이학석사 학위논문

Representations by a binary quadratic form with class number 4

(류수가 4인 이변수 이차형식의 표현)

2013년 2월

서울대학교 대학원

수리과학부

김정진

Representations by a binary quadratic form with class number 4

(류수가 4인 이변수 이차형식의 표현)

지도교수 오 병 권

이 논문을 이학석사 학위논문으로 제출함

2012년 12월

서울대학교 대학원
수 리 과 학 부
김정진

김정진의 이학석사 학위논문을 인준함

2012년 12월

위 원 장______________ 인

부위원장______________ 인

위 원______________ 인

Representations by a binary quadratic form with class number 4

by

KIM JUNGJIN

A DISSERTATION

Submitted to the faculty of the Graduate School
in partial fulfillment of the requirements
for the degree Master of Science
in the Department of Mathematics
Seoul National University
February, 2013

Abstract

A homogeneous quadratic polynomial $F(x,y) = ax^2 + bxy + cy^2$ $(a,\ b,\ c \in \mathbb{Z})$ is called a *binary quadratic form*. In this thesis, we consider the binary form $F(x,y) = x^2 + 64y^2$ which has class number 4. Our aim is to give an explicit closed formula for the equation $F(x,y) = n$ for any integer n. To do this, we adopt the method developed in [3]. In section 5, we collect all results proved in the previous sections and provide a closed formula of the above equation explicitly.

Key words : class number 4, binary quadratic forms
Student number : 2011-20265

Contents

Representations by a binary quadratic form with class number 4

1 Introduction

A homogeneous quadratic polynomial $F(x, y) = ax^2 + bxy + cy^2$ $(a,\ b,\ c \in \mathbb{Z})$ is called a *binary quadratic form*. It is quite an old problem to find all solutions of the diophantine equation

$$F(x, y) = k \tag{1.1}$$

for an integer k. If

$$F_i(x, y) = a_i x^2 + b_i xy + c_i y^2 \quad \text{for} \quad i = 1,\ 2, \cdots,\ h$$

are all equivalence classes of primitive binary forms of discriminant d for any non-square integer d, then it is well known that for any integer k with $gcd(k, d) = 1$,

$$\sum_{i=1}^{h} \sharp\{(x, y) \in \mathbb{Z}^2 \mid F_i(x, y) = k\} = w \sum_{n|k} \left(\frac{d}{n}\right),$$

$$\text{where} \quad w = \begin{cases} 2 & \text{if } d < -4, \\ 4 & \text{if } d = -4, \\ 6 & \text{if } d = -3 \end{cases}$$

and $\left(\frac{d}{n}\right)$ is a Kronecker's symbol.

Hence if the class number of F is 1 (more generally, if the number of equivalence classes in the genus of F is 1), then we know the complete answer on the number of solutions of the equation (1.1). If k is a prime, then we have an effective criterion whether or not the equation (1.1) has a solution(see, for details [1]).

Recently Sun and Williams [4] solved this problem completely when the class number of F is less than or equal to 4 under the assumption that $\sharp\{(x, y) \in \mathbb{Z}^2 \mid G(x, y) = p\}$ is known for any prime p and any form G in the genus of F.

Also Oh and Min [3] introduced a little bit simple method and gave a closed formula for the number of solutions of the equation $x^2 + 32y^2 = n$. Note that the class of $x^2 + 32y^2 = n$ is 4. In this thesis, we consider the equation $x^2 + 64y^2 = n$. Our aim is to give a closed formula for the number of solutions of the above equation. To do that, we adopt the method developed in [3]. Throughout this thesis, we always assume that the set of primes that are represented by any form of discriminant -256 is completely known.

In Section 3, we introduce some notations, terminologies and prove some lemmas. Everything is quite similar to [3].

In Section 4, we consider the case when n is a prime power. Note that

$$\sharp\{(x,y) \in \mathbb{Z}^2 \mid x^2+64y^2 = n\} = \sharp\{(x,y) \in \mathbb{Z}^2 \mid x^2+4y^2 = n,\ \ y \equiv 0 \pmod 4\}.$$

So we may consider the equation $x^2 + 4y^2 = n$. Among solutions (x, y) of this equations, we decide the number of solutions (x, y) such that $y \equiv 0 \pmod 4$. The reason why we consider this equation instead of the original equation is because the class number of $x^2 + 4y^2$ is one.

In Section 5, we will consider the general case. Finally we summarize all results in Section 6 and provide the closed formula for the number of solutions.

2 Binary Quadratic Forms

Definition 2.1. For fixed integers a, b, c the homogeneous quadratic polynomial

$$F = F(x, y) = ax^2 + bxy + cy^2$$

is called a *binary quadratic form*, or simply a *form*, and is denoted by $\{a,\ b,\ c\}$. The integer

$$d = b^2 - 4ac$$

is called the *discriminant* of the form. It is easy to see that

$$d \equiv 0 \ \text{ or } \ 1 \pmod 4.$$

Definition 2.2. Let $F(x, y)$, $G(x, y)$ be binary forms. If there are integers r, s, t, u such that $ru - st = 1$ and

$$G(X, Y) = F(rX + sY, tX + uY),$$

then two forms F and G are said to be *equivalent*. If F and G are equivalent, we will write $F \cong G$.

We denote by $h(d)$ the number of equivalence classes of primitive forms with discriminant d. From now on we will always assume that every binary form $F(x, y) = ax^2 + bxy + cy^2 (a,\ b,\ c \in \mathbb{Z})$ is positive definite, that is, $a > 0$ and $d < 0$.

Theorem 2.3. *Let k be a positive integer such that $gcd(k, d) = 1$ and denote by $\psi(k)$ the total number of solutions to*

$$k = F_1(x, y), \quad \cdots \quad , F_{h(d)}(x, y),$$

where F_i is a representative of each equivalence class of discriminant d. Then

$$\psi(k) = w \sum_{n|k} \left(\frac{d}{n}\right), \qquad \text{where} \quad w = \begin{cases} 2 & \text{if } d < -4, \\ 4 & \text{if } d = -4, \\ 6 & \text{if } d = -3 \end{cases}$$

and $\left(\frac{d}{n}\right)$ is a Kronecker's symbol.

