K^2, \tag{1.15}$$

where α is a positive integer.
Combining Equation (1.11) and (1.15) to get

$$Kp = \alpha K^2 \Rightarrow p = \alpha K, \tag{1.16}$$

which means that $K|p$，but since p is a prime number，and K<p，so that K=1.

If one of $|u|, |v|$ is smaller than $\frac{K}{2}$, then

$u^2 + 3v^2 < (\frac{K}{2})^2 + 3(\frac{K}{2})^2 = K^2$, so that r<K in Equation (1.13).

Meanwhile,

$$rK^2p = (u^2 + 3v^2)(m^2 + 3n^2) = (um + 3vn)^2 + 3(vm - un)^2. \tag{1.17}$$

But

$$um + 3vn)m^2 + 3n^2 \equiv 3\text{（mod K）},$$

So that

$$K^2|(um + 3vn)^2$$

Because $u \equiv m(\mathrm{mod}\,K)$，$v \equiv n(\mathrm{mod}\,K)$

So that

$$um - vn \equiv uv - vu \equiv 0(\mathrm{mod}\,K). \tag{1.18}$$

Combining Equations (1.17) and (1.18) to get

$$(\frac{um+3vn}{K})^2 + 3(\frac{vm-un}{K})^2 = rp.$$

Because $\frac{\mathrm{um}+3\mathrm{vn}}{\mathrm{K}}=\mathrm{m}'$ is an integer, we know that $\frac{\mathrm{vm}-\mathrm{un}}{\mathrm{K}}=\mathrm{n}'$ must also be an integer, thus

$$\mathrm{m}'^2+3\mathrm{n}'^2=\mathrm{rp},$$

where m', n' are all integers, and r<K. By Fermat's Method of Infinite Descent, the lemma is proved.

Using Lemma 1.1, we know that there exist integers m, n such that $a=p=m^2+3n^2$. if we choose x=n+m, y=n-m, then

$\mathrm{x}^2+\mathrm{xy}+\mathrm{y}^2=\mathrm{m}^2+3\mathrm{n}^2=\mathrm{a}$, and Diophantine equation (1.1) has non-trivial solutions (n+m, n-m, 1).

1.3 When $\mathbf{a}=\mathbf{2}$ or 3

When a=2, it's clear that (1.1) has no non-trivial solutions.
When a=3, set $m=0,n=1$, then we have $m^2+3n^2=a$.
Lemma 1.2: If integers p, q could both be written as the form of $\mathrm{m}^2+3\mathrm{n}^2$, then its multiplication could pq also be written as the form of $\mathrm{m}'^2+3\mathrm{n}'^2$.
Proof.
Let $\mathrm{p}=\mathrm{u}^2+3\mathrm{v}^2$, $\mathrm{q}=\mathrm{m}^2+3\mathrm{n}^2$, then

$$\mathrm{pq}=(\mathrm{u}^2+3\mathrm{v}^2)(\mathrm{m}^2+3\mathrm{n}^2)=(\mathrm{um}+3\mathrm{vn})^2+3(\mathrm{vm}-\mathrm{un})^2. \quad (1.19)$$

That concludes our proof.

Conclusion
Write $\mathbf{a}=\mathbf{c}^2\mathbf{p}_1\mathbf{p}_2\ldots\mathbf{p}_\mathbf{k}$, use the same arguments as equation (1.1), we can get that if $\exists\mathrm{p}_\mathrm{i}\equiv5(\mathrm{mod}\ 6)$, then (1.1) has no non-trivial solutions.
According to equation (1.3), if $\exists\mathrm{p}_\mathrm{i}=2$, then (1.1) has no non-trivial solution.
Conversely, according to equations (1.2) and (1.3), combined with Lemma 1.2, if $\forall\mathrm{p}_\mathrm{i}\equiv1(\mathrm{mod}\ 6)$ or $=3$, then (1.1) has non-trivial solutions.

