이학석사 학위논문

Multiples of a prime represented by some binary forms

(이변수 이차형식으로 표현되는 소수의 배수들)

2014년 8월

서울대학교 대학원

수리과학부

전 계 정

Multiples of a prime represented by some binary forms

(이변수 이차형식으로 표현되는 소수의 배수들)

지도교수 오 병 권

이 논문을 이학석사 학위논문으로 제출함

2014년 6월

서울대학교 대학원

수리과학부

전 계 정

전 계 정의 이학석사 학위논문을 인준함

2014년 6월

위 원 장 _____ (인)

부 위 원 장 _____ (인)

위 원 _____ (인)

Multiples of a prime represented by some binary forms

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Master of Science
to the faculty of the Graduate School of
Seoul National University

by

GEAJEONG JEON

Dissertation Director : Professor Byeong-Kweon Oh

Department of Mathematical Sciences
Seoul National University

August 2014

Abstract

For a (positive definite integral) binary form $f(x,y) = ax^2 + bxy + cy^2$, the set of integers n such that $f(x,y) = n$ has an integer solution is defined by $Q(f)$. In 1938, Delone proved that two inequivalent binary forms f and g satisfy $Q(f) = Q(g)$ if and only if $(f,g) \simeq (x^2 + xy + y^2,\ x^2 + 3y^2)$. Recently, Oh found a simple criterion on binary forms f and g satisfying $Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}$, for any prime p. In this thesis, we find all binary forms f and g such that $Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}$ for any prime less than or equal to 13 by using Oh's criterion, where $D_f \equiv 5 \pmod 8$, $4D_f = D_g$ and $\left(\frac{D_f}{p}\right) = 1$.

Key words: Multiples of a prime, Representations of binary quadratic forms
Student Number: 2007-20287

Contents

Chapter 1

Introduction

For fixed $a, b, c \in \mathbb{Z}$, the homogeneous quadratic polynomial

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

is called a binary quadratic form and is denoted by $[a, b, c]$. For an integer n, if there are integers a, b such that $f(a, b) = n$, then we say that n is represented by f. Let $Q(f)$ be the set of all integers that are represented by f. It has a long and rich history on deciding the set $Q(f)$ since Fermat's theorem on the representation by a sum of two squares. If the class number (the number of equivalence classes in the genus) of a form f is one, then the set $Q(f)$ is determined by its local structure. So in this case, it is quite easy to determine the set $Q(f)$. However if the class number of f is bigger than 1, there is no simple method on deciding the set $Q(f)$ as far as the author knows.

In 1938, Delone proved in [4] that for two positive definite primitive integral binary forms f and g, $Q(f) = Q(g)$ if and only if f is equivalent to g or, as an exceptional case, the pair (f, g) is equivalent to $(x^2+xy+y^2,\ x^2+3y^2)$. This result means that the set of integers that are represented by a positive definite binary quadratic form decides the form itself except the sole case. This result was generalized to indefinite case in [5]. As a natural generalization of this result, one may consider the set of an arithmetic progression instead of the set of integers that are represented by a form. Recently, Oh gave a simple criterion in [6] on finding all pairs of reduced forms (f, g) such that $Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}$ for any prime p.

In this thesis, we just focus on finding all pairs of reduced forms $(f, g) \simeq ([a, b, a], [4a, 2b, a])$ such that $Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}$ for any prime p less than or equal 13, where $D_f \equiv 5 \pmod 8$, $4D_f = D_g$, $\left(\frac{D_f}{p}\right) = 1$, and p^2 is represented by $\left[4, 2, \frac{1-D_f}{4}\right]$. To do this, we will use Oh's criterion. In fact there are only finitely many pairs (f, g) satisfying the above property for any prime p.

In Chapter 2, we introduce basic terminologies and theories of binary quadratic forms. We define the class number $h(f)$ of a binary form f and provide a simple method on finding all binary forms with discriminant given in advance.

In Chapter 3, we establish the existence of a group law on the proper equivalence classes of primitive forms of the given discriminant D and develop its main properties. The group law is called composition, which was introduced by Gauss. We also introduce ambiguous classes and ambiguous forms. It is well known that if D is an odd integer less than -4, then the number of ambiguous classes with discriminant D is $2^{\lambda(D)-1}$, where $\lambda(D)$ is the number of odd prime factors of D. This fact plays an important role on computing the number of pairs (f, g) that we want to find in this thesis.

In Chapter 4, we compute all reduced forms (f, g) satisfying all assumptions given above for any prime p less than or equal 13. The results will be summarized in Tables (4.1) to (4.5).

Any unexplained notations and terminologies on binary quadratic forms can be found on [1] and [2].

Chapter 2

Basic theory of Binary Quadratic Form

In this chapter, we introduce some notations and terminologies on binary quadratic forms.

Definition 2.0.1. For fixed $a, b, c \in \mathbb{Z}$, the homogeneous quadratic polynomial

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

is called a *binary quadratic form* and is denoted by $[a, b, c]$. The integer

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

is called the discriminant of the form.

We note that $D_f \equiv 0$ or $1 \pmod 4$. For the binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, let M_f be the symmetric matrix $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. From the definition, we have $D_f = -4 \cdot \det(M_f)$. If D_f is a perfct square, then f is factorized into a product of two linear forms with integer coefficients. From now on, we always assume that D_f is not a perfect square.