Proof. See [[2], 12.4.1]. □

For unexplained terminology, notation and basic facts on binary forms we refer the readers to [1] or [2].

3 Some technical lemmas

In this section, we give some technical lemmas that we need in the future.

Theorem 3.1. *Let $n = 2^a m$ for some integers m and a such that m is an odd positive integer and $a \geqslant 1$. Then*

$$\sharp\{(x, y) \in \mathbb{Z}^2 \mid x^2 + 64y^2 = 2^a m\} = \begin{cases} 0 & \text{if } a = 1, 3, 5, \\ 2\sum_{k|m} \left(\frac{-1}{k}\right) & \text{if } a = 2, 4, \\ 4\sum_{k|m} \left(\frac{-1}{k}\right) & \text{otherwise.} \end{cases}$$

Proof. If $a = 1$, then $x^2 + 64y^2 = 2m \equiv 2 \pmod 4$. Clearly there is no solution of this equation. Assume that $a \geqslant 2$. Then x is clearly even. If we put $x = 2s$, then $s^2 + 16y^2 = 2^{a-2}m$. Therefore

$$\sharp\{(x, y) \in \mathbb{Z}^2 \mid \ x^2 + 64y^2 = 2^a m\} = \sharp\{(x, y) \in \mathbb{Z}^2 \mid \ x^2 + 16y^2 = 2^{a-2}m\}.$$

Clearly $d(\{1, 0, 16\}) = -64$ and one may easily check that $h(-64) = 1$. Therefore if $a = 2$,

$$\sharp\{(x, y) \in \mathbb{Z}^2 \mid \ x^2 + 16y^2 = m\} = 2\sum_{k|m} \left(\frac{-64}{k}\right) = 2\sum_{k|m} \left(\frac{-1}{k}\right).$$

If $a = 3$, then $x^2 + 16y^2 = 2m \equiv 2 \pmod 4$. Clearly there is no solution of this equation. Suppose that $a \geqslant 4$. Then the integer x is clearly even. If we put $x = 2t$, then $t^2 + 4y^2 = 2^{a-4}m$. Therefore

$$\sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + 16y^2 = 2^{a-2}m\} = \sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + 4y^2 = 2^{a-4}m\}.$$

Clearly $d(\{1,0,4\}) = -16$ and one may easily check that $h(-16) = 1$. Therefore if $a = 4$,

$$\sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + 4y^2 = m\} = 2\sum_{k|m}\left(\frac{-16}{k}\right) = 2\sum_{k|m}\left(\frac{-1}{k}\right).$$

If $a = 5$, $x^2 + 4y^2 = 2m \equiv 2 \pmod 4$. Clearly there is no solution of this equation. Suppose that $a \geqslant 6$. Then the integer x is even again. Hence

$$\sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + 4y^2 = 2^{a-4}m\} = \sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + y^2 = 2^{a-6}m\}.$$

Note that the class number of $x^2 + y^2$ is one. Therefore if $a = 6$,

$$\sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + y^2 = m\} = 4\sum_{k|m}\left(\frac{-4}{k}\right) = 4\sum_{k|m}\left(\frac{-1}{k}\right).$$

Suppose that $a \geqslant 7$ and (s,t) is an integer solution to $x^2 + y^2 = 2^{a-6}m$. Then

$$\left(\frac{s+t}{2}\right)^2 + \left(\frac{s-t}{2}\right)^2 = \frac{1}{2}\left(s^2 + t^2\right) = 2^{a-7}m.$$

Hence $\left(\frac{s+t}{2}, \frac{s-t}{2}\right)$ is an integer solution of $x^2 + y^2 = 2^{a-7}m$.

Conversely, suppose that (s,t) is an integer solution of $x^2 + y^2 = 2^{a-7}m$. Then

$$(s+t)^2 + (s-t)^2 = 2(s^2 + t^2) = 2^{a-6}m.$$

Hence $(s+t, s-t)$ is an integer solution of $x^2 + y^2 = 2^{a-6}m$. Therefore

$$\begin{aligned}
\sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + y^2 = 2^{a-6}m\} &= \sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + y^2 = 2^{a-7}m\} \\
&= \sharp\{(x,y) \in \mathbb{Z}^2 \mid \ x^2 + y^2 = m\} \\
&= 4\sum_{k|m}\left(\frac{-1}{k}\right).
\end{aligned}$$

This completes the proof. $\square$

Now we consider the case when n is odd. For a binary quadratic form F and a positive integer n, we define

$$R(n,F) := \{(x,y) \in \mathbb{Z}^2 \mid F(x,y) = n\} \quad \text{and} \quad r(n,f) := |R(n,F)|.$$

We can easily show that $d(1,0,64) = -256$ and $h(-256) = 4$. Note that the reduced forms of the classes of discriminant -256 are

$$F_1 = \{1,0,64\},\ F_2 = \{4,4,17\},\ F_3 = \{5,2,13\} \ \text{ and } \ F_4 = \{5,-2,13\}.$$

Then by Theorem 2.3, we have

$$r(n,F_1) + r(n,F_2) + r(n,F_3) + r(n,F_4) = 2\sum_{k|n} \left(\frac{-1}{k}\right).$$

Note that $F_1(x,y) \equiv 0,\ 1,\ 4 \pmod 8$. Hence if $n \neq 1 \pmod 8$, then $r(n,F_1) = 0$. Now suppose that $n \equiv 1 \pmod 8$. Then $r(n,F_3) = r(n,F_4) = 0$. Hence

$$r(n,F_1) + r(n,F_2) = 2\sum_{k|n} \left(\frac{-1}{k}\right).$$

Lemma 3.2. *Let $n = p_1^{e_1} \cdots p_t^{e_t} q_1^{f_1} \cdots q_u^{f_u} s_1^{h_1} \cdots s_w^{h_w}$, where p_i, q_j and s_l are primes such that $p_i \equiv 5 \pmod 8$, $q_j \equiv 1 \pmod 8$ and $s_l \equiv 3 \pmod 4$ and e_i, f_j and h_l are positive integers. If h_l is odd for some l, then $r(n, x^2+64y^2) = 0$. If h_l is even for any l, then*

$$\sharp\{(x,y) \in \mathbb{Z}^2 \mid x^2+64y^2 = n\} = \sharp\{(x,y) \in \mathbb{Z}^2 \mid x^2+64y^2 = p_1^{e_1} \cdots p_t^{e_t} q_1^{f_1} \cdots q_u^{f_u}\}.$$

Proof. Assume that p is a prime such that $p \equiv 3 \pmod 4$. Since -2 is a quadratic non-residue modulo p, for any integers x and y satisfying $x^2 + 64y^2 \equiv 0 \pmod p$, they are divisible by p.