1.5 If Equation (1.1) has one integer solution, then it has infinite integer solutions

Suppose (a_0,b_0,c_0) is one integer solution for Equation (1.1), then let $ac_0{}^2=\mathrm{q}$

Without loss of generality, suppose

$$a_0{}^2+\mathrm{a}_0\,\mathrm{b}_0+b_0{}^2=\mathrm{q}, \quad (1.19)$$

where $b_0=\frac{1}{2}(-a_0-\sqrt{-3a_0{}^2+4q}$, $b_0=\frac{1}{2}(-a_0+\sqrt{-3a_0{}^2+4q})$.

Suppose x=a, y=b are an arbitrary group of rational solutions for the following equation,

$$x^2+\mathrm{xy}+y^2=\mathrm{q}. \quad (1.20)$$

Let

$b - b_0 = k(a - a_0)$， where k is a rational coefficient.

$$a = \frac{a_0(-1+2k+2k^2)+(1+2k)\sqrt{-3a_0{}^2+4q}}{2(1+k+k^2)}. \tag{1.21}$$

$$b = \frac{-a_0(1+4k+k^2)+(-1+k^2)\sqrt{-3a_0{}^2+4q}}{2(1+k+k^2)} \;. \tag{1.22}$$

Substitute $\sqrt{4q - 3\mathrm{a}_0{}^2} = -2\mathrm{b}_0 - \mathrm{a}_0$ into Equations (1.21), (1.22) to get

$$a = -\frac{a_0+b_0+2b_0k-a_0k^2}{1+k+k^2}, b = \frac{b_0-b_0k^2-a_0k(2+k)}{1+k+k^2}.$$

Since equation (1.1) is quadratic homogeneous equation, we get that

$$a = -a_0 - b_0 - 2b_0k + a_0k^2, b = b_0 - b_0k^2 - a_0k(2+k)$$

are one group of rational solutions for Equation (1.1).

Let $k = m/n$,where m,n are integers without any common factor except 1， then

$$a = -\mathrm{a}_0 - \mathrm{b}_0 + \frac{a_0m^2}{n^2} - \frac{2b_0x}{n}, b = \mathrm{b}_0 - \frac{b_0m^2}{n^2} - \frac{a_0m(2+\frac{m}{n})}{n},$$

Considering the homogeneity of Equation (1.1), we have

$$x = \mathrm{an}^2 = -\mathrm{b}_0 n(2m+n) + \mathrm{a}_0(m^2-n^2),$$
$$y = \mathrm{bn}^2 = -\mathrm{a}_0 n(m+2n) + \mathrm{b}_0(-m^2+n^2),$$
$$z = m^2 + \mathrm{mn} + n^2$$

m， n could take different integer values to generate infinite groups of solutions for Equation (1.1).

The above derivations are done semi-automatically by applying the Wolframe Mathematica software， and the original code is shown below.

Solve[a0^2+a0 b0+b0^2==q,b0]
{{b0->1/2 (-a0-$\sqrt{-3\mathrm{a0}^2+4q}$)},{b0->1/2 (-a0+$\sqrt{-3\mathrm{a0}^2+4q}$)}}

Solve[{b-b0==k(a-a0),a^2+a b+b^2==q}/.%1[[1]],{a,b}]//Simplify
{{a->a0,b->1/2 (-a0-$\sqrt{-3\mathrm{a0}^2+4q}$)},{a->(a0 (-1+2 k+2 k^2)+(1+2 k) $\sqrt{-3\mathrm{a0}^2+4q}$)/(2 (1+k+$k^2$)),b->(-a0 (1+4 k+$k^2$)+(-1+$k^2$) $\sqrt{-3\mathrm{a0}^2+4q}$)/(2 (1+k+$k^2$))}}