Definition 2.0.2. For a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$,

(1) if $D_f < 0$ and $a > 0$, then $4af(x, y) = (2ax+by)^2 - D_f y^2$ and so $f(x, y) \geq 0$ for any $(x, y) \in \mathbb{Z}^2$. Furthermore $f(x, y) = 0$ if and only if $x = y = 0$. The binary form f is called *positive definite* if it satisfies this condition.

(2) If $D_f < 0$ and $a < 0$, then $4af(x,y) = (2ax+by)^2 - D_f y^2$ and so $f(x,y) \leq 0$ for any $(x,y) \in \mathbb{Z}^2$. The binary form f is called *negative definite* if it satisfies this condition.

(3) If $D_f > 0$, then f is called *indefinite*. Note that if f is indefinite, then the values $f(x,y)$ could be both positive and negative according to the integers x, y.

Definition 2.0.3. For two binary quadratic forms f and g, if there is a matrix $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ such that $M_f = T^t \cdot M_g \cdot T$, then we say that f is *equivalent* to g, and is denoted by $f \sim g$. In particular, we say that f is *proper equivalent* to g if $\det(T) = 1$, and f is *improper equivalent* to g if $\det(T) = -1$.

Assume that a binary form f is equivalent to g. Clearly $D_f = D_g$. Furthermore f is positive definite if and only if g is positive definite. For a binary form f, the set of binary forms equivalent to f is called the class of f.

Theorem 2.0.4. *In every class $\mathscr{C}$ of forms, there is always a form $[a,b,c] \in \mathscr{C}$ which satisfies the condition*

$$|b| \leq |a| \leq |c| .$$

Proof. See [1]. □

Theorem 2.0.5. *The number of classes with discriminant D is finite.*

Proof. See [1]. □

Theorem 2.0.6. *The number of classes of positive definite forms with discriminant D is equal to the number of the set of integers a, b, c satisfying*

$$b^2 - 4ac = D, \qquad \begin{cases} -a < b \leq a < c \quad or \\ 0 \leq b \leq a = c. \end{cases} \qquad \cdots (1)$$

Proof. See [1]. □

From now on, we always assume that a binary quadratic form is positive definite and integral.

Definition 2.0.7. A binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ satisfying the condition (1) of Theorem 2.0.6 is called a *reduced form*.

Definition 2.0.8. For a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$, we say that the form f is *primitive* if $(a,b,c) = 1$, and is *imprimitive* if $(a,b,c) > 1$.

Let $(a,b,c) = g > 1$. Clearly $\left[\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right]$ is a primitive form with discriminant $\frac{D}{g^2}$. Also if a form f is equivalent to a primitive form g, then f is also primitive. From now on, we deote by $h(D)$ the number of classes of primitive forms with discriminant D. Then the number of classes of forms with discriminant D is equal to $\sum_{g^2|D, g>0} h\left(\frac{D}{g^2}\right)$.

Definition 2.0.9. For an integer n and a binary quadratic form $f(x,y)$, if there are integers a and b such that $f(a,b) = n$, then we say that n is represented by $f(x,y)$. The set of integer solutions (x,y) which satisfy $f(x,y) = n$ is denoted by $R(n,f)$, that is, $R(n,f) = \{(x,y) \in \mathbb{Z}^2 \mid f(x,y) = n\}$. If $(a,b) \in R(n,f)$ and $\gcd(a,b) = 1$, then we say that (a,b) is a *proper solution*.

Definition 2.0.10. For a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$, the set of integer that are represented by f is denoted by $Q(f)$.

Lemma 2.0.11. *For binary quadratic forms f and g, if they are in the same class, then $Q(f) = Q(g)$.*

Proof. If n is represented by f, then there is an integer solution $(a,b) \in \mathbb{Z}^2$ such that $f(a,b) = n$. From the assumption that $f \sim g$, there is a matrix $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ such that $\det T = \pm 1$ and $f(a,b) = g(ra+sb, ta+ub)$. Since $g(ra+sb,\ ta+ub) = f(a,b) = n$ and $ra+sb, ta+ub \in \mathbb{Z}$. Hence n is represented by g. This implies that $Q(f) \subset Q(g)$. The converse is trivial. $\square$

Chapter 3

Composition of binary quadratic forms

3.1 Composition law of binary forms

In this section, we establish the existence of a group law on the proper equivalence classes of primitive forms of the given discriminant D and develop its main properties. This group law is traditionally called *composition*.

Lemma 3.1.1. *For a primitive form $f = [a, b, c]$, f represents an integer prime to M, for any integer M.*

Proof. See [2]. □

Lemma 3.1.2. *For two equivalent primitive forms $f = [a_1, b, c_1]$ and $g = [a_2, b, c_2]$, if there is an integer l such that $l \mid c_1$, $l \mid c_2$ and $gcd(a_1, a_2, l) = 1$, then $[la_1, b, l^{-1}c_1] \sim [la_2, b, l^{-1}c_2]$.*

Proof. See [2]. □

Definition 3.1.3. For two primitive forms $f_1 = [a_1, b_1, c_1]$ and $f_2 = [a_2, b_2, c_2]$ with discriminant D, we say that they are *concordant* if

(1) $a_1 a_2 \neq 0$;

(2) $b_1 = b_2 = b$;

(3) the form $f_3 = [a_1a_2, b, *]$ with discriminant D is integral.