Now assume that x and y are integers such that $x^2 + 64y^2 = n$. Since $s_l \equiv 3 \pmod 4$, both x and y are divisible by s_l by the above observation. Hence there are integers m and n such that

$$m^2 + 64n^2 = p_1^{e_1} \cdots p_t^{e_t} q_1^{f_1} \cdots q_u^{f_u} s_1^{h_1} \cdots s_l^{\delta} \cdots s_w^{h_w},$$

where δ is 0 or 1 such that $\delta \equiv h_l \pmod 2$. The lemma follows directly from this. □

Lemma 3.3. *For any positive integer n such that $n \equiv 1 \pmod 8$,*

$$r(n,F_1) = \sharp\{(x,y) \in \mathbb{Z}^2 \mid x^2 + 4y^2 = n,\ \ y \equiv 0 \pmod 4\}.$$

Proof. Suppose that (s,t) is an integer solution of $x^2+64y^2=n$. Then

$$s^2+4(4t)^2=n.$$

Hence $(s,4t)$ is an integer solution of $x^2+4y^2=n$.

Conversely, suppose that (s,t) is an integer solution of $x^2+4y^2=n$ such that $t\equiv 0 \pmod 4$. Then

$$s^2+64\left(\frac{t}{4}\right)^2=n.$$

Hence $(s,\frac{t}{4})$ is an integer solution of $x^2+64y^2=n$. □

Lemma 3.4. *For any positive integer n such that $n\equiv 1 \pmod 8$,*

$$r(n,F_2)=\sharp\{(x,y)\in\mathbb{Z}^2 \mid x^2+4y^2=n,\ \ y\equiv 2 \pmod 4\}.$$

Proof. Suppose that (s,t) is an integer solution of $4x^2+4xy+17y^2=n$. Then

$$(2s+t)^2+4(2t)^2=n.$$

Hence $(2s+t,2t)$ is an integer solution of $x^2+4y^2=n$.

Conversely, suppose that (s,t) is an integer solution of $x^2+4y^2=n$ such that $t\equiv 2 \pmod 4$. Then

$$4\left(\frac{2s-t}{4}\right)^2+4\left(\frac{2s-t}{4}\right)\left(\frac{t}{2}\right)+17\left(\frac{t}{2}\right)^2=n.$$

Since $2s-t$ is divisible by 4, $(\frac{2s-t}{4},\frac{t}{2})$ is an integer solution of $4x^2+4xy+17y^2=n$. □

Definition 3.5. Two solutions (x_1,y_1), (x_2,y_2) of the equation $x^2+4y^2=n$ are called *essentially different* if

$$(x_1,y_1)\neq(x_2,y_2),\ (x_2,-y_2),\ (-x_2,y_2)\ \text{ and }\ (-x_2,-y_2).$$

Lemma 3.6. *Let k,m,n be positive integers such that $k>1$, $gcd(k,mn)=1$, and $gcd(m,n)=1$. Assume that (x_1,y_1), (x_2,y_2) are the solutions of $x^2+ky^2=n$ and (s_1,t_1), (s_2,t_2) are the solutions of $x^2+ky^2=m$ such that $s_1t_1y_1\neq 0$.*

If at least one pair of the above two equations is essentially different, then both

$$(x_1s_1+ky_1t_1,x_1t_1-y_1s_1),\ (x_1s_1-ky_1t_1,x_1t_1+y_1s_1)$$

and

$$(x_1s_1 \pm ky_1t_1, x_1t_1 \mp y_1s_1),\ (x_2s_2 \pm ky_2t_2, x_2t_2 \mp y_2t_2)$$

are all essentially different solutions of the equation $x^2 + ky^2 = nm$.

Proof. Suppose that

$$(x_1s_1 + ky_1t_1, x_1t_1 - y_1s_1),\ (x_1s_1 - ky_1t_1, x_1t_1 + y_1s_1)$$

are not essentially different solutions of $x^2 + ky^2 = nm$. Then we may assume that, for example,

$$(x_1s_1 + ky_1t_1, x_1t_1 - y_1s_1) = (x_1s_1 - ky_1t_1, x_1t_1 + y_1s_1).$$

Thus $ky_1t_1 = 0$, which is a contradiction. By considering all the other cases similarly to this, we may conclude that both $(x_1s_1 + ky_1t_1, x_1t_1 - y_1s_1)$ and $(x_1s_1 - ky_1t_1, x_1t_1 + y_1s_1)$ are essentially different.