Solve[{b-b0==k(a-a0),a^2+a b+b^2==q}/.%1[[2]],{a,b}]//Simplify
{{a->a0,b->1/2 (-a0+$\sqrt{-3\mathrm{a0}^2+4q}$)},{a->(a0 (-1+2 k+2 k^2)-(1+2 k) $\sqrt{-3\mathrm{a0}^2+4q}$)/(2 (1+k+$k^2$)),b->-((a0 (1+4 k+$k^2$)+(-1+$k^2$) $\sqrt{-3\mathrm{a0}^2+4q}$)/(2 (1+k+$k^2$)))}}

%2/.$\sqrt{4q-3\mathrm{a0}^2}$->-2b0-a0//Simplify
{{a->a0,b->b0},{a->-((a0+b0+2 b0 k-a0 k^2)/(1+k+k^2)),b->(b0-b0 k^2-a0 k (2+k))/(1+k+k^2)}}
%3/.$\sqrt{4q-3\mathrm{a0}^2}$->2b0+a0//Simplify
{{a->a0,b->b0},{a->-((a0+b0+2 b0 k-a0 k^2)/(1+k+k^2)),b->(b0-b0 k^2-a0 k (2+k))/(1+k+k^2)}}
%4-%5
{{0,0},{0,0}}

result=%5[[2]]
{a->-((a0+b0+2 b0 k-a0 k^2)/(1+k+k^2)),b->(b0-b0 k^2-a0 k (2+k))/(1+k+k^2)}
{a,b,r}/.{##&@@result,r->1}
{-((a0+b0+2 b0 k-a0 k^2)/(1+k+k^2)),(b0-b0 k^2-a0 k (2+k))/(1+k+k^2),1}
finalresult=%(1+k+k^2)
{-a0-b0-2 b0 k+a0 k^2,b0-b0 k^2-a0 k (2+k),1+k+k^2}

It is known that (a_0, b_0) is one group of solutions for equation $\boldsymbol{x^2} + \mathrm{xy} + \boldsymbol{y^2} = 1$. The function "finalresult" returns infinite groups of solutions, where k is a rational number.

finalresult/.k->x/y
{-a0-b0+(a0 x^2)/y^2-(2 b0 x)/y,b0-(b0 x^2)/y^2-(a0 x (2+x/y))/y,1+x^2/y^2+x/y}

finalxandyresult=y^2 %10//Simplify
{-b0 y (2 x+y)+a0 (x^2-y^2),-a0 x (x+2 y)+b0 (-x^2+y^2),x^2+x y+y^2}

"finalxandyresult" is uses as below: when we choose arbitrary x and y, and initial solution (a_0, b_0), it returns a group of solutions.

2. Study for equations in the form of $\mathbf{p = m^2 + qn^2}$

Here we study the integer solutions for Diophantine equation in the form of

$$ax^2 + \mathrm{b}xy + cy^2 = dz^2. \tag{2.1}$$

According to our discussion in Section 1.1, it could be converted to the problem of studying integer solutions for cases when d has not perfect square factors. In that case, the following linear translation could be used to remove the $\mathrm{b}xy$ term.

$$\mathrm{x} = \alpha\mathrm{x}' + \beta\mathrm{y}$$
$$\mathrm{y} = \mu\mathrm{x} + \tau\mathrm{y}$$

As we discussed in Section 1, this problem could be converted to the following question: If there are integers $\mathrm{m, n}$, such that $\mathrm{rp} = \mathrm{m}^2 + 3\mathrm{n}^2$, then Equation (1.1) has integer solutions.

Then the question is, in general, if $\mathrm{p} = \mathrm{m}^2 + \mathrm{qn}^2$,and p is a prime number or 1， what kind of number q should be? For the case that q is negative, *Disquisitiones Arithmeticae* written by Gauss has done a thorough investigation, especially for the case when $\mathrm{p} = 1$， q is negative, the corresponding equation is called the Pell Equation.

