ON NORM FORM DIOPHANTINE EQUATIONS

S. SUBBURAM AND R. THANGADURAI

Abstract. Let $\mathcal{R}$ be a principal ideal domain. In this article, we study the principal ideals of a quadratic extension ring $\mathcal{R}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathcal{R}\}$ where $d \in \mathcal{R}$ such that $\sqrt{d} \notin \mathcal{R}$. As an application, we solve some norm form diophantine problems.

1. Introduction

Let $\mathcal{R}$ be a principal ideal domain. Let d be an element of $\mathcal{R}$ such that the polynomial $X^2 - d$ is irreducible in $\mathcal{R}[X]$. Then

$$\mathcal{R}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathcal{R}\}$$

is an integral domain under the usual addition and multiplication. Also, $\mathcal{R}[\sqrt{d}]$ is a $\mathcal{R}$-module with a basis $\{1, \sqrt{d}\}$. Let $x\mathcal{R}$ be the principal ideal generated by the element x of $\mathcal{R}$. We denote $\gcd_{\mathcal{R}}(x, y)$ the greatest common divisor of the ideals $x\mathcal{R}$ and $y\mathcal{R}$, in $\mathcal{R}$. For any x and y in $\mathbb{Z}$, the set of all rational integers, $\gcd(x, y) = \gcd_{\mathbb{Z}}(x, y)$.

Consider the equation $X^2 - dY^2 = m$ with $d, m \in \mathcal{R}$. Let (a, b) and (u, v), $a, b, u, v \in \mathcal{R}$ and $\gcd_{\mathcal{R}}(a, db) = \gcd_{\mathcal{R}}(u, dv) = \mathcal{R}$, be solutions of $X^2 - dY^2 = m$. Then we call (a, b) is an associate of (u, v) in $\mathcal{R}[\sqrt{d}]$, if $a + b\sqrt{d}$ is an associate of $u + v\sqrt{d}$ or $u - v\sqrt{d}$.

In 1801, C. F. Gauss proved: Let p be any prime in $\mathbb{Z}$. Then the equation $X^2 + Y^2 = p$ has a solution (x, y) in $\mathbb{Z} \times \mathbb{Z}$ if and only if there is an element n in $\mathbb{Z}$ such that $n^2 + 1 \in p\mathbb{Z}$. Moreover, such solution is unique up to its associates in $\mathbb{Z}[\sqrt{-1}]$ (see [2]). Note that $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-1}]$ are principal ideal domains. In this paper, we have the following general theorem.

Theorem 1. *Let $\mathcal{R}$ and $\mathcal{R}[\sqrt{d}]$ be principal ideal domains and let p be any prime element of $\mathcal{R}$ such that $\gcd_{\mathcal{R}}(d, p) = \mathcal{R}$. Then the equation $X^2 - dY^2 = up$ has a solution (x, y) in $\mathcal{R} \times \mathcal{R}$ for some unit u in $\mathcal{R}$ if and only if there is an element $n \in \mathcal{R}$ such that $n^2 - d \in p\mathcal{R}$. Moreover, such solution is unique up to its associates in $\mathcal{R}[\sqrt{d}]$.*

Since $\mathbb{Q}[X]$, the set of all rational polynomials in variable X, is a principal ideal domain, we have the following corollary.

Corollary 1.1. *Let d be a rational number which is not a perfect square in $\mathbb{Q}$ and let f be any irreducible polynomial in $\mathbb{Q}[X]$. Then the equation $Y^2 - dZ^2 = uf$ has a solution (f_1, f_2) in $\mathbb{Q}[X] \times \mathbb{Q}[X]$ for some non-zero u in $\mathbb{Q}$ if and only if there is an element $g \in \mathbb{Q}[X]$ such that $g^2 - d \in f\mathbb{Q}[X]$. Moreover, such solution is unique up to its associates in $\mathbb{Q}(\sqrt{d})[X]$.*

In 1940, I. Niven [5] proved that a Gaussian integer of the form $a + 2bi$ is expressible as a sum of two squares of Gaussian integers if and only if not both $a/2$ and b are odd integers. In 2011, D. Wei in [9] proposed a method for determining which integers can be written as a sum of two integral squares for quadratic fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$, where p is a prime.

Let K be a number field, $\mathcal{O}_K$ be its ring of integers and $d \in \mathcal{O}_K$ such that $\mathcal{O}_K$ and $\mathcal{O}_K[\sqrt{d}]$ are principal ideal domains. If we put $\mathcal{R} = \mathcal{O}_K$ in Theorem 1, then we have,

Corollary 1.2. *Let K be a number field, $\mathcal{O}_K$ be its ring of integers and $d \in \mathcal{O}_K$ such that $\mathcal{O}_K$ and $\mathcal{O}_K[\sqrt{d}]$ are principal ideal domains. Let p be any prime element in $\mathcal{O}_K$ such that $\gcd_{\mathcal{O}_K}(d, p) = \mathcal{O}_K$. Then the equation $X^2 - dY^2 = up$ has a solution (x, y) in $\mathcal{O}_K \times \mathcal{O}_K$ for some unit u in $\mathcal{O}_K$ if and only if there is an element $n \in \mathcal{O}_K$ such that $n^2 - d \in p\mathcal{O}_K$. Moreover, such solution is unique up to its associates in $\mathcal{O}_K[\sqrt{d}]$.*

Legendre, Gauss and Ramanujan studied diagonal integral quadratic forms of 3 or 4 variables. Here we apply our method to study diagonal integral quadratic forms in 4 variables as follows. Let $(\cdot \mid p)$ denotes the Legendre symbol.