Suppose that

$$(x_1s_1 + ky_1t_1, x_1t_1 - y_1s_1),\ (x_2s_2 + ky_2t_2, x_2t_2 - y_2t_2)$$

are not essentially different solutions of $x^2 + ky^2 = nm$. Then, for example, we have

$$\begin{bmatrix} x_1 & ky_1 \\ -y_1 & x_1 \end{bmatrix} \begin{bmatrix} s_1 \\ t_1 \end{bmatrix} = \begin{bmatrix} x_2 & ky_2 \\ -y_2 & x_2 \end{bmatrix} \begin{bmatrix} s_2 \\ t_2 \end{bmatrix}.$$

Since $x_2^2 + ky_2^2 = n$,

$$\frac{1}{n} \begin{bmatrix} x_2 & -ky_2 \\ y_2 & x_2 \end{bmatrix} \begin{bmatrix} x_1 & ky_1 \\ -y_1 & x_1 \end{bmatrix} \begin{bmatrix} s_1 \\ t_1 \end{bmatrix} = \begin{bmatrix} s_2 \\ t_2 \end{bmatrix}.$$

If we define $\alpha = x_1x_2 + ky_1y_2$ and $\beta = x_1y_2 - x_2y_1$, then we have

$$\begin{bmatrix} \alpha & -k\beta \\ \beta & \alpha \end{bmatrix} \begin{bmatrix} s_1 \\ t_1 \end{bmatrix} = \begin{bmatrix} ns_2 \\ nt_2 \end{bmatrix}.$$

Thus $\alpha s_1 \equiv k\beta t_1 \pmod{n}$ and $\beta s_1 \equiv -\alpha t_1 \pmod{n}$,

$$\alpha(s_1^2 + kt_1^2) \equiv \alpha m \equiv 0 \pmod{n}.$$

Since $gcd(n, m) = 1$, $\alpha = \pm n$ and $\beta = 0$. Therefore

$$x_1 = \pm x_2 \quad \text{and} \quad y_1 = \pm y_2$$

which is a contradiction. All other cases can be done in a similar manner. Therefore

$$(x_1s_1 \pm ky_1t_1, x_1t_1 \mp y_1s_1),\ (x_2s_2 \pm ky_2t_2, x_2t_2 \mp y_2t_2)$$

are essentially different. □

4 Prime power case

Lemma 4.1. *Let e be a positive integer and p be a prime such that $p \equiv 5 \pmod 8$. The equation $x^2+4y^2=p^{2e}$ has an integer solution (x,y) such that $gcd(xy,p)=1$.*

Proof. We will use an induction on e.

Assume that $e=1$. Let a and b be integers such that $a^2+4b^2=p$. Note that such an integer solution always exists. Then $(a^2-4b^2, 2ab)$ is the solution of $x^2+4y^2=p^2$. Clearly $gcd((a^2-4b)\cdot 2ab, p)=1$.

Assume that s and t be integers such that $s^2+4t^2=p^{2e}$ and $gcd(st,p)=1$. Then

$$(s(a^2-4b^2)\pm 4t(2ab) \quad \text{and} \quad s(2ab)\mp t(a^2-4b^2))$$

are all solutions of the equation $x^2+4y^2=p^{2(e+1)}$. Since $4sab$ is not divisible by p, at least one of $s(2ab)-t(a^2-4b^2)$ and $s(2ab)+t(a^2-4b^2)$ is not divisible by p. Hence at least one of $(s(a^2-4b^2)+4t(2ab), s(2ab)-t(a^2-4b^2))$ and $(s(a^2-4b^2)-4t(2ab), s(2ab)+t(a^2-4b^2))$ is the solution of $x^2+4y^2=p^{2(e+1)}$ satisfying the hypothesis. □

Lemma 4.2. *For any positive integer e and a prime p such that $p \equiv 5 \pmod 8$,*

$$\sharp\{(x,y)\in\mathbb{Z}^2 \mid x^2+64y^2=p^{2e}\} = \begin{cases} 2e+2 & \text{if } e\equiv 0 \pmod 2, \\ 2e & \text{if } e\equiv 1 \pmod 2. \end{cases}$$

Proof. Let (s_i,t_i) be a pair of integer solution of $x^2+4y^2=p^{2(e-i)}$ such that $gcd(s_it_i,p)=1$. Note that such a solution always exists by the above lemma. Then

$$(p^is_i, p^it_i) \quad \text{for } i=0,1,\cdots,e-1 \quad \text{and} \quad (p^e,0)$$

are all pairs of mutually essentially different solutions of the equation $x^2+4y^2=p^{2e}$. Furthermore for any solution (s,t) of $x^2+4y^2=p^{2e}$, (s,t) is not essentially different to exactly one of the above solutions. Among all these solutions, we can count the number of solutions such that the y-coordinate is divisible by p.

First, note that $t_{e-1}=2ab$ for integers a and b such that $a^2+4b^2=p$. Hence $t_{e-1}\equiv 2 \pmod 4$. From the proof of the above lemma, we know that

$$t_{e-k-1}=s_{e-k}(2ab)\mp t_{e-k}(a^2-4b^2).$$

In any cases,

$$t_{e-k-1}-t_{e-k}\equiv 2 \pmod 4.$$

Then the number of solutions of $x^2 + 4y^2 = p^{2e}$ such that $y \equiv 0 \pmod 4$ is

$$\begin{cases} 4 \cdot \dfrac{e}{2} + 2 = 2e + 2 & \text{if } e \equiv 0 \pmod 2, \\ 4 \cdot \dfrac{e-1}{2} + 2 = 2e & \text{if } e \equiv 1 \pmod 2. \end{cases}$$

Therefore the lemma directly follows from Lemma 3.3. □

5 General case

In this section we consider the general case. Recall that n is an integer such that $n \equiv 1 \pmod 8$.

Lemma 5.1. *Assume that $n = p_1^{e_1} \cdots p_t^{e_t}$, where p_i is a prime such that $p_i \equiv 5 \pmod 8$ and e_i is a positive integer for any i. Then*

$$r(n, F_1) = \begin{cases} \displaystyle\prod_{i=1}^{t}(e_i + 1) + (-1)^w & \textit{if } e_i \equiv 0 \pmod 2 \textit{ for any } i, \\ \displaystyle\prod_{i=1}^{t}(e_i + 1) & \textit{otherwise}, \end{cases}$$

where $w = \sharp\{i \mid e_i \equiv 2 \pmod 4\}$.

Proof. Since $n \equiv 1 \pmod 8$, $e_1 + \cdots + e_t$ is even.