The form f_3 is also primitive and we call the form f_3 is the *composition* of f_1 and f_2. When a_1 and a_2 are coprime, the condition (3) follows automatically from (1) and (2). Note that the $*$ in (3) is determined by a_1a_2, b and D. From now on, we will use this character if it is determined by the other coefficients and the discriminant.

Lemma 3.1.4. *For two classes $\mathscr{C}_1$ and $\mathscr{C}_2$ of primitive forms with discriminant $D \neq 0$, there are concordant forms $f_1 = [a_1, b, *] \in \mathscr{C}$ and $f_2 = [a_2, b, *] \in \mathscr{C}$ such that*

$$gcd(a_1, a_2) = gcd(a_1, M) = gcd(a_2, M) = 1 \text{ for any given integer } M.$$

Proof. See [2]. □

Lemma 3.1.5. *For two classes $\mathscr{C}_1$ and $\mathscr{C}_2$ of primitive forms with discriminant $D \neq 0$, there is a class $\mathscr{C}$ such that the composition of $f_1 \in \mathscr{C}_1$ and $f_2 \in \mathscr{C}_2$ always lies in $\mathscr{C}$.*

Proof. See [2]. □

Theorem 3.1.6. *For two primitive classes $\mathscr{C}_1$ and $\mathscr{C}_2$ with discriminant D, we write*

$$\mathscr{C} = \mathscr{C}_1\mathscr{C}_2,$$

where $\mathscr{C}$ is the class given by Lemma 3.1.5. This rule of composition gives the structure of a finite abelian group to the set of primitive classes of discriminant D. Further, the inverse $\mathscr{C}^{-1}$ of the class $\mathscr{C}$ is the class containing the forms which are improperly equivalent to one of forms in $\mathscr{C}$.

Proof. See [2]. □

Definition 3.1.7. The finite abelian group in theorem 3.1.6 is called G_D. The order of this group G_D is denoted by $h(D)$, which is the class number called of a primitive form with discriminant D.

One may easily show that the identity class $\mathscr{E}$ of G_D is the class containing the form $x^2 - \frac{D}{4}y^2$ if D is even, $x^2 + xy + \frac{1-D}{4}$ otherwise.

Example 3.1.8. For $D_f = -96$, one may easily compute by using Theorem 2.0.6 that $h(-96) = 4$.
Let $G_{-96} = \{\mathscr{E},\ \mathscr{C}_1,\ \mathscr{C}_2,\ \mathscr{C}_3\}$. Then the four reduced primitive forms contained in each class are

$$f_0 = [1,0,24] \in \mathscr{E},\ f_1 = [3,0,8] \in \mathscr{C}_1,\ f_2 = [5,2,5] \in \mathscr{C}_2,\ f_3 = [4,4,7] \in \mathscr{C}_3.$$

Then we have

$$f_1 \cdot f_1 = [3,0,8] \cdot [3,0,8] \sim [3,0,8] \cdot [8,0,3] \sim [24,0,1] \sim [1,0,24] = f_0,$$

$$f_2 \cdot f_2 = [5,2,5] \cdot [5,2,5] \sim [5,2,5] \cdot [1,2,25] \sim [5,2,1] \sim [1,0,24] = f_0,$$

$$f_3 \cdot f_3 = [4,4,7] \cdot [4,4,7] \sim [4,52,175] \cdot [7,52,100] \sim [28,52,25] \sim [1,0,24] = f_0.$$

This computation implies that the group G_{-96} is isomorphic to the direct product of two copies of $\mathbb{Z}/2\mathbb{Z}$, i.e, $G_{-96} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

3.2 Ambiguous forms and classes

Definition 3.2.9. The classes $\mathscr{C}$ such that $\mathscr{C}^2 = \mathscr{E}$ or $\mathscr{C}^{-1} = \mathscr{C}$ are called *ambiguous classes*, where $\mathscr{E}$ is the identity class. They are the classes which are improperly equivalent to themselves by Theorem 3.1.6.

It is well known that an improper automorph S of a form f, if exists, satisfies

$$S^2 = I.$$

Hence there exists a primitive vector b such that

$$Sb = -b,$$

and this can be extended to a basis $a, b \in \mathbb{Z}^2$ with $\det(a, b) = 1$. Furthermore there is an integer w such that

$$Sa = a + wb.$$

First if we replace the basis $\{a, b\}$ by $\{a+ub, b\}$, then w is replaced by $w-2u$ for any integer u. Hence we may suppose that

$$w = 0 \text{ or } 1$$

without loss of generality. Thus f is equivalent to one of the two types

$$f_a = [a, 0, c],\ D_{f_a} = -4ac;$$

$$g_a = [a, a, c],\ D_{g_a} = a^2 - 4ac.$$

We shall consider these as *ambiguous forms* of the first and second kind, respectively.