Here we consider the case that q is a positive integer, and p is a prime number. To facilitate our derivations in the next, the following conceptions are introduced.[2]

1. Quadratic integer field: for square-free integer q, $\mathbb{Z}[\mathrm{w(q)}]$ denotes all algebraic integers in $\mathbb{Q}[\sqrt{-q}]$, where $w(q)=\begin{cases}\frac{1+\sqrt{-q}}{2}, & q\equiv 3(\mathrm{mod}\ 4),\\ \sqrt{-q}, & q\equiv 1,2(\mathrm{mod}\ 4).\end{cases}$

2. **Simple field**：on a quadratic integer field, any algebraic number has unique factorization, then this quadratic algebraic domain is called quadratic simple field, simplified as simple field.

3. **Trace and norm:** For any $\alpha\in\mathbb{Z}[w(q)]$， let $\overline{\alpha}$ is the conjugate of complex number α. Then the trace of α is defined as $T_{\sqrt{-q}}(\alpha)=\alpha+\overline{\alpha}$.

The norm of α is defined as, $N_{\sqrt{-q}}(\alpha)=\alpha\overline{\alpha}$.

Let's take $\mathbb{Z}[\sqrt{-5}]$ as an example.

Since $9=3*3=(2+\sqrt{-5})*(2+\sqrt{-5})$, $\mathbb{Z}[\sqrt{-5}]$ is not a simple field.

Let $a,b\in\mathbb{Z},,=a+b\sqrt{-5}\in\mathbb{Z}[w(q)]$, then $\overline{\alpha}=a-b\sqrt{-5}$

and $T_{\sqrt{-5}}(\alpha)=2a$，$N_{\sqrt{-5}}(\alpha)=a^2+5b^2$，$a\pm b\sqrt{-5}$ are two roots for equation $x^2+2ax+a^2+5b^2$=0.

2.1 The study of p=m^2+qn^2 when $\mathbb{Z}[w(q)]$ is a simple field

Let's study the case when $\mathbb{Z}[w(q)]$ is a simple field. First, we should know that $\mathbb{Z}[w(7)]$ is a simple field.

Theorem 2.1： A odd prime number p could be expressed as p=m^2+7n^2 if and only if $\left(-\frac{7}{p}\right)=0$，1, $p\equiv 0$，1，2，4(mod 7)，where m，n are integers.

Proof.

For p<7 this theorem is easily to show. In fact,

Necessity：p=m^2+7n$^2\equiv m^2(\mathrm{mod}7)$, so that $\left(\frac{p}{7}\right)=1$.

Sufficiency:

$$(\frac{-7}{p})=\left(\frac{-1}{p}\right)\left(\frac{7}{p}\right)=(-1)^{\frac{p-1}{2}}(\frac{7}{p})$$

$$=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{7-1}{2}}(\frac{p}{7})$$

$$=(-1)^{(p-1)}\left(\frac{p}{7}\right)=\left(\frac{p}{7}\right)$$

Thus there exists integer n, such that

$$p|n^2+7.$$

Because $\mathbb{Z}[w(7)]$ is a simple field, any irreducible number is prime. So that if p is irreducible on $\mathbb{Z}[w(7)]$， then Equation (2.2) could be rewritten as $p|(n+\sqrt{-7})(n-\sqrt{-7})$.

Thus on $\mathbb{Z}[w(7)]$, $p|\left(n+\sqrt{-7}\right)$ or $p|(n+\sqrt{-7})$, but this is impossible.

If p is reducible, let p=xy，its norm is $N_{\sqrt{-7}}(x)>1, N_{\sqrt{-7}}(y)>1$

$p^2=N_{\sqrt{-7}}(p)=N_{\sqrt{-7}}(x)N_{\sqrt{-7}}(y)$

so that,

$$N_{\sqrt{-7}}(x)=p$$

Let $x=\frac{a+b\sqrt{-7}}{2}, a, b\in\mathbb{Z}$，then we have $N_{\sqrt{-7}}(x)=\frac{a^2+7b^2}{4}=p$

$$a^2+7b^2=4p. \tag{2.2}$$

Equation (2.2) module 8，notice that p is odd, then

$$a^2-b^2\equiv 4p\ \equiv 4\ (\mathrm{mod}\ 8). \tag{2.3}$$

From Equation (2.3) to get：a，b are both even numbers, take n= $\left(\frac{a}{2}\right)^2$, m= $\left(\frac{b}{2}\right)^2$.