First assume that there is an i such that $e_i \equiv 1 \pmod 2$. Note that the number of such i's is even. Without loss of generality we assume that $e_1 \equiv e_2 \equiv 1 \pmod 2$. Let

$$(a_1, b_1), \quad \cdots \quad , (a_u, b_u)$$

be all essentially different solutions of $x^2 + 4y^2 = p^{e_1}$ and

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2 + 4y^2 = p_2^{e_2} \cdots p_t^{e_t}$. Since $p_1^{e_1} \equiv p_2^{e_2} \cdots p_t^{e_t} \equiv 5 \pmod 8$, $a_i b_i c_j d_j \equiv 1 \pmod 2$ for any i and j. Furthermore since $4u$ $(4v)$ is the number of solutions of $x^2+4y^2 = p_1^{e_1}$ ($x^2+4y^2 = p_2^{e_2} \cdots p_t^{e_t}$, respectively),

$$u = \frac{1}{2}(e_1 + 1) \quad \text{and} \quad v = \frac{1}{2}(e_2 + 1) \cdots (e_t + 1).$$

Now

$$(a_ic_j + 4b_id_j, a_id_j - b_ic_j) \quad \text{and} \quad (a_ic_j - 4b_id_j, a_id_j + b_ic_j)$$

are all essentially different solutions of $x^2 + 4y^2 = n$ by Lemma 3.6. Hence we have at least $2uv$ essentially different solutions of $x^2 + 4y^2 = n$. Since

$$4 \cdot 2uv = 2(e_1 + 1) \ \cdots \ (e_t + 1),$$

those $2uv$ solutions are exactly all essentially different solutions of $x^2+4y^2 = n$. Since

$$(a_id_j + b_ic_j) - (a_id_j - b_ic_j) = 2b_ic_j \equiv 2 \pmod 4,$$

the number of solutions of $x^2 + 4y^2 = n$ with $y \equiv 0 \pmod 4$ is exactly half of the number of all solutions. This completes the proof.

Now assume that $e_i \equiv 0 \pmod 2$ for any i. We will use an induction on t. We already proved the lemma when $t = 1$. Assume that the formula holds on the case when n has t different prime factors. Consider the equation $x^2 + 4y^2 = p_1^{e_1} \cdots p_t^{e_t} p_{t+1}^{e_{t+1}}$. Let

$$(a_1, b_1), \quad \cdots \quad , (a_u, b_u)$$

be all essentially different solutions of $x^2 + 4y^2 = p_1^{e_1} \cdots p_t^{e_t}$ and

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2 + 4y^2 = p_{t+1}^{e_{t+1}}$. Note that every solution of $x^2 + 4y^2 = p_1^{e_1} \cdots p_t^{e_t} p_{t+1}^{e_{t+1}}$ is not essentially different to exactly one of

$$(a_ic_j + 4b_id_j, a_id_j - b_ic_j) \quad \text{and} \quad (a_ic_j - 4b_id_j, a_id_j + b_ic_j).$$

We assume that $b_1 = d_1 = 0$. Then clearly $b_i > 0$ and $d_j > 0$ for any $i, j \geqslant 2$. We define $\epsilon = 1$ if $e_{t+1} \equiv 2 \pmod 4$, $\epsilon = 0$ otherwise. Furthermore we define

$$\Phi := \prod_{i=1}^{t}(e_i + 1) + (-1)^w, \quad \text{where} \quad w = \sharp\{i \mid \ e_i \equiv 2 \pmod 4\}.$$

Then

$$\alpha := \sharp\{i \mid \ b_i \equiv 0 \pmod 4\} = \frac{1}{4}(\Phi - 2) + 1$$

and

$$\alpha' := \sharp\{i \mid \ d_j \equiv 0 \pmod 4\} = \frac{1}{4}(e_{t+1} + 1 + (-1)^\epsilon - 2) + 1.$$

Now the number of solutions of $x^2+4y^2 = p_1^{e_1}\cdots p_t^{e_t}p_{t+1}^{e_{t+1}}$ with $y \equiv 0 \pmod 4$ is

$$T := 8(\alpha-1)(\alpha'-1) + 4(\alpha-1) + 4(\alpha'-1) + 2 + 8(u-\alpha)(v-\alpha').$$

Since

$$2\prod_{i=1}^{t}(e_i+1) = 2+4(u-1) \quad \text{and} \quad 2(e_{t+1}+1) = 2+4(v-1),$$

$$T = \prod_{i=1}^{t}(e_i+1) + (-1)^{w+\epsilon}.$$

The lemma follows directly from this. □

Let Q be the set of all primes that are represented by x^2+64y^2 and R be the set of all primes that are represented by $4x^2+4xy+17y^2$.

Lemma 5.2. *For any prime p, the equation $x^2+64y^2 = p$ has an integer solution if and only if $p \equiv 1 \pmod 8$ and 2 is biquadratic residue modulo p.*

Proof. See [[1],1.4.23]. □

Example 5.3. Note that

$$Q = \{17, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457, 521, 569, 641\cdots\}.$$

Lemma 5.4. *Let $n = q_1^{f_1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$, where $q_j \in Q$ and $r_k \in R$ for any j, k. Then*

$$r(n, F_1) = \begin{cases} 0 & \text{if} \quad \sum_{k=1}^{v} g_k \equiv 1 \pmod 2, \\ 2\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1) & \text{if} \quad \sum_{k=1}^{v} g_k \equiv 0 \pmod 2. \end{cases}$$

Proof. We will use an induction on $\sum f_j + \sum g_k$.

Assume that $\sum f_j + \sum g_k = 1$. If $f_j = 1$ for some j, then the lemma follows from the fact $q_j \in Q$. If $g_k = 1$ for some k, then the lemma follows from the fact $r_k \in R$. Assume that the formula holds on the case when $\sum f_j + \sum g_k = m$. Assume that $\sum f_j + \sum g_k = m+1$. Note that one of f_j or g_k is greater than or equal to 1. Without loss of generality, we assume that $f_1 \geqslant 1$. Let (a,b) be the solution of $x^2+4y^2=q_1$. Note that $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 4$.

Case 1. Assume that $\sum_{k=1}^{v} g_k \equiv 0 \pmod 2$.