Corollary 1.3. *Let F be a quadratic extension over $\mathbb{Q}$ and let p be a prime element in $\mathbb{Z}$ as well as in $\mathcal{O}_F$, the ring of integers of F.*

(i) *(a)Let $F = \mathbb{Q}(\sqrt{-3})$. If there exists an element $n \in \mathcal{O}_F$ such that $n^2 - 2 \in p\mathcal{O}_F$, then the equation $X_1^2 - X_2^2 - 2Y_1^2 + 2Y_2^2 = \pm p$ has a rational integer solution.*
(b) If $p \equiv 5, 11 \pmod{12}$ and $p \equiv 1, 7 \pmod 8$, then the equation $X_1^2 - X_2^2 - 2Y_1^2 + 2Y_2^2 = \pm p$ has a rational integer solution.

(ii) *(a) Let $F = \mathbb{Q}(\sqrt{-11})$. If there exists an element $n \in \mathcal{O}_F$ such that $n^2 - 2 \in p\mathcal{O}_F$, then the equation $X_1^2 - 3X_2^2 - 2Y_1^2 + 6Y_2^2 = \pm p$ has a rational integer solution.*
(b) If $(p \mid 11) = -1$ and $p \equiv 1, 7 \pmod 8$, then the equation $X_1^2 - 3X_2^2 - 2Y_1^2 + 6Y_2^2 = \pm p$ has a rational integer solution.

In 2007, N. Saradha and A. Srinivasan [8] while studying solutions of some generalized Ramanujan - Nagell equation, they proved the following. For any square-free rational integer $d > 1$ and for any odd prime p, the equation $X^2 + dY^2 = p$ has at most one solution (x, y), $x \geq 0$ and $y \geq 0$, in integers. In this paper, we prove the following theorem.

Theorem 2. *Let p be a prime element in $\mathcal{R}$ such that $\gcd_{\mathcal{R}}(d, p) = \mathcal{R}$. Then the equation*

$$X^2 - dY^2 = p$$

has at most one solution $(x, y) \in \mathcal{R} \times \mathcal{R}$ up to its associates in $\mathcal{R}[\sqrt{d}]$.

In order to prove the above results, we need to study principal ideals structure dealt in Theorem 3. Let E be the quotient field of $\mathcal{R}$. Throughout the article, the elements n_1, n_2, m_1 and m_2 are in $\mathcal{R}$ such that $n_1 + n_2\sqrt{d}$ and $m_1 + m_2\sqrt{d}$ are linearly independent over E. Also the submodule $\mathfrak{a}$ of $\mathcal{R}[\sqrt{d}]$ is of the form $\mathfrak{a} = (n_1 + n_2\sqrt{d})\mathcal{R} \oplus (m_1 + m_2\sqrt{d})\mathcal{R}$. Here $m_1n_2 - n_1m_2 \neq 0$.

Theorem 3. *Let $\mathfrak{a}$ be an ideal in $\mathcal{R}[\sqrt{d}]$ with $\gcd_{\mathcal{R}}(n_1, n_2, m_1, m_2) = \mathcal{R}$. Then*

$$\mathfrak{a} = (a + b\sqrt{d})\mathcal{R}[\sqrt{d}]$$

for some $a, b \in \mathcal{R}$ if and only if $a^2 - db^2 = u(m_1n_2 - n_1m_2)$ for some unit u in $\mathcal{R}$, with

$$bm_1 - am_2, am_1 - bdm_2, bn_1 - an_2, an_1 - dbn_2 \in (m_1n_2 - n_1m_2)\mathcal{R}.$$

The following corollary is an improvement of the results obtained by C. S. Queen [10] where she gave a simple characterization of principal ideal domains and as an application, it was proved that if $p \equiv 5 \pmod 8$ is any prime, then $\mathbb{Z}[\sqrt{2p}]$ is not a principal ideal domain. However Corollary 3.1 covers much more classes of real quadratic fields.

Corollary 3.1. *Let $p \equiv 5 \pmod 8$ be any prime. Let $d = pn$ be a square-free positive integer for some integer n, such that $d \equiv 2, 3 \pmod 4$. Then $\mathbb{Z}[\sqrt{d}]$ is not a principal ideal domain.*

Theorem 4. *Let d be a square-free integer, p any odd prime, $a \geq 1$ an integer and $k = \pm 2, \pm 4, \pm p^a$ or $\pm 2p^a$. Then the equation $X^2 - dY^2 = k$ has at most one integral solution (x, y), $\gcd(x, dy) = 1$, up to its associates in $\mathbb{Z}[\sqrt{d}]$.*

2. Preliminaries

We shall start with some lemmas.

Lemma 1. *The additive subgroup $\mathfrak{a}$ is an ideal in $\mathcal{R}[\sqrt{d}]$ if and only if*

$$m_1^2 - m_2^2 d, n_1^2 - n_2^2 d, dm_2n_2 - n_1m_1 \in (n_2m_1 - m_2n_1)\mathcal{R}.$$

Proof. It is clear that $\mathfrak{a}$ is an ideal in $\mathcal{R}[\sqrt{d}]$ if and only if for any element $a + b\sqrt{d}$ of $\mathcal{R}[\sqrt{d}]$ and for any $x, y \in \mathcal{R}$, there exist x_1 and y_1 in $\mathcal{R}$ such that

$$[(n_1 + n_2\sqrt{d})x + (m_1 + m_2\sqrt{d})y](a + b\sqrt{d}) = (n_1 + n_2\sqrt{d})x_1 + (m_1 + m_2\sqrt{d})y_1.$$

This is equivalent to

$$(n_1x + m_1y)a + db(n_2x + m_2y) = n_1x_1 + m_1y_1 \text{ and } (n_1x + m_1y)b + a(n_2x + m_2y) = n_2x_1 + m_2y_1.$$