Equation (2.2) could be written as：

$$p=\left(\frac{a}{2}\right)^2+7\left(\frac{b}{2}\right)^2=n^2+7m^2\ ,$$

and this finishes the proof for the necessity.

More generally, the above theorem could be extended to the general case, when $\mathbb{Z}[w(q)]$ is a simple field.

Theorem 2.2: For any integer q>1, $\mathbb{Z}[w(q)]$ is a simple field，and for any odd prime number p，if $\left(\frac{-q}{p}\right)=0$，1，then when $q\equiv 3(\mathrm{mod}\ 8)$，there exist integers n, m, such that $4p=n^2+qm^2$, when $q\not\equiv 3(\mathrm{mod}\ 8)$，there exist integers n，m, such that $p=n^2+qm^2$.

To prove Theorem 2.2, all we need to do is to replace 7 in Theorem 2.1 with q.

2.2 One method of determining whether a quadratic integer field is a simple field

From Theorem 2.2， we have its contraposition as follows.

Lemma 2.3： For any integer q>1, when $q \not\equiv 3 (\mathrm{mod}\ 8)$, if there exist an odd prime number p, such that$(-\frac{q}{p}) = 0{,}1$, and p cannot be written as $p = n^2 + qm^2$.

When $q \equiv 3(\mathrm{mod}\ 8)$， if there exists odd prime number, such that$(-\frac{q}{p}) = 0，1$， and 4p cannot be written as $4p = n^2 + qm^2$, then $\mathbb{Z}[w(q)]$ is not a simple field.

From Theorem 2.3, we can have the following result.

Theorem 2.4： For positive integer q，q>1, and $q \not\equiv 3(\mathrm{mod}\ 8)$，if there exists an odd prime number p,p<q, and $(\frac{-q}{p}) = 0{,}1$， then $\mathbb{Z}[w(q)]$ is not a simple field; For positive integer q，q>1, and $q \equiv 3(\mathrm{mod}\ 8)$， if there exists an odd prime number p, 4p<q, and $(\frac{-q}{p}) = 0{,}1$， then $\mathbb{Z}[w(q)]$ is not a simple field.

Applying Theorem 2.4， we can get：

Corollary 2.5： If q>16, and q is a composite number, then $\mathbb{Z}[w(q)]$ is not a simple field.

Proof.

Suppose q is a composite number, and it has no perfect square factor， then there must exist a prime number p, such that $p<\sqrt{q}$， and p|q， then we have 4p<q， $\left(\frac{-q}{p}\right) = 0$, satisfying the conditions in Theorem 2.4, so that the Corollary stands.

Next we will discuss the case when q is an odd prime number.

Corollary 2.6： If q>7 ， and $q \not\equiv 3(\mathrm{mod}\ 8)$， then $\mathbb{Z}[w(q)]$ is not a simple field.

Proof.

If there exists odd prime number p, such that,

$$q \equiv -1\ (\mathrm{mod}\ p) \Leftrightarrow q^2 \equiv -q\ (\mathrm{mod}\ p) \Leftrightarrow (\frac{-q}{p}) = 1,$$

while p|q+1.

Set q+1=$2^k p_1^{i_1} p_2^{i_2} \ldots\ldots p_l^{i_l}$, where $p_1, p_2, \ldots, p_l$ are prime numbers， then there must be $p = p_j, j = 1{,}2, \ldots, l$.

According to Theorem 2.4， above result could be easily proved. So that q+1 must have the form of 2^{k_1}. Similarly, we can prove that, q+9 also has the form of 2^{k2}.