Let (c,d) be the solution of $x^2+4y^2=n$ such that $d \equiv 2 \pmod 4$. Note that $c \equiv 1 \pmod 2$. Then

$$(ac+4bd, ad-bc) \quad \text{and} \quad (ac-4bd, ad+bc)$$

are solutions of $x^2+4y^2 = q_1^{f_1+1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$. Since

$$(ac+4bd)(ac-4bd) \equiv (ac)^2-(4bd)^2 \equiv 0 \pmod{q_1},$$

we may assume, without loss of generality, that $ac+4bd \equiv ad-bc \equiv 0 \pmod{q_1}$. Hence

$$\left(\frac{ac+4bd}{q_1}\right)^2 + 4\left(\frac{ad-bc}{q_1}\right)^2 = q_1^{f_1-1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}.$$

Note that $ad-bc \equiv 2 \pmod 4$. Since $f_1-1+f_2+\cdots+f_u+\sum g_k = n$ and $\sum g_k \equiv 0 \pmod 2$, this is contradiction to the induction hypothesis. Therefore

$$r(n, x^2+4y^2) \;=\; r(n, x^2+64y^2).$$

The lemma follows from this.

Case 2. Assume that $\sum_{k=1}^{v} g_k \equiv 1 \pmod 2$.

Let (c',d') be the solution of $x^2+4y^2=n$ such that $d' \equiv 0 \pmod 4$. Note that $c' \equiv 1 \pmod 2$. Then

$$(ac'+4bd', ad'-bc') \quad \text{and} \quad (ac'-4bd', ad'+bc')$$

are solutions of $x^2+4y^2 = q_1^{f_1+1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$. Since

$$(ac'+4bd')(ac'-4bd') \equiv (ac')^2-(4bd')^2 \equiv 0 \pmod{q_1},$$

we may assume, without loss of generality, that $ac'+4bd' \equiv ad'-bc' \equiv 0 \pmod{q_1}$. Hence

$$\left(\frac{ac'+4bd'}{q_1}\right)^2 + 4\left(\frac{ad'-bc'}{q_1}\right)^2 = q_1^{f_1-1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}.$$

Note that $ad' - bc' \equiv 0 \pmod 4$. Since $f_1 - 1 + f_2 + \cdots + f_u + \sum g_k = n$ and $\sum g_k \equiv 1 \pmod 2$, this is impossible by induction hypothesis. Therefore

$$r(n, x^2 + 4y^2) \;=\; r(n, 4x^2 + 4xy + 17y^2) \quad \text{and} \quad r(n, x^2 + 64y^2) = 0.$$

The lemma follows from this. □

Theorem 5.5. *Let $n = p_1^{e_1} \cdots p_t^{e_t} q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$, where p_i, q_j, r_k are all primes such that $q_j \in Q, r_k \in R$ and $p_i \equiv 5 \pmod 8$ and e_i, f_j, g_k are all positive integers. If $e_1 + \cdots + e_t \equiv 1 \pmod 2$, then $r(n, x^2 + 64y^2) = 0$. If $e_1 + \cdots + e_t \equiv 0 \pmod 2$, then*

$\sharp\{(x, y) \in \mathbb{Z}^2 \mid x^2 + 64y^2 = n\} =$

$$\begin{cases} \prod_{j=1}^{u}(f_j + 1)\prod_{k=1}^{v}(g_k + 1)\left(\prod_{i=1}^{t}(e_i + 1) + (-1)^{w+1}\right) & \text{if } (*) \text{ holds,} \\ \prod_{j=1}^{u}(f_j + 1)\prod_{k=1}^{v}(g_k + 1)\left(\prod_{i=1}^{t}(e_i + 1) + (-1)^{w}\right) & \text{if } (**) \text{ holds,} \\ \prod_{j=1}^{u}(f_j + 1)\prod_{k=1}^{v}(g_k + 1)\prod_{i=1}^{t}(e_i + 1) & \text{otherwise,} \end{cases}$$

where $w = \sharp\{e_i \mid e_i \equiv 2 \pmod 4\}$,

$$(*) \quad e_i \equiv 0 \pmod 2 \ \text{ for any } i \ \text{ and } \ \sum_{k=1}^{v} g_k \equiv 1 \pmod 2 \quad \text{and}$$

$$(**) \quad e_i \equiv 0 \pmod 2 \ \text{ for any } i \ \text{ and } \ \sum_{k=1}^{v} g_k \equiv 0 \pmod 2.$$

Proof. First assume that there is an i such that $e_i \equiv 1 \pmod 2$. Note that the number of such i's is even. Without loss of generality we assume that $e_1 \equiv e_2 \equiv 1 \pmod 2$. Let

$$(a_1, b_1), \quad \cdots \quad , (a_u, b_u)$$

be all essentially different solutions of $x^2 + 4y^2 = p_1^{e_1} \cdots p_t^{e_t}$. Since the number of solutions of $x^2 + 4y^2 = p_1^{e_1} \cdots p_t^{e_t}$ is $4u$, we have

$$u = \frac{1}{2}\prod_{i=1}^{t}(e_i + 1).$$

By Lemma 5.1, we have

$$\alpha := \sharp\{i \mid \ b_i \equiv 0 \pmod 4\} = \frac{1}{2}u.$$

Now we consider the following three subcases.

Case 1. Assume that $\sum_{k=1}^{v} g_k \equiv 1 \pmod 2$.

Let

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2+4y^2 = q_1^{f_1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$. Note that $d_j \equiv 2 \pmod 4$ for any j by Lemma 5.4. Since the number of solutions of $x^2+4y^2 = q_1^{f_1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$ is $4v$, we have

$$v = \frac{1}{2}\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1).$$

Then

$$(a_ic_j + 4b_id_j, a_id_j - b_ic_j) \quad \text{and} \quad (a_ic_j - 4b_id_j, a_id_j + b_ic_j)$$

are all essentially different solutions of $x^2+4y^2 = n$ by Lemma 3.6. Note that $a_id_j \mp b_ic_j \equiv 0 \pmod 4$ for any i, j when $b_i \equiv 2 \pmod 4$ for any i. Hence

$$\begin{aligned} r(n, F_1) &= 8(u-\alpha)v \\ &= \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\prod_{i=1}^{t}(e_i+1). \end{aligned}$$

Case 2. Assume that $\sum_{k=1}^{v} g_k \equiv 0 \pmod 2$ and f_j and g_k are even for all j,k.