Lemma 3.2.10. *Every ambiguous class contains at least one ambiguous form.*

Proof. See [2]. □

Lemma 3.2.11. *Let D be a negative integer such that $D \equiv 1 \pmod 4$ and let $\lambda(D)$ be the number of distinct odd prime divisors of D. Then the number of positive definite ambiguous forms having discriminant D is $2^{\lambda(D)}$.*

Proof. See [2]. □

Definition 3.2.12. For a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, we define

$$O(f) = \{T \in GL_2(\mathbb{Z}) \mid M_f = T^t \cdot M_f \cdot T\},$$
$$O^+(f) = \{T \in SL_2(\mathbb{Z}) \mid M_f = T^t \cdot M_f \cdot T\},$$

where M_f is the symmetric matrix corresponding to f. The group $O(f)$ is called the automorphism group(or isometry group) of the form f and $O^+(f)$ is called the proper automorphism group of the form f.

Lemma 3.2.13. *For a positive definite binary quadratic form $f(x, y)$ with discriminant D,*

(1) *if $D = -3$, then $|O^+(f)| = 6$;*

(2) *if $D = -4$, then $|O^+(f)| = 4$;*

(3) *if $D < -4$, then $|O^+(f)| = 2$ and $O^+(f) = \{\pm I_2\}$.*

Proof. See [1]. □

Theorem 3.2.14. *If D is an odd integer less than -4, then the number of ambiguous classes with discriminant D is $2^{\lambda(D)-1}$.*

Proof. For a proper automorphism group O^+, it is well known that the number of ambiguous forms in a given ambiguous class is $\left|O^+/\left(O^+\right)^2\right|$. The theorem follows directly from Lemmas 3.2.11 and 3.2.13. □

We will use this theorem to compute the number of pairs that we want to find in the next chapter.

Chapter 4

Representations of multiples of a prime

4.1 Represention of binary forms

For any integral binary quadratic form f and a prime p, we may consider f as a binary form defined over the p-adic integer ring $\mathbb{Z}_p$. In that case, we will use the notation f_p.

Let f and g be positive definite binary forms and let p be an odd prime. Assume that

$$Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}. \tag{4.1.1}$$

Then one may easily show that $f_q \simeq g_q$ for any prime $q \neq p, 2$. Furthermore $f_p \simeq [0,1,0]$ if and only if $g_p \simeq [0,1,0]$. If $f_p \not\simeq [0,1,0]$, then one may easily show that

$$\lambda_p(f) \simeq \lambda_p(g) \quad \text{or} \quad (\lambda_p(f), \lambda_p(g)) \simeq ([1,1,1],\ [1,0,3]),$$

where λ_p is the Watson transformation (for the definition, see [6]).

From now on, we assume that

$$f_p \simeq g_p \simeq [0,1,0]. \tag{4.1.2}$$

Note that this condition is equivalent to

$$\left(\frac{D_f}{p}\right) = \left(\frac{D_g}{p}\right) = 1.$$

When $f_2 \simeq g_2$, such pairs satisfying (4.1.1) are classified in [6] and [7] for small primes. Now we assume that $f_2 \not\simeq g_2$. In this case, one may easily show that

$$(f_2, g_2) \simeq ([1,1,1],[1,0,3]).$$

Without loss of generality, we assume that

$$f_2 \simeq [1,1,1] \quad \text{and} \quad g_2 \simeq [1,0,3]. \tag{4.1.3}$$

This condition is equivalent to $D_f \equiv 5 \pmod 8$ and $D_g \equiv 20 \pmod{32}$. Under this condition, Oh proved in [6] that:

Theorem 4.1.1. *(Oh) Under the assumptions that*

$$f_p \simeq g_p \simeq [0,1,0], \quad f_2 \simeq [1,1,1] \quad \textit{and} \quad g_2 \simeq [1,0,3],$$

$Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}$ *if and only if there are odd integers* a, b *such that* $f \sim [a,b,a], g \sim [4a,2b,a]$ *and* p^2 *is represented by* $\left[4, 2, \dfrac{1-D_f}{4}\right]$.

Proof. See [6]. □

From the above theorem if one wants to find the pairs satisfying (4.1.1) one has to check whether or not the following equation

$$p^2 = 4x^2 + 2xy + \frac{1-D_f}{4}y^2$$

has an integral solution. Since $4p^2 = (4x+y)^2 - D_f y^2$, it follows that

$$0 \le -D_f \le 4p^2 - 1. \tag{4.1.4}$$

Therefore the number of such pairs is finite for any prime p.

Theorem 4.1.2. *Let* $\lambda(D)$ *be the number of odd prime divisors of* D *for* $D \equiv 5 \pmod 8$. *For any prime* p *such that* $\left(\frac{D}{p}\right) = 1$, *the number of pairs* (f,g) *such that* $Q(f) \cap p\mathbb{Z} = Q(g) \cap p\mathbb{Z}$ *and* $D_f = D$, $D_g = 4D$ *is* 0 *or* $2^{\lambda(D)-1}$ *up to equivalence.*

Proof. Assume that such pair exists. Then p^2 is represented by $\left[4, 2, \frac{1-D}{4}\right]$. Since every ambiguous form with discriminant D is of the form $[a, b, a]$ for some $a, b \in \mathbb{Z}^+$, the number of such pairs (f, g) is $2^{\lambda(D)-1}$ up to equivalence by Theorem 3.2.14. □

In the subsequent sections, we will frequently use the following equivalences of binary forms:

(1) $[a, a, b] \sim [b, a-2b, b]$. If we let $M_1 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, then

$$\det M_1 = 1 \text{ and } M_1^t \begin{pmatrix} a & \frac{a}{2} \\ \frac{a}{2} & b \end{pmatrix} M_1 = \begin{pmatrix} b & \frac{a}{2}-b \\ \frac{a}{2}-b & b \end{pmatrix}.$$