That is,

$$n_1[(n_1x + m_1y)b + a(n_2x + m_2y)] - n_2[(n_1x + m_1y)a + db(n_2x + m_2y)] \in (m_2n_1 - n_2m_1)\mathcal{R}$$

and

$$m_1[(n_1x + m_1y)b + a(n_2x + m_2y)] - m_2[(n_1x + m_1y)a + db(n_2x + m_2y)] \in (m_2n_1 - n_2m_1)\mathcal{R},$$

as $x_1, y_1 \in \mathcal{R}$. Thus, we have that $\mathfrak{a}$ is an ideal in $\mathcal{R}[\sqrt{d}]$ if and only if

$$b(n_1^2 - n_2^2 d)x + b(n_1m_1 - dm_2n_2)y \in (m_2n_1 - n_2m_1)\mathcal{R}$$

and

$$yb(m_1^2 - m_2^2 d) + bx(n_1m_1 - dm_2n_2) \in (m_2n_1 - n_2m_1)\mathcal{R}$$

for any b, x, $y \in \mathcal{R}$. This proves the result. □

Remark. *Suppose the ideal $\mathfrak{a} = (a + b\sqrt{d})\mathcal{R}[\sqrt{d}]$ for some $a + b\sqrt{d} \in \mathfrak{a}$. Then $\gcd_{\mathcal{R}}(a, b) = \mathcal{R}$ if and only if $\gcd_{\mathcal{R}}(n_1, n_2, m_1, m_2) = \mathcal{R}$.* This can be easily proven.

Proof of Theorem 3. It is clear that for some $a, b \in \mathcal{R}$, $\mathfrak{a} = (a + b\sqrt{d})\mathcal{R}[\sqrt{d}]$ if and only if (i) and (ii) hold:

(i) For any $x_1 + y_1\sqrt{d} \in \mathcal{R}[\sqrt{d}]$, there exist unique x and y in $\mathcal{R}$ such that $(a + b\sqrt{d})(x_1 + y_1\sqrt{d}) = (n_1 + n_2\sqrt{d})x + (m_1 + m_2\sqrt{d})y$;
(ii) For any $x, y \in \mathcal{R}$, there exist unique x_1 and y_1 in $\mathcal{R}$ such that $(n_1 + n_2\sqrt{d})x + (m_1 + m_2\sqrt{d})y = (a + b\sqrt{d})(x_1 + y_1\sqrt{d})$.

In the above observation, (i) is equivalent to the following; for any $x_1, y_1 \in \mathcal{R}$, there exist unique x and y in $\mathcal{R}$ such that

$$n_1x + m_1y = ax_1 + bdy_1 \text{ and } n_2x + m_2y = bx_1 + ay_1.$$

That is (i) is equivalent to, for any $x_1, y_1 \in \mathcal{R}$,

$$(am_2 - bm_1)x_1 + (dbm_2 - am_1)y_1, (an_2 - bn_1)x_1 + (dbn_2 - an_1)y_1 \in (m_2n_1 - n_2m_1)\mathcal{R}.$$

So (i) holds if and only if

$$bm_1 - am_2, am_1 - bm_2d, an_2 - bn_1, dbn_2 - an_1 \in (m_1n_2 - n_1m_2)\mathcal{R}.$$

Now we shall consider (ii). Since $a + b\sqrt{d}, a - b\sqrt{d} \neq 0$ and $\mathcal{R}[\sqrt{d}]$ is an integral domain,

$$a^2 - b^2d \neq 0.$$

Then (ii) holds if and only if for any $x, y \in \mathcal{R}$, there exist unique x_1 and y_1 in $\mathcal{R}$ such that

$$n_1x + m_1y = ax_1 + bdy_1, \text{ and } n_2x + m_2y = bx_1 + ay_1.$$

So (ii) is equivalent to the following; for any $x, y \in \mathcal{R}$,

$$(an_2 - bn_1)x + (am_2 - bm_1)y \in (a^2 - b^2d)\mathcal{R} \text{ and } (an_1 - dbn_2)x + (am_1 - dbm_2)y \in (a^2 - db^2)\mathcal{R}.$$

That is,

$$an_1 - dbn_2, am_1 - dbm_2, an_2 - bn_1, am_2 - bm_1 \in (a^2 - db^2)\mathcal{R}$$

and hence $a(m_1n_2 - n_1m_2), b(m_1n_2 - n_1m_2) \in (a^2 - db^2)\mathcal{R}$. Since $\gcd_{\mathcal{R}}(a, b) = \mathcal{R}$, we have,

$$(m_1n_2 - n_1m_2)\mathcal{R} \subseteq (a^2 - db^2)\mathcal{R}. \tag{1}$$

Now, since $bm_1 - am_2, am_1 - bm_2d \in (m_1n_2 - n_1m_2)\mathcal{R}$,

$$m_2(a^2 - db^2), m_1(a^2 - db^2) \in (m_1n_2 - n_1m_2)\mathcal{R}.$$

Similarly, since $an_2 - bn_1, dbn_2 - an_1 \in (m_1n_2 - n_1m_2)\mathcal{R}$, we have

$$n_1(a^2 - db^2), n_2(a^2 - db^2) \in (m_1n_2 - n_1m_2)\mathcal{R}.$$

So $\gcd_{\mathcal{R}}(n_1, n_2, m_1, m_2)(a^2 - db^2) \subseteq (m_1n_2 - n_1m_2)\mathcal{R}$. Therefore

$$(a^2 - db^2)\mathcal{R} \subseteq (m_1n_2 - n_1m_2)\mathcal{R}. \tag{2}$$

From (1) and (2), we have $a^2 - db^2 = u(m_1n_2 - n_1m_2)$ for some unit $u \in \mathcal{R}$. This proves the theorem. □

The following lemma gives a link explicitly between the generators of a principal ideal and the integral solutions of the equation $x^2 - dy^2 = k$.