Let

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2+4y^2 = q_1^{f_1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$. Note that $d_j \equiv 0 \pmod 4$ for any j by Lemma 5.4. We assume that $d_1 = 0$. Then clearly $d_j > 0$ for any $j \geqslant 2$. Since the number of solutions of $x^2+4y^2 = q_1^{f_1}\cdots q_u^{f_u} r_1^{g_1}\cdots r_v^{g_v}$ is $4v-2$, we have

$$v = \frac{1}{2}\left(\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)+1\right).$$

Then

$$(a_ic_j + 4b_id_j, a_id_j - b_ic_j),\ (a_ic_j - 4b_id_j, a_id_j + b_ic_j) \quad \text{and} \quad (a_ic_1, \mp b_ic_1)$$

are all essentially different solutions of $x^2 + 4y^2 = n$ by Lemma 3.6. Note that $a_id_j \mp b_ic_j \equiv 0 \pmod 4$ for any i, j and $\mp b_ic_1 \equiv 0 \pmod 4$ for any i when $b_i \equiv 0 \pmod 4$ for any i. Hence

$$\begin{aligned} r(n, F_1) &= 8\alpha(v-1) + 4\alpha \\ &= \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\prod_{i=1}^{t}(e_i+1). \end{aligned}$$

Case 3. Assume that $\sum_{k=1}^{v} g_k \equiv 0 \pmod 2$ and f_j or g_k is odd for some j or k. Let

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2 + 4y^2 = q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$. Note that $d_j \equiv 0 \pmod 4$ for all j by Lemma 5.4. Since the number of solutions of $x^2 + 4y^2 = q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$ is $4v$, we have

$$v = \frac{1}{2}\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1).$$

Then

$$(a_ic_j + 4b_id_j, a_id_j - b_ic_j) \quad \text{and} \quad (a_ic_j - 4b_id_j, a_id_j + b_ic_j)$$

are all essentially different solutions of $x^2+4y^2 = n$ by Lemma 3.6. Note that $a_id_j \mp b_ic_j \equiv 0 \pmod 4$ for any i, j when $b_i \equiv 0 \pmod 4$ for any i. Hence

$$\begin{aligned} r(n, F_1) &= 8\alpha v \\ &= \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\prod_{i=1}^{t}(e_i+1). \end{aligned}$$

This completes the proof.

Now assume that $e_i \equiv 0 \pmod 2$ for any i. Let

$$(a_1, b_1), \quad \cdots \quad , (a_u, b_u)$$

be all essentially different solutions of $x^2+4y^2=p_1^{e_1}\cdots p_t^{e_t}$. We assume that $b_1=0$. Then clearly $b_i>0$ for any $i\geqslant 2$. Since the number of solutions of $x^2+4y^2=p_1^{e_1}\cdots p_t^{e_t}$ is $4u-2$, we have

$$u=\frac{1}{2}\left(\prod_{i=1}^{t}(e_i+1)+1\right).$$

Furthermore by Lemma 5.1, if we define

$$\Phi:=\prod_{i=1}^{t}(e_i+1)+(-1)^w,\quad \text{where}\ \ w=\sharp\{i\mid\ e_i\equiv 2\pmod 4\},$$

then

$$\alpha:=\sharp\{i\mid\ b_i\equiv 0\pmod 4\}=\frac{1}{4}(\Phi-2)+1.$$

Now we consider the following three subcases.

Case 1. Assume that $\sum_{k=1}^{v} g_k\equiv 1\pmod 2$.

Let

$$(c_1,d_1),\quad\cdots\quad,(c_v,d_v)$$

be all essentially different solutions of $x^2+4y^2=q_1^{f_1}\cdots q_u^{f_u}r_1^{g_1}\cdots r_v^{g_v}$. Note that $d_j\equiv 2\pmod 4$ for any j by Lemma 5.4. Since the number of solutions of $x^2+4y^2=q_1^{f_1}\cdots q_u^{f_u}r_1^{g_1}\cdots r_v^{g_v}$ is $4v$, we have

$$v=\frac{1}{2}\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1).$$

Then

$$(a_ic_j+4b_id_j,a_id_j-b_ic_j),\ (a_ic_j-4b_id_j,a_id_j+b_ic_j)\quad\text{and}\quad(a_1c_j,\mp a_1d_j)$$

are all essentially different solutions of $x^2+4y^2=n$ by Lemma 3.6. Note that $a_id_j\mp b_ic_j\equiv 0\pmod 4$ for any i, j when $b_i\equiv 2\pmod 4$ for any i and $\mp a_1d_j\equiv 2\pmod 4$ for any j. Hence

$$\begin{aligned} r(n,F_1) &= 8(u-\alpha)v\\ &= \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\left(\prod_{i=1}^{t}(e_i+1)+(-1)^{w+1}\right). \end{aligned}$$

Case 2. Assume that $\sum_{k=1}^{v} g_k\equiv 0\pmod 2$ and f_j and g_k are even for all j,k.

Let

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2 + 4y^2 = q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$. Note that $d_j \equiv 0 \pmod 4$ for any j by Lemma 5.4. We assume that $d_1 = 0$. Then clearly $d_j > 0$ for any $j \geqslant 2$. Since the number of solutions of $x^2 + 4y^2 = q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$ is $4v - 2$, we have

$$v = \frac{1}{2}\left(\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)+1\right).$$

Then

$$(a_i c_j \pm 4b_i d_j, a_i d_j \mp b_i c_j),\ (a_1 c_j, \mp a_1 d_j),\ (a_i c_1, \mp b_i c_1) \quad \text{and} \quad (a_1 c_1, 0)$$

are all essentially different solutions of $x^2 + 4y^2 = n$ by Lemma 3.6. Note that $a_i d_j \mp b_i c_j \equiv 0 \pmod 4$ and $\mp b_i c_1 \equiv 0 \pmod 4$ for any i, j when $b_i \equiv 0 \pmod 4$ for any i and $\mp a_1 d_j \equiv 0 \pmod 4$ for any j. Hence

$$\begin{aligned} r(n, F_1) &= 8(\alpha-1)(v-1) + 4(\alpha-1) + (v-1) + 2 \\ &= \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\left(\prod_{i=1}^{t}(e_i+1) + (-1)^w\right). \end{aligned}$$

Case 3. Assume that $\sum_{k=1}^{v} g_k \equiv 0 \pmod 2$ and f_j or g_k is odd for some j or k.