(2) $[a, b, c] \sim [a, 2at+b, at^2+bt+c]$. If we let $M_2 = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, then

$$\det M_2 = 1 \text{ and } M_2^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M_2 = \begin{pmatrix} a & at+\frac{b}{2} \\ at+\frac{b}{2} & at^2+bt+c \end{pmatrix}.$$

(3) $[a, b, c] \sim [c, -b, a]$. If we let $M_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, then

$$\det M_3 = 1 \text{ and } M_3^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M_3 = \begin{pmatrix} c & -\frac{b}{2} \\ -\frac{b}{2} & a \end{pmatrix}.$$

4.2 The case when $p = 3$

In this section, we find all pairs (f, g) of reduced forms satisfying

(i) $Q(f) \cap 3\mathbb{Z} = Q(g) \cap 3\mathbb{Z}$;

(ii) $D_f \equiv 5 \pmod 8$, $4D_f = D_g$ and $\left(\frac{D_f}{3}\right) = 1$;

(iii) 3^2 is represented by $\left[4, 2, \frac{1-D_f}{4}\right]$.

By the condition (4.1.4) below Theorem 4.1.1, the discriminant of f has to satisfy $-35 \leq D_f \leq 0$. Furthermore since D_f satisfies the condition (ii), $D_f = -11$ or -35. Also 3^2 has to be represented by $\left[4, 2, \frac{1-D_f}{4}\right]$, so we confirm that there is an integer solution (x, y) such that $4 \cdot 3^2 = (4x+y)^2 - D_f y^2$ for each D_f.

(1) $\underline{D_f = -11.}$

Since $(1, 1)$ is an integer solution of the equation $36 = (4x + y)^2 + 11y^2$, $p^2(= 9)$ is represented by $[4, 2, 3]$. Note that $[1, 1, 3]$ is the unique reduced form with discriminant -11. By Theorem 4.1.1, We have $f = [1, 1, 3] \sim [3, -5, 3]$ and $g = [12, -10, 3] \sim [3, 10, 12] \sim [3, -2, 4]$. Hence the pair of reduced forms satisfying the condition from (i) to (iii) given above for $p = 3$ is

$$(f, g) \simeq ([1, 1, 3], [3, -2, 4]).$$

(2) $\underline{D_f = -35.}$

Since $(0, 1)$ is an integer solution of the equation $36 = (4x + y)^2 + 35y^2$, $p^2(= 9)$ is represented by $[4, 2, 9]$. Note that there are exactly two reduced ambiguous froms with discriminant -35. By Theorem 4.1.1, We have $f = [1, 1, 9] \sim [9, -17, 9]$, $g = [36, -34, 9] \sim [9, 34, 36] \sim [9, -2, 4] \sim [4, 2, 9]$ and $f = [3, 1, 3]$, $g = [12, 2, 3] \sim [3, -2, 12]$. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 3$ are

$$(f, g) \simeq ([1, 1, 9], [4, 2, 9]) \text{ or } ([3, 1, 3], [3, -2, 12]).$$

The following table provides all reduced forms (f, g) for $p = 3$.

D_f	$(f,\ g)$
-11	$[1, 1, 3]$, $[3, -2, 4]$
-35	$[1, 1, 9]$, $[4, 2, 9]$
	$[3, 1, 3]$, $[3, -2, 12]$

Table 4.1 $p = 3$

4.3 The case when $p = 5$

In this section, we find all pairs (f, g) of reduced forms satisfying

(i) $Q(f) \cap 5\mathbb{Z} = Q(g) \cap 5\mathbb{Z}$;

(ii) $D_f \equiv 5 \pmod 8$, $4D_f = D_g$ and $\left(\frac{D_f}{5}\right) = 1$;

(iii) 5^2 is represented by $\left[4, 2, \frac{1 - D_f}{4}\right]$.

By the condition (4.1.4) below Theorem 4.1.1, the discriminant of f has to satisfy $-99 \leq D_f \leq 0$. Furthermore since D_f satisfies the condition (ii), $D_f = -11, -19, -51, -59, -91, -99$. Also 5^2 has to be represented by $\left[4, 2, \frac{1-D_f}{4}\right]$, so we confirm that there is an integer solution (x, y) such that $4 \cdot 5^2 = (4x + y)^2 - D_f y^2$ for each D_f.

(1) $\underline{D_f = -11.}$

Since $(-1, 3)$ is an integer solution of the equation $100 = (4x + y)^2 + 11y^2$, $p^2(= 25)$ is represented by $[4, 2, 3]$. Note that $[1, 1, 3]$ is the unique reduced form with discriminant -11. By Theorem 4.1.1, We have $f = [1, 1, 3] \sim [3, -5, 3]$ and $g = [12, -10, 3] \sim [3, 10, 12] \sim [3, -2, 4]$. Hence the pair of reduced forms satisfying the condition from (i) to (iii) given above for $p = 5$ is