Because q+9-(q+1)=2^{k_2}-2^{k_1}=8，so that k_2=4，k_1=3，thus q could just be 7, that concludes our proof for Corollary 2.6.

Corollary 2.7： If q>7，$q > 7 (\mathrm{mod}\ 8)$, and $\mathbb{Z}[w(q)]$ is a simple field, then
q is a prime number，and there exists a prime number p, such that 4p-1=q，
p+2，when q>12，p+6 is also a prime number, and when q>16，q+4 is a
prime number.

Proof.
According to Corollary 2.5, if q>16，and q is a composite number, then $\mathbb{Z}[w(q)]$ is not a simple field.
For $8 \leq q \leq 16$，q could only be 11，and 11 is a prime number. So that we proved that q is a prime number.
Next we prove that there exists p，such that 4p-1=q is a prime number. According to $q \equiv 3 (\mathrm{mod}\ 8)$, $\frac{q+1}{4}$ must be an odd number, so that there exists a prime number p，

p≤ $\frac{q+1}{4}$，and $p | \frac{q+1}{4}$.

If $\frac{q+1}{4}$ is a composite number, then $\frac{q+1}{4} = mp$，and m is an odd number. So that

$m \geq 3$，and $p \leq \frac{q+1}{12} < \frac{q}{4}$.

But $p | \frac{q+1}{4}$=> $p | (q+1)$=>$\left(\frac{-q}{p}\right) = 1$, according to Theorem 2.4, the statement is proved.

Replace $\frac{q+1}{4}$ with $\frac{q+9}{4}$, we can prove that p+2 is a prime number.

Replace it with $\frac{q+25}{4}$, when $q > 12$,p,$\frac{q+25}{12} < \frac{q}{4}$, then p+6 is also a prime number.

Notice that q+4 is an odd number, so that if it is a composite number,
then there must exist an odd prime number p，$p \leq q+4$, and $p | q+4$.
If $q+4$ is a composite number, then there exists p$< q+4$ and $p | q+4$.

If $3 | q+4$，then $q \equiv -1 \ (\mathrm{mod}\ 3)$，since q>16,and $\left(\frac{-q}{3}\right) = 1$，3<$\frac{q}{4}$, according to Theorem 2.4, q+4 must be a prime number.

If $3 \nmid q+4$，then $q+4 = mp$，$m \geq 5$.

If q≥ f，then p= $\frac{q+4}{m} \leq \frac{q+4}{5} < \frac{q}{4}$, according to Theorem 5.4, q+4 must be a prime number.

Applying Corollary 2.5，2.6，2.7, we can construct the following algorithm to check whether $\mathbb{Z}[w(q)]$ is a simple field:

if(q<=18) then{verifying one by one}

if(q>18) then {check whether $q \equiv 3 (\mathrm{mod}\ 8)$ is prime, and $\frac{q+1}{4}, \frac{q+9}{4}, \frac{q+25}{4}$ are all prime, if one of these is not prime, then $\mathbb{Z}[w(q)]$ is not a simple field},

and using computer algorithms to get that, in the range of 18 to 10000，there are the following potential simple fileds：19，43，67，163，907，5923.

To further refine this result, we propose the following theorem.

Theorem 2.8 If $\mathbb{Z}[w(q)]$ is a simple field, and x is a positive even number,$x^2 < q(\frac{q}{16} - 1)$, then $q + x^2$ is a prime number.

Proof.

We will prove it by contradiction.

If $q + x^2$ is a composite number，then there exists an odd prime number, such that $p|q + x^2$ =>$\left(\frac{-q}{p}\right) = 1$.

If $p < \frac{q}{4}$, then it contradicts with Theorem 2.4。

Because q is an odd number，so that $p > \frac{q}{4}$.

Let $q + x^2 = mp$, if m< $\frac{q}{4}$, then for the prime factor p’of m, we have $p' \leq m < \frac{q}{4}$, which contradicts to Theorem 2.4.