Let

$$(c_1, d_1), \quad \cdots \quad , (c_v, d_v)$$

be all essentially different solutions of $x^2 + 4y^2 = q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$. Note that $d_j \equiv 0 \pmod 4$ for any j by Lemma 5.4. Since the number of solutions of $x^2 + 4y^2 = q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v}$is $4v$, we have

$$v = \frac{1}{2}\prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1).$$

Then

$$(a_i c_j + 4b_i d_j, a_i d_j - b_i c_j),\ (a_i c_j - 4b_i d_j, a_i d_j + b_i c_j) \quad \text{and} \quad (a_1 c_j, \mp a_1 d_j)$$

are all essentially different solutions of $x^2 + 4y^2 = n$ by Lemma 3.6. Note that $a_i d_j \mp b_i c_j \equiv 0 \pmod 4$ for any i, j when $b_i \equiv 0 \pmod 4$ for any i and $\mp a_1 d_j \equiv 0 \pmod 4$ for any j. Hence

$$\begin{aligned} r(n, F_1) &= 8(\alpha - 1)v + 4v \\ &= \prod_{j=1}^{u}(f_j + 1)\prod_{k=1}^{v}(g_k + 1)\left(\prod_{i=1}^{t}(e_i + 1) + (-1)^w\right). \end{aligned}$$

The theorem follows directly from this. □

6 Summary

In this section, we summarize all results proved in the previous sections and give a closed formula for the number of solutions of the equation $x^2 + 64y^2 = n$.

Assume that n is even. Let $n = 2^a m$ for some integers m and a such that m is an odd positive integer and $a \geqslant 1$. Then

$$\sharp\{(x, y) \in \mathbb{Z}^2 \mid x^2 + 64y^2 = n\} = \begin{cases} 0 & \text{if } a = 1, 3, 5, \\ 2\sum_{k|m}\left(\frac{-1}{k}\right) & \text{if } a = 2, 4, \\ 4\sum_{k|m}\left(\frac{-1}{k}\right) & \text{otherwise.} \end{cases}$$

Assume that n is odd. Let $n = p_1^{e_1} \cdots p_t^{e_t} q_1^{f_1} \cdots q_u^{f_u} r_1^{g_1} \cdots r_v^{g_v} s_1^{h_1} \cdots s_w^{h_w}$, where p_i, q_j, r_k, s_l are all primes such that $q_j \in Q, r_k \in R$ and $p_i \equiv 5 \pmod 8$, $s_l \equiv 3 \pmod 4$ and e_i, f_j, g_k, h_l are all positive integers. If h_l is odd for some l, then $r(n, x^2 + 64y^2) = 0$. If h_l is even for any l, then

$$\sharp\{(x, y) \in \mathbb{Z}^2 \mid x^2+64y^2 = n\} = \sharp\{(x, y) \in \mathbb{Z}^2 \mid x^2+64y^2 = p_1^{e_1} \cdots p_t^{e_t} q_1^{f_1} \cdots q_u^{f_u}\}.$$

If $e_1 + \cdots + e_t \equiv 1 \pmod 2$, then $r(n, x^2 + 64y^2) = 0$. If $e_1 + \cdots + e_t \equiv 0 \pmod 2$, then

$\sharp\{(x,y)\in\mathbb{Z}^2 \mid x^2+64y^2=n\} =$

$$\begin{cases} \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\left(\prod_{i=1}^{t}(e_i+1)+(-1)^{w+1}\right) & \text{if } (*) \text{ holds,} \\ \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\left(\prod_{i=1}^{t}(e_i+1)+(-1)^{w}\right) & \text{if } (**) \text{ holds,} \\ \prod_{j=1}^{u}(f_j+1)\prod_{k=1}^{v}(g_k+1)\prod_{i=1}^{t}(e_i+1) & \text{otherwise,} \end{cases}$$

where $w=\sharp\{e_i \mid e_i\equiv 2 \pmod 4\}$,

$(*)$ $e_i\equiv 0 \pmod 2$ for any i and $\sum_{k=1}^{v} g_k \equiv 1 \pmod 2$ and

$(**)$ $e_i\equiv 0 \pmod 2$ for any i and $\sum_{k=1}^{v} g_k \equiv 0 \pmod 2$.

References

[1] D. A. Cox, *Primes of the form* x^2+ny^2, John-Wiley and Sons, 1989.

[2] L. K. Hua, *Introduction to number theory*, Springer-Verlag, 1982.

[3] S.-Y. Min and B.-K. Oh, *The number of integer solutions of* $x^2+32y^2=n$, In preperation.

[4] Z.-H. Sun and K. S. Williams, *On the number of representations of* n *by* $ax^2+bxy+cy^2$, Acta Arith. 122(2006), 101-171.

국문초록

동차 이차방정식 $F(x,y) = ax^2+bxy+cy^2$ 을 이변수 이차형식이라 한다. 이 논문에서는 류수가 4인 이차형식 $F(x,y) = x^2+64y^2$ 을 다룬다. 이 논문의 목적은 임의의 정수 n에 대하여 $F(x,y) = n$의 해의 개수에 대한 명확한 공식을 제공하는 것이다. 그러기 위해서 S.-Y. Min와 B.-K. Oh가 증명하는 방법을 채택한다. 제5절에서는 앞 절에서 증명된 모든 결과를 정리하고 앞에서 언급한 이차형식의 해의 개수에 대한 공식을 명확하게 제시한다.

주요 어휘 : 류수4, 이변수 이차형식
학번: 2011-20265