$$(f, g) \simeq ([1, 1, 3], [3, -2, 4]).$$

(2) $\underline{D_f = -19.}$

Since $(2, 1)$ is an integer solution of the equation $100 = (4x + y)^2 + 19y^2$, $p^2(= 25)$ is represented by $[4, 2, 5]$. Note that $[1, 1, 5]$ is the unique reduced form with discriminant -19. By Theorem 4.1.1, We have $f = [1, 1, 5] \sim [5, -9, 5]$ and $g = [20, -18, 5] \sim [5, 18, 20] \sim [5, -2, 4] \sim [4, 2, 5]$. Hence the pair of reduced forms satisfying the condition from (i) to (iii) given above for $p = 5$ is

$$(f, g) \simeq ([1, 1, 5], [4, 2, 5]).$$

(3) $\underline{D_f = -51.}$

Since $(-2, 1)$ is an integer solution of the equation $100 = (4x+y)^2+51y^2$, $p^2(= 25)$ is represented by $[4, 2, 13]$. Note that there are exactly two reduced ambiguous froms with discriminant -51. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 5$ are

$$(f, g) \simeq ([1, 1, 13], [4, 2, 13]) \text{ or } ([3, 3, 5], [5, 4, 11]).$$

(4) $\underline{D_f = -91.}$

Since $(-1, 1)$ is an integer solution of the equation $100 = (4x+y)^2+91y^2$, $p^2(= 25)$ is represented by $[4, 2, 23]$. Note that there are exactly two reduced ambiguous froms with discriminant -91. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 5$ are

$$(f, g) \simeq ([1, 1, 23], [4, 2, 23]) \text{ or } ([5, 3, 5], [5, 4, 19]).$$

(5) $\underline{D_f = -99.}$

Since $(0, 1)$ is an integer solution of the equation $100 = (4x + y)^2 + 99y^2$, $p^2(= 25)$ is represented by $[4, 2, 25]$. Note that there are exactly two reduced ambiguous froms with discriminant -99. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 5$ are

$$(f, g) \simeq ([1, 1, 25], [4, 2, 25]) \text{ or } ([5, 1, 5], [5, -2, 20]).$$

The following table provides all reduced forms (f, g) for $p = 5$.

D_f	$(f,\ g)$	D_f	$(f,\ g)$
-11	$[1, 1, 3]$, $[3, -2, 4]$	-91	$[1, 1, 23]$, $[4, 2, 23]$
-19	$[1, 1, 5]$, $[4, 2, 5]$		$[5, 3, 5]$, $[5, 4, 19]$
-51	$[1, 1, 13]$, $[4, 2, 13]$	-99	$[1, 1, 25]$, $[4, 2, 25]$
	$[3, 3, 5]$, $[5, 4, 11]$		$[5, 1, 5]$, $[5, -2, 20]$

Table 4.2 $p = 5$

4.4 The case when $p = 7$

In this section, we find all pairs (f, g) of reduced forms satisfying

(i) $Q(f) \cap 7\mathbb{Z} = Q(g) \cap 7\mathbb{Z}$;

(ii) $D_f \equiv 5 \pmod 8$, $4D_f = D_g$ and $\left(\frac{D_f}{7}\right) = 1$;

(iii) 7^2 is represented by $\left[4, 2, \frac{1 - D_f}{4}\right]$.

By the condition (4.1.4) below Theorem 4.1.1, the discriminant of f has to satisfy $-195 \leq D_f \leq 0$. Furthermore since D_f satisfies the condition (ii), $D_f = -19, -27, -59, -75, -83, -115, -131, -139, -171,$
$-187, -195$. Also 7^2 has to be represented by $\left[4, 2, \frac{1-D_f}{4}\right]$, so we confirm that there is an integer solution (x, y) such that $4 \cdot 7^2 = (4x + y)^2 - D_f y^2$ for each D_f.

(1) $\underline{D_f = -19.}$

Since $(-2, 3)$ is an integer solution of the equation $196 = (4x+y)^2+19y^2$, $p^2(= 49)$ is represented by $[4, 2, 5]$. Note that $[1, 1, 5]$ is the unique reduced form with discriminant -19. By Theorem 4.1.1, We have $f = [1, 1, 5] \sim [5, -9, 5]$ and $g = [20, -18, 5] \sim [5, 18, 20] \sim [5, -2, 4] \sim [4, 2, 5]$. Hence the pair of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ is

$$(f, g)] \simeq ([1, 1, 5], [4, 2, 5]).$$

(2) $\underline{D_f = -27.}$

Since $(3, 1)$ is an integer solution of the equation $196 = (4x + y)^2 + 27y^2$, $p^2(= 49)$ is represented by $[4, 2, 7]$. Note that $[1, 1, 7]$ is the unique reduced form with discriminant -27. By Theorem 4.1.1, We have $f = [1, 1, 7] \sim [7, -13, 7]$ and $g = [28, -26, 7] \sim [7, 26, 28] \sim [7, -2, 4] \sim [4, 2, 7]$. Hence the pair of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ is

$$(f, g) \simeq ([1, 1, 7], [4, 2, 7]).$$

(3) $\underline{D_f = -75.}$

Since $(3, -1)$ is an integer solution of the equation $196 = (4x+y)^2+75y^2$, $p^2(= 49)$ is represented by $[4, 2, 19]$. Note that there are exactly two reduced ambiguous froms with discriminant -75. By Theorem 4.1.1, We have $f = [1, 1, 19] \sim [19, -37, 19]$, $g = [76, -74, 19] \sim [19, 74, 76] \sim [19, -2, 4] \sim [4, 2, 19]$ and $f = [3, 3, 7] \sim [7, -11, 7]$, $g = [28, -22, 7] \sim [7, 22, 28] \sim [7, -6, 12]$. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ are