Lemma 2. *Let $k = x^2 - dy^2$ be an element in $\mathcal{R}$ for some $x, y \in \mathcal{R}$ with $\gcd_{\mathcal{R}}(x, dy) = \mathcal{R}$. If*

(1) *$kn = m^2 - d$ for some $n, m \in \mathcal{R}$*
(2) *$mx + dy, my + x \in k\mathcal{R}$ or $mx - dy, my - x \in k\mathcal{R}$,*

then there exists a principal ideal $\mathcal{P}$ in $\mathcal{R}[\sqrt{d}]$ such that

$$\mathcal{P} = n\mathcal{R} + (m + \sqrt{d})\mathcal{R}.$$

Moreover, if $\mathcal{P} = (a + b\sqrt{d})\mathcal{R}[\sqrt{d}]$ for some $a, b \in \mathcal{R}$, then

$$(a, b) = \left(\frac{mx + dy}{k}, \frac{my + x}{k}\right) \text{ or } \left(\frac{mx - dy}{k}, \frac{x - my}{k}\right).$$

Proof. Since $(m^2 - d) \in n\mathcal{R}$, by Lemma 1, we see that $\mathcal{P} = n\mathcal{R} + (m + \sqrt{d})\mathcal{R}$ is an ideal in $\mathcal{R}[\sqrt{d}]$. Therefore, it is enough to prove that $\mathcal{P}$ is a principal ideal.

First we shall prove that if $mx + dy, my + x \in k\mathcal{R}$, then $\mathcal{P}$ is the principal ideal generated by $a + b\sqrt{d}$, where

$$(a, b) = \left(\frac{mx + dy}{k}, \frac{my + x}{k}\right).$$

Since $\mathcal{P} = n\mathcal{R} + (m + \sqrt{d})\mathcal{R}$, by putting $n_1 = n$, $n_2 = 0$, $m_1 = m$ and $m_2 = 1$ in Theorem 3, we see that it is enough to prove the following conditions;

$$bm - a, am - bd \in n\mathcal{R}, \text{ and } a^2 - db^2 = n,$$

because it is clear that

$$\gcd_{\mathcal{R}}(a, b) = \gcd_{\mathcal{R}}\left(\left(\frac{mx + dy}{k}\right), \left(y\left(\frac{mx + dy}{k}\right) - x\left(\frac{my + x}{k}\right)\right)\right) = \mathcal{R}.$$

Since $n = (m^2 - d)/k$, we have that

$$\left(\frac{mx + dy}{k}\right)^2 - d\left(\frac{my + x}{k}\right)^2 = n.$$

That is, $a^2 - db^2 = n$. So we need only to check the conditions $bm - a, am - bd \in n\mathcal{R}$. Now, consider

$$bm - a = \frac{m(my + x)}{k} - \frac{(mx + dy)}{k} = \frac{m^2y - dy}{k} = ny \in n\mathcal{R}.$$

Similarly, we have $am - bd \in n\mathcal{R}$. Thus $\mathcal{P}$ is the principal ideal in $\mathcal{R}[\sqrt{d}]$, generated by $a + b\sqrt{d}$.

Since $(x, y) \in \mathcal{R} \times \mathcal{R}$ is a solution of $X^2 - dY^2 = k$ with $\gcd_{\mathcal{R}}(x, dy) = \mathcal{R}$, $(x, -y) \in \mathcal{R} \times \mathcal{R}$ is also a solution of the equation with $\gcd_{\mathcal{R}}(x, -dy) = \mathcal{R}$. Therefore the above statement is true for $(x, -y)$ also. This proves the lemma. □

Lemma 3. *Let k be an element in $\mathcal{R}$ and let (x_1, y_1) and (x_2, y_2) in $\mathcal{R} \times \mathcal{R}$ be two solutions of the equation*

$$x^2 - dy^2 = k$$

with $\gcd_{\mathcal{R}}(x_1, dy_1) = \gcd_{\mathcal{R}}(x_2, dy_2) = \mathcal{R}$. If $kn = m^2 - d$ for some $m, n \in \mathcal{R}$ and if one of the following four is true.

(1) $mx_1 + dy_1, my_1 + x_1 \in k\mathcal{R}$, $mx_2 + dy_2, my_2 + x_2 \in k\mathcal{R}$;
(2) $mx_1 - dy_1, my_1 - x_1 \in k\mathcal{R}$, $mx_2 - dy_2, my_2 - x_2 \in k\mathcal{R}$;
(3) $mx_1 + dy_1, my_1 + x_1 \in k\mathcal{R}$, $mx_2 - dy_2, my_2 - x_2 \in k\mathcal{R}$;
(4) $mx_1 - dy_1, my_1 - x_1 \in k\mathcal{R}$, $mx_2 + dy_2, my_2 + x_2 \in k\mathcal{R}$,

then (x_1, y_1) is an associate of (x_2, y_2) in $\mathcal{R}[\sqrt{d}]$.