So that $mp > q^2/16$, i.e., $x^2 > q(\frac{q}{4} - 1)$, contradiction.

Theorem 2.9.If $\mathbb{Z}[w(q)]$ is a simple field， and x is a positive odd number, $x^2 < q(\frac{q}{4} - 1)$，then $\frac{q+x^2}{4}$ is a prime number.

Proof.

If $\frac{q+x^2}{4}$ is a composite number, according to Corollary 2.6，q must satisfy $q \equiv 3$（mod 8），so that $\frac{q+x^2}{4}$ is an odd number，thus there exists an odd prime number p，such that p|$\frac{q+x^2}{4}$，i.e.， $p|q + x^2$， so that we have：

$\left(\frac{-q}{p}\right) = 1$. If p< $\frac{q}{4}$, then it contradicts to Theorem 2.4，meanwhile since q is an odd number，so that p>$\frac{q}{4}$.

Let $\frac{q+x^2}{4} = mp$ ，if m< $\frac{q}{4}$，then for any prime factor p’ of m, we have $p' \leq m < \frac{q}{4}$, which is in contradiction with Theorem 2.4.

So that $\mathrm{mp} > \mathrm{q}^2/16$，i.e., $\frac{\mathrm{q}+\mathrm{x}^2}{4} > \frac{\mathrm{q}^2}{16}$, and $\mathrm{x}^2 > q(\frac{\mathrm{q}}{4} - 1)$，contradiction.

Combining Theorem 2.8，2.9, we can get another algorithm to check whether $\mathbb{Z}[\mathrm{w}(\mathrm{q})]$ is simple field:

if(q<=18) then{verifying one by one}

if(q>18) then {for all even x s.t. $x^2 < q(\frac{q}{16} - 1)$, if $q + x^2$ is not prime,

then $\mathbb{Z}[\mathrm{w}(\mathrm{q})]$ is not simple field}.

Following this algorithm, we can compute to get from 18 to 1000, then only possible simple fields are: 19，43，67，163, which is exactly the right answer.

Conclusion

Lagrange, Legendre, and Gauss are pioneers of studying quadratic Diophantine equations. They focused on using reciprocity law, discriminant to classify and solve the quadratic Diophantine equations. But due to the variety and complexity of this kind of problems, the law of quadratic reciprocity, discriminant, and other equivalent methods[1] are not enough for fully understanding the essential rules underneath these problems. Based on the masterpieces done by Gauss and Dirichlet, algebraic number theory[2] disclosed further common rules in these problems. After finishing this manuscript, the author's teacher suggested reference [3], from which I learned more background of related problems.

In this study, we systematically studied the solutions of one type of ternary quadratic Diophantine equations, with some results presented. Meanwhile, preliminary methods are used to study the simple field problem, which, to the author's best knowledge, is the first of this work. Computer softwares are also used to simplify the verification process.

As some of the future work, the major tools used to study related problems and conclusions in reference [3] will be studied carefully. They also make the author realize that the work done in this study belongs to the hot topics in major number theory study.

In the future, the author will try to use Theorem 2.4 and 2.8 and 2.9 to prove that there are only finitely many q such that $\mathbb{Z}[\mathrm{w}(\mathrm{q})]$ is simple field. If I succeed, then it will be an elementary proof for a difficult theorem.

References.

[1] 高斯著，潘承彪，张明尧译 《算术研究》，2011.8

[2]. 潘承洞，潘承彪著 《代数数论》，2001.5

[3]. D.GoldFeld GAUSS' CLASS NUMBER PROBLEM FOR IMAGINARY QUADRATIC FIELDS, BULLETIN of OF THE AMERICAN MATHEMATICAL SOCIETY Vol 13,1985

[4]. H. M. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. 14 (1967), 1-27

[5] KIM S. HASSE-MINKOWSKI THEOREM[J].