$$(f, g) \simeq ([1, 1, 19], [4, 2, 19]) \text{ or } ([3, 3, 7], [7, -6, 12]).$$

(4) $\underline{D_f = -115.}$

Since $(2, 1)$ is an integer solution of the equation $196 = (4x+y)^2+115y^2$, $p^2(= 49)$ is represented by $[4, 2, 30]$. Note that there are exactly two reduced ambiguous froms with discriminant -115. By Theorem 4.1.1, We have $f = [1, 1, 29] \sim [29, -57, 29]$, $g = [116, -114, 29] \sim [29, 114, 116] \sim [29, -2, 4] \sim [4, 2, 29]$ and $f = [5, 5, 7] \sim [7, -9, 7]$, $g = [28, -18, 7] \sim [7, 18, 28] \sim [7, 4, 17]$. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ are

$$(f, g) \simeq ([1, 1, 29], [4, 2, 29]) \text{ or } ([5, 5, 7], [7, 4, 17]).$$

(5) $\underline{D_f = -171.}$

Since $(1, 1)$ is an integer solution of the equation $196 = (4x+y)^2+171y^2$, $p^2(= 49)$ is represented by $[4, 2, 43]$. Note that there are exactly two reduced ambiguous froms with discriminant -171. By Theorem 4.1.1, We have $f = [1, 1, 43] \sim [43, -85, 43]$, $g = [172, -170, 43] \sim [43, 170, 172] \sim [43, -2, 4] \sim [4, 2, 43]$ and $f = [7, 5, 7]$, $g = [28, 10, 7] \sim [7, -10, 28] \sim [7, 4, 25]$. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ are

$$(f, g) \simeq ([1, 1, 43], [4, 2, 43]) \text{ or } ([7, 5, 7], [7, 4, 25]).$$

(6) $\underline{D_f = -187.}$

Since $(1, -1)$ is an integer solution of the equation $196 = (4x+y)^2+187y^2$, $p^2(= 49)$ is represented by $[4, 2, 47]$. Note that there are exactly two reduced ambiguous froms with discriminant -187. By Theorem 4.1.1, We

have $f = [1, 1, 47] \sim [47, -93, 47]$, $g = [188, -186, 47] \sim [47, 186, 188] \sim [47, -2, 4] \sim [4, 2, 47]$ and $f = [7, 3, 7]$, $g = [28, 6, 7] \sim [7, -6, 28]$. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ are

$$(f, g) \simeq ([1, 1, 47], [4, 2, 47]) \text{ or } ([7, 3, 7], [7, -6, 28]).$$

(7) $\underline{D_f = -195.}$

Since $(0, 1)$ is an integer solution of the equation $196 = (4x+y)^2+195y^2$, $p^2(= 49)$ is represented by $[4, 2, 49]$. Note that there are exactly four reduced ambiguous froms with discriminant -195. By Theorem 4.1.1, We have $f = [1, 1, 49] \sim [49, -97, 49]$, $g = [196, -194, 49] \sim [49, 194, 196] \sim [49, -2, 4] \sim [4, 2, 49]$ and $f = [7, 1, 7]$, $g = [28, 2, 7] \sim [7, -2, 28]$. We also have $f = [3, 3, 17] \sim [17, -31, 17]$, $g = [68, -62, 17] \sim [17, 62, 68] \sim [17, -6, 12] \sim [12, 6, 17]$ and $f = [5, 5, 11] \sim [11, -17, 11]$, $g = [44, -34, 11] \sim [11, 34, 44] \sim [11, -10, 20]$. Hence all pairs of reduced forms satisfying the condition from (i) to (iii) given above for $p = 7$ are

$$(f, g) \simeq ([1, 1, 49], [4, 2, 49]) \text{ or } ([7, 1, 7], [7, -2, 28]) \text{ or}$$

$$\simeq ([3, 3, 17], [12, 6, 17]) \text{ or } ([5, 5, 11], [11, -10, 20]).$$

Note that there is no integer solution (x, y) such that $196 = (4x + y)^2 - D_f y^2$ for $D_f = -59, -83, -131, -139$.

The following table provides all reduced forms (f, g) for $p = 7$.

D_f	$(f,\ g)$	D_f	$(f,\ g)$
-19	$[1, 1, 5]$, $[4, 2, 5]$	-171	$[7, 5, 7]$, $[7, 4, 25]$
-27	$[1, 1, 7]$, $[4, 2, 7]$	-187	$[1, 1, 47]$, $[4, 2, 47]$
-75	$[1, 1, 19]$, $[4, 2, 19]$		$[7, 3, 7]$, $[7, -6, 28]$
	$[3, 3, 7]$, $[7, -6, 12]$	-195	$[1, 1, 49]$, $[4, 2, 49]$
-115	$[1, 1, 29]$, $[4, 2, 29]$		$[7, 1, 7]$, $[7, -2, 28]$
	$[5, 5, 7]$, $[7, 4, 17]$		$[3, 3, 17]$, $[12, 6, 17]$
-171	$[1, 1, 43]$, $[4, 2, 43]$		$[5, 5, 11]$, $[11, -10, 20]$

Table 4.3 $p = 7$

4.5 The case when $p = 11$ or $p = 13$

Similarly we can find all pairs (f, g) of reduced forms satisfy the conditions given above for $p = 11$ or 13. Therefore we just arrange the pairs (f, g) as table for each p in order to avoid repeated process.