Proof. Since $mx_1 + dy_1, my_1 + x_1 \in k\mathcal{R}$ or $mx_1 - dy_1, my_1 - x_1 \in k\mathcal{R}$, by Lemma 2, for the pair (x_1, y_1), we can associate a principal ideal

$$\mathcal{P} = n\mathcal{R} + (m + \sqrt{d})\mathcal{R} = \begin{cases} \left(\frac{mx_1 + dy_1}{k} + \frac{my_1 + x_1}{k}\sqrt{d}\right)\mathcal{R}[\sqrt{d}] \text{ or} \\ \left(\frac{mx_1 - dy_1}{k} + \frac{x_1 - my_1}{k}\sqrt{d}\right)\mathcal{R}[\sqrt{d}] \end{cases}$$

Similarly, by Lemma 2 again, for the other pair (x_2, y_2), we have,

$$\mathcal{P} = n\mathcal{R} + (m+\sqrt{d})\mathcal{R} = \begin{cases} \left(\frac{mx_2+dy_2}{k} + \frac{my_2+x_2}{k}\sqrt{d}\right)\mathcal{R}[\sqrt{d}] \text{ or} \\ \left(\frac{mx_2-dy_2}{k} + \frac{x_2-my_2}{k}\sqrt{d}\right)\mathcal{R}[\sqrt{d}] \end{cases},$$

because $mx_2 + dy_2, my_2 + x_2 \in k\mathcal{R}$ or $mx_2 - dy_2, my_2 - x_2 \in k\mathcal{R}$. So there are four possibilities for $\mathcal{P}$. Without loss of generality we can assume that

$$\mathcal{P} = n\mathcal{R} + (m+\sqrt{d})\mathcal{R} = \left(\frac{mx_1+dy_1}{k} + \frac{my_1+x_1}{k}\sqrt{d}\right)\mathcal{R}[\sqrt{d}]$$

and

$$\mathcal{P} = n\mathcal{R} + (m+\sqrt{d})\mathcal{R} = \left(\frac{mx_2+dy_2}{k} + \frac{my_2+x_2}{k}\sqrt{d}\right)\mathcal{R}[\sqrt{d}].$$

Since any two generators of a principal ideal are associates, we conclude that

$$\left(\frac{mx_1+dy_1}{k} + \frac{my_1+x_1}{k}\sqrt{d}\right) \text{ and } \left(\frac{mx_2+dy_2}{k} + \frac{my_2+x_2}{k}\sqrt{d}\right)$$

are associates. Therefore, there exists a unit $a + b\sqrt{d}$ in $\mathcal{R}[\sqrt{d}]$ such that

$$(mx_1 + dy_1) + (my_1 + x_1)\sqrt{d} = (a + b\sqrt{d})\left((mx_2 + dy_2) + (my_2 + x_2)\sqrt{d}\right).$$

This implies that

$$x_1 + y_1\sqrt{d} = \left(a + b\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right).$$

This proves the lemma. □

Lemma 4. *Let p be a prime element in $\mathcal{R}$ such that $\gcd_{\mathcal{R}}(d, p) = \mathcal{R}$, and $p = x^2 - dy^2$ for some $x, y \in \mathcal{R}$. Then there exist $n, m \in \mathcal{R}$ such that*

(a) *$pn = m^2 - d$;*
(b) *$mx + dy, my + x \in p\mathcal{R}$ or $mx - dy, my - x \in p\mathcal{R}$.*

Proof. Let $p = x^2 - dy^2$ be prime in $\mathcal{R}$ such that $\gcd_{\mathcal{R}}(d, p) = \mathcal{R}$, for some $x, y \in \mathcal{R}$. First we shall prove that there exists an element $\alpha \in \mathcal{R}$ such that $y\alpha \equiv 1 \pmod{p}$. Since p is prime in $\mathcal{R}$, the ideal $p\mathcal{R}$ is a maximal ideal in $\mathcal{R}$. So, $\mathcal{R}/p\mathcal{R}$ is a field. Since $\gcd_{\mathcal{R}}(x, dy) = \mathcal{R}$, we have $y + p\mathcal{R} \neq p\mathcal{R}$. So, for the element $y + p\mathcal{R} \in \mathcal{R}/p\mathcal{R}$, there exists a unique element $\alpha + p\mathcal{R}$ in $\mathcal{R}/p\mathcal{R}$ such that $(y + p\mathcal{R})(\alpha + p\mathcal{R}) = 1 + p\mathcal{R}$. That is, $y\alpha - 1 \in p\mathcal{R}$. Since $x^2 \equiv dy^2 \pmod{p}$, we see that $(x\alpha)^2 \equiv d(y\alpha)^2 \pmod{p}$. Therefore, $(x\alpha)^2 \equiv d \pmod{p}$, because $y\alpha - 1 \in p\mathcal{R}$. By letting $m = x\alpha$, we have $pn = m^2 - d$ for some $n \in \mathcal{R}$. Thus, we have

$$(m^2 - d)x^2 = m^2x^2 - dx^2 = m^2x^2 - d(p + dy^2) = (mx + dy)(mx - dy) - dp.$$

So, $(mx + dy)(mx - dy) \in p\mathcal{R}$. This implies that $mx + dy \in p\mathcal{R}$ or $mx - dy \in p\mathcal{R}$, because $p\mathcal{R}$ is prime ideal in $\mathcal{R}$. If $mx + dy \in p\mathcal{R}$, then

$$mxy + dy^2 = mxy + x^2 - p = x(my + x) - p \in p\mathcal{R}.$$

This gives that $x(my + x) \in p\mathcal{R}$. That is, $x \in p\mathcal{R}$ or $my + x \in p\mathcal{R}$. Since $\gcd_{\mathcal{R}}(x, dy) = \mathcal{R}$, $x \notin p\mathcal{R}$. This means that $my + x \in p\mathcal{R}$.

From this, we have that if $mx - dy \in p\mathcal{R}$, then $my - x \in p\mathcal{R}$, since $(x, -y) \in \mathcal{R} \times \mathcal{R}$ is also a solution of $X^2 - dY^2 = p$. This proves the lemma. □

Lemma 5. *If $\mathcal{R}[\sqrt{d}]$ is a principal ideal domain and if n_1, n_2, m_1 and m_2 satisfy*

(1) $\gcd_{\mathcal{R}}(n_1, n_2, m_1, m_2) = \mathcal{R}$;
(2) $m_1^2 - m_2^2 d, n_1^2 - n_2^2 d, dm_2n_2 - n_1m_1 \in (n_2m_1 - m_2n_1)\mathcal{R}$,

then the equation

$$x^2 - dy^2 = u(n_2m_1 - m_2n_1)$$

has a solution $(x, y) \in \mathcal{R} \times \mathcal{R}$, $\gcd_{\mathcal{R}}(x, dy) = \mathcal{R}$, *for some unit* u *in* $\mathcal{R}$.

Proof. Since $m_1^2 - m_2^2 d, n_1^2 - n_2^2 d, dm_2n_2 - n_1m_1 \in (n_2m_1 - m_2n_1)\mathcal{R}$, by Lemma 1, $\mathfrak{a} = (n_1 + n_2\sqrt{d})\mathcal{R} \oplus (m_1 + m_2\sqrt{d})\mathcal{R}$ is an ideal in $\mathcal{R}[\sqrt{d}]$. Since $\mathcal{R}[\sqrt{d}]$ is a principal ideal domain, we see that $\mathfrak{a} = (a + b\sqrt{d})\mathcal{R}[\sqrt{d}]$, for some $a, b \in \mathcal{R}$. By the remark followed by Lemma 1, we see that $\gcd_{\mathcal{R}}(a, b) = \mathcal{R}$. So, by Theorem 3, we have that $a^2 - db^2 = u(n_2m_1 - m_2n_1)$ for some unit u in $\mathcal{R}$. □

Let $m \neq 0$ be in $\mathcal{R}$. Put $n_2 = 1$, $m_1 = m$, $m_2 = 0$ in Lemma 5. Then we have the following corollary.

Corollary 6. *Let* $\mathcal{R}[\sqrt{d}]$ *be a principal ideal domain and let* $m \neq 0$ *be an element in* $\mathcal{R}$. *If* $n^2 - d \in m\mathcal{R}$ *for some* $n \in \mathcal{R}$, *then the equation* $x^2 - dy^2 = um$ *has a solution* $(x, y) \in \mathcal{R} \times \mathcal{R}$, $\gcd_{\mathcal{R}}(x, dy) = \mathcal{R}$, *for some unit* u *in* $\mathcal{R}$.

Lemma 7. *Let* $\mathcal{R}[\sqrt{d}]$ *be principal ideal domain and let* p *be a prime element in* $\mathcal{R}$ *such that* $\gcd_{\mathcal{R}}(d, p) = \mathcal{R}$. *Then* $n^2 - d \in p\mathcal{R}$ *for some* $n \in \mathcal{R}$ *if and only if the equation* $x^2 - dy^2 = up$ *has a solution* $(x, y) \in \mathcal{R} \times \mathcal{R}$ *for some unit* u *in* $\mathcal{R}$.

Proof follows from Corollary 6 and Lemma 4.

Lemma 8. *Let* d *be a square-free integer and let* $k = x^2 - dy^2$ *be an integer for some integers* x *and* y *with* $\gcd(x, dy) = 1$. *For any integer* m, *we have,*

(1) *if* $k|(mx + dy)$, *then* $k|(my + x)$;
(2) *if* $k|(mx - dy)$,*then* $k|(my - x)$.

Proof. We have $k = x^2 - dy^2$ with $\gcd(x, dy) = 1$. Therefore, $\gcd(x, k) = 1$. If $k|(mx + dy)$, then $k|(mxy + dy^2) = mxy - k + x^2 = x(my + x) - k$ and hence $k|x(my + x)$. Since $\gcd(x, k) = 1$, $k|(my + x)$, as desired. Since $k = x^2 - d(-y)^2$, by (1), we have (2). □

Lemma 9. *Let* d *be a square-free integer and let* $k = x^2 - dy^2$ *be an integer for some integers* x *and* y *with* $\gcd(x, dy) = 1$. *Then there exist integers* m *and* n *such that* $kn = m^2 - d$.
Proof. Given that $k = x^2 - dy^2$. Then $x^2 \equiv dy^2 (\mathrm{mod}\ k)$. This implies that$(xy^{-1})^2 \equiv d (\mathrm{mod}\ k)$. From this, we see that there exist integers n and $m = (xy^{-1})$ such that $kn = m^2 - d$. □

Lemma 10. *Let* d *be a square-free integer and let* $k = \pm 2, \pm 4, \pm p^a$ *or* $\pm 2p^a$ *for any odd prime* p *and any integer* $a \geq 1$. *Suppose that the equation* $x^2 - dy^2 = k$ *has an integral solution* (x, y) *such that* $\gcd(x, dy) = 1$. *Let* m *be an integer such that* $k|(m^2 - d)$. *Then either* $k|(mx + dy)$ *or* $k|(mx - dy)$ *is true.*
Proof. Given that $k = \pm 2, \pm 4, \pm p^a$ or $\pm 2p^a$ and $x^2 - dy^2 = k$ for some integers x and y with $\gcd(x, dy) = 1$. Let m be an integer such that $k|(m^2 - d)$. Note that

$$(m^2 - d)x^2 = (mx + dy)(mx - dy) - dk.$$

Since $k|(m^2 - d)$, we see that $k|[(mx + dy)(mx - dy)]$.

If $2 \mid k$, then x, d, y and m are odd, since $\gcd(x, dy) = 1$. That is, mx and dy are odd. Therefore 4 divides one of the even numbers $(mx + dy)$ and $(mx - dy)$.

Next we shall show that if $p^a \mid k$, then $p^a \mid (mx+dy)$ or $p^a \mid (mx-dy)$. Suppose that $p|(mx+dy)$ and $p|(mx-dy)$. So $p|2mx$. Since p is an odd prime with $\gcd(p,m)=1$, we have $p|x$. So $p|dy$ and hence $p \mid \gcd(x,dy)$, which is a contradiction to $\gcd(x,dy)=1$. So $p^a|(mx+dy)$ or $p^a|(mx-dy)$, since $p^a|[(mx+dy)(mx-dy)]$

From these, we conclude that $k|(mx+dy)$ or $k|(mx-dy)$. □

3. Proofs of Theorems 1 and 2

Proof of Theorem 2. Suppose that there are two solutions (x_1,y_1) and (x_2,y_2) in $\mathcal{R}$ satisfying the equation $x^2-dy^2=p$. Since p is a prime element in $\mathcal{R}$ such that $\gcd_{\mathcal{R}}(d,p)=\mathcal{R}$, by Lemma 4, we have $pn=m^2-d$ for some $n,m\in\mathcal{R}$ and one of the following four is true

(1) $mx_1+dy_1, my_1+x_1 \in p\mathcal{R}$, $mx_2+dy_2, my_2+x_2 \in p\mathcal{R}$;
(2) $mx_1+dy_1, my_1+x_1 \in p\mathcal{R}$, $mx_2-dy_2, my_2-x_2 \in p\mathcal{R}$;
(3) $mx_1-dy_1, my_1-x_1 \in p\mathcal{R}$, $mx_2+dy_2, my_2+x_2 \in p\mathcal{R}$;
(4) $mx_1-dy_1, my_1-x_1 \in p\mathcal{R}$, $mx_2-dy_2, my_2-x_2 \in p\mathcal{R}$.

So, by Lemma 3, we have that (x_1,y_1) is an associate of (x_2,y_2) in $\mathcal{R}[\sqrt{d}]$. This proves the theorem. □

Proof of Theorem 1. Proof follows from Lemma 7 and Theorem 2. □

4. Proof of Corollary 1.3.

It is well known (see for instance, [3]) that if D is a square-free integer $D \equiv 1(\mathrm{mod}4)$ and $H=\mathbb{Q}(\sqrt{D})$, then

$$\mathcal{O}_H = \mathbb{Z} \oplus \frac{1+\sqrt{D}}{2}\mathbb{Z}.$$

Also, if D is a square-free integer with $D \equiv 1(\mathrm{mod}4)$ and $H=\mathbb{Q}(\sqrt{2},\sqrt{D})$, then

$$\mathcal{O}_H = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \frac{1+\sqrt{D}}{2}\mathbb{Z} \oplus \frac{\sqrt{2}+\sqrt{2D}}{2}\mathbb{Z},$$

and for $D=-1,-3,-11$, the class number of $\mathcal{O}_H$ is 1 (see for instance, [6]). Also, it is known that the class number of $\mathbb{Q}(\sqrt{-D})$ is 1 for $D=2,3$.

To prove (i) of (a), we let $H=\mathbb{Q}(\sqrt{2},\sqrt{-3})$. Then, we have

$$\mathcal{O}_H = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \frac{1+\sqrt{-3}}{2}\mathbb{Z} \oplus \frac{\sqrt{2}+\sqrt{-6}}{2}\mathbb{Z}.$$

If $F=\mathbb{Q}(\sqrt{-3})$, then,

$$\mathcal{O}_F = \mathbb{Z} \oplus \frac{1+\sqrt{-3}}{2}\mathbb{Z}.$$

If $\mathcal{R}=\mathcal{O}_F(\sqrt{2})=\mathcal{O}_F \oplus \mathcal{O}_F\sqrt{2}$, then

$$\mathcal{R} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \frac{1+\sqrt{-3}}{2}\mathbb{Z} \oplus \frac{\sqrt{2}+\sqrt{-6}}{2}\mathbb{Z}.$$

Therefore, $\mathcal{O}_H=\mathcal{R}$ and we see that the class number of $\mathcal{O}_H$ is 1. Therefore the class number of $\mathcal{O}_F(\sqrt{2})$ is 1 and the class number of $\mathcal{O}_F$ is also 1. By Theorem 1, we have the following: For

any prime element $p \in \mathcal{O}_F$, the equation $x^2 - 2y^2 = \pm p$ has a solution (x, y) with x, $y \in \mathcal{O}_F$ if and only if there is an element $n \in \mathcal{O}_F$ such that $n^2 - 2 \in p\mathcal{O}_F$. Let

$$x = x_1 + \frac{1+\sqrt{-3}}{2}x_2 \text{ and } y = y_1 + \frac{1+\sqrt{-3}}{2}y_2$$

for some integers x_1, x_2, y_1 and y_2. Then $\pm p = x^2 - 2y^2$ is equivalent to that

$$\pm p = \left(x_1 + \frac{1+\sqrt{-3}}{2}x_2\right)^2 - 2\left(y_1 + \frac{1+\sqrt{-3}}{2}y_2\right)^2.$$

Since p is a rational prime, we get,

$$x_1^2 + x_1x_2 - \frac{1}{2}x_2^2 - 2y_1^2 - 2y_1y_2 + y_2^2 = \pm p \text{ and } x_1x_2 + \frac{1}{2}x_2^2 - 2y_1y_2 - y_2^2 = 0.$$

When we subtract the above two equations, we have

$$x_1^2 - x_2^2 - 2y_1^2 + 2y_2^2 = \pm p.$$

This proves the result.

(b) Let F and H be as in (i) (a). Since $p \equiv 1, 7 \pmod 8$, we get 2 is a square modulo p. Therefore there exists n such that $n^2 - 2 \in p\mathcal{O}_F$. Since $p \equiv 5, 11 \pmod{12}$, we see that p is a non-square modulo 3. Therefore p is a prime element in $\mathcal{O}_F$. Therefore the assertion follows from (i) (a).

Proof of (ii) is similar to the proof of (i) by taking $H = \mathbb{Q}(\sqrt{2}, \sqrt{-11})$ and $F = \mathbb{Q}(\sqrt{-3})$. □

5. Proof of Corollary 3.1.

First we treat the case when $d = pn$ where $d \equiv 2 \pmod 4$, even integer. Let $\mathfrak{a} = (6+\sqrt{d})\mathbb{Z} + (4+\sqrt{d})\mathbb{Z}$. Since $n_1 = 6, n_2 = 1, m_1 = 4$ and $m_2 = 1$, we see that

$$m_1n_2 - m_2n_1 = -2$$

and

$$m_1^2 - m_2^2d = 16 - d, n_1^2 - n_2^2d = 36 - d, \text{ and } dm_2n_2 - m_1n_1 = d - 24.$$

Hence 2 divides $\gcd(16-d, 36-d, d-24)$, as d is even and so $\mathfrak{a}$ is an ideal. If it is a principal ideal, by Theorem 3, there exist integers a and b such that

$$a^2 - b^2d = \pm(m_1n_2 - n_1m_2) = \pm 2,$$

but this is impossible as $p \equiv 5 \pmod 8$. Hence, $\mathbb{Z}[\sqrt{d}]$ is not a principal ideal domain.

Next, assume that $d = pn$ where $d \equiv 3 \pmod 4$, odd case. Let $\mathfrak{a} = (5+3\sqrt{d})\mathbb{Z} + (1+\sqrt{d})\mathbb{Z}$ be an additive subgroup of $\mathbb{Z}[\sqrt{d}]$. Since $m_1n_2 - n_1m_2 = -2$ and we see that $2|\ \gcd(1-d, 25-9d, 3d-5)$, as d is odd. Therefore, $\mathfrak{a}$ is an ideal in $\mathbb{Z}[\sqrt{d}]$. If possible, $\mathfrak{a}$ is a principal ideal. Then, by Theorem 3, there exist integers a and b such that

$$a^2 - pnb^2 = \pm 2.$$

Then we have,

$$a^2 \equiv \pm 2 \pmod p$$

which is impossible as ± 2 are non-square modulo p with $p \equiv 5 \pmod 8$. Hence $\mathfrak{a}$ is not a principal ideal and so $\mathbb{Z}[\sqrt{d}]$ is not a principal ideal domain.

□

6. Proof of Theorem 4

Suppose that there are two integral solutions (x_1, y_1) and (x_2, y_2) to the equation $x^2 - dy^2 = k$, such that $\gcd(x_1, dy_1) = \gcd(x_2, dy_2) = 1$ and (x_1, y_1) is not an associate of (x_2, y_2) in $\mathbb{Z}[\sqrt{d}]$. By Lemma 9, there exist integers m and n such that $kn = m^2 - d$. Also, by Lemma 10, the following is true:

(1) $k|(mx_1 + dy_1)$ or $k \mid (mx_1 - dy_1)$
(2) $k|(mx_2 + dy_2)$ or $k \mid (mx_2 - dy_2)$.

Therefore, by Lemma 8, we have one of the following

(1) $mx_1 + dy_1, my_1 + x_1 \in k\mathbb{Z}$, $mx_2 + dy_2, my_2 + x_2 \in k\mathbb{Z}$;
(2) $mx_1 + dy_1, my_1 + x_1 \in k\mathbb{Z}$, $mx_2 - dy_2, my_2 - x_2 \in k\mathbb{Z}$;
(3) $mx_1 - dy_1, my_1 - x_1 \in k\mathbb{Z}$, $mx_2 + dy_2, my_2 + x_2 \in k\mathbb{Z}$;
(4) $mx_1 - dy_1, my_1 - x_1 \in k\mathbb{Z}$, $mx_2 - dy_2, my_2 - x_2 \in k\mathbb{Z}$.

By Lemma 3, we get that (x_1, y_1) is an associate of (x_2, y_2) in $\mathbb{Z}[\sqrt{d}]$. This is a contradiction. This proves the theorem. □

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers, *Mathematika*, **13** (1966), 204-216.
[2] L. E. Dickson, Diophantine Analysis, Chelsea Publishing Company, New York, (1971).
[3] J. Esmonde and M. Ram Murty, Problems in Algebraic Number Theory, Springer-Verlog, (1999).
[4] C. J. A. Evelyn and E. H. Linfoot, On a problem in the additive theory of numbers, *J. Reine Angew. Math.*, **164** (1931), 131-140.
[5] I. Niven, Integers of quadratic fields as sums of squares, *Trans. Amer. Math. Soc.*, **48** (3) (1940), 405 -417.
[6] H. K. Kim and Y. M. Kim, A classification of certain biquadratic fields of class number 1, *Bull. Korean Math. Soc.*, **28** (1) (1991), 15-21.
[7] S. Ramanujan, The lost notebook and other unpublished papers, Narosa Publishing House, New Delhi, 1988.
[8] N. Saradha and A. Srinivasan, Solutions of some generalized Ramanujan- Nagell equations via binary quadratic forms, *Publ. Math. Debrecen*, **71/3-4** (2007), 349-374.
[9] D. Wei, On the sum of two integral squares in quadratic fields $\mathbb{Q}(\sqrt{\pm p})$, *Acta Arith.*, **147** (2011), 253-260
[10] C. S. Queen, A simple characterization of principal ideal domains, *Acta Arith.*, **LXIV**, (2) (1993) 125-128.

(S. Subburam) Department of Mathematics, SASTRA University, Thanjavur - 613401, India.
E-mail address: ssubburam@maths.sastra.edu

(R. Thangadurai) Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019, India
E-mail address: thanga@hri.res.in