The following table provides all pairs (f, g) of reduced forms satisfying (4.1.1) for $p = 11$.

D_f	$(f,\ g)$	D_f	$(f,\ g)$
-35	$[1,1,9]$, $[4,2,9]$	-403	$[1,1,101]$, $[4,2,101]$
	$[3,1,3]$, $[3,-2,12]$		$[11,9,11]$, $[11,4,37]$
-43	$[1,1,11]$, $[4,2,11]$	-435	$[1,1,109]$, $[4,2,109]$
-51	$[1,1,13]$, $[4,2,13]$		$[3,3,37]$, $[12,6,37]$
	$[3,3,5]$, $[5,4,11]$		$[5,5,23]$, $[20,10,23]$
-123	$[1,1,31]$, $[4,2,31]$		$[11,7,11]$, $[11,8,41]$
	$[3,3,11]$, $[11,-6,12]$	-459	$[1,1,115]$, $[4,2,115]$
-195	$[1,1,49]$, $[4,2,49]$		$[11,5,11]$, $[11,-10,44]$
	$[7,1,7]$, $[7,-2,28]$	-475	$[1,1,119]$, $[4,2,119]$
	$[3,3,17]$, $[12,6,17]$		$[11,3,11]$, $[11,-6,44]$
	$[5,5,11]$, $[11,-10,20]$	-483	$[1,1,121]$, $[4,2,121]$
-259	$[1,1,65]$, $[4,2,65]$		$[11,1,11]$, $[11,-2,44]$
	$[7,7,11]$, $[11,8,25]$		$[3,3,41]$, $[12,6,41]$
-315	$[1,1,79]$, $[4,2,79]$		$[7,7,19]$, $[19,-14,28]$
	$[5,5,17]$, $[17,-10,20]$		
	$[7,7,13]$, $[13,12,27]$		
	$[9,9,11]$, $[11,4,29]$		

Table 4.4 $p = 11$

The following table provides all pairs (f, g) of reduced forms satisfying (4.1.1) for $p = 13$.

D_f	$(f,\ g)$	D_f	$(f,\ g)$
-27	$[1,1,7]$, $[4,2,7]$	-555	$[1,1,139]$, $[4,2,139]$
-35	$[1,1,9]$, $[4,2,9]$		$[3,3,47]$, $[12,6,47]$
	$[3,1,3]$, $[3,-2,12]$		$[5,5,29]$, $[20,10,29]$
-43	$[1,1,11]$, $[4,2,11]$		$[13,11,13]$, $[13,4,43]$
-51	$[1,1,13]$, $[4,2,13]$	-595	$[1,1,149]$, $[4,2,149]$
	$[3,3,5]$, $[5,4,11]$		$[5,5,31]$, $[20,10,31]$
-75	$[1,1,19]$, $[4,2,19]$		$[7,7,23]$, $[23,-14,28]$
	$[3,3,7]$, $[7,-6,12]$		$[13,9,13]$, $[13,8,47]$
-147	$[1,1,37]$, $[4,2,37]$	-627	$[1,1,157]$, $[4,2,157]$
	$[3,3,13]$, $[12,6,13]$		$[3,3,53]$, $[12,6,53]$
-235	$[1,1,59]$, $[4,2,59]$		$[13,7,13]$, $[13,12,51]$
	$[5,5,13]$, $[13,-10,20]$		$[11,11,17]$, $[17,12,39]$
-315	$[1,1,79]$, $[4,2,79]$	-651	$[1,1,163]$, $[4,2,163]$
	$[5,5,17]$, $[17,-10,20]$		$[3,3,55]$, $[12,6,55]$
	$[7,7,13]$, $[13,12,27]$		$[13,5,13]$, $[13,-10,52]$
	$[9,9,11]$, $[11,4,29]$		$[7,7,25]$, $[25,-14,28]$
-387	$[1,1,97]$, $[4,2,97]$	-667	$[1,1,167]$, $[4,2,167]$
	$[9,9,13]$, $[13,8,31]$		$[13,3,13]$, $[13,-6,52]$
-451	$[1,1,113]$, $[4,2,113]$	-675	$[1,1,169]$, $[4,2,169]$
	$[11,11,13]$, $[13,4,35]$		$[13,1,13]$, $[13,-2,52]$

Table 4.5 $p = 13$

Bibliography

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

[2] J. W. S. Cassels, *Rational quadratic forms*, Academic Press, 1987.

[3] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Wiley, 1997.

[4] B. N. Delone, *Geometry of positive quadratic forms addendum*, Uspehi Mat. Nauk **4**(1938).

[5] Delang Li, *Indefinite binary forms representing the same number*, Math. Proc. Camb. Phil. Soc. **92**(1982), 29-33.

[6] B. K. Oh, *Positive binary forms representing the same arithmetic progressions*, Preprint.

[7] N. R. Lim, *Binary quadratic forms representing same multiples of a prime*, Master Thesis SNU(2014).

국문초록

양의 정부호 이변수 이차형식 $f(x,y)=ax^2+bxy+cy^2$에 의해 표현되는 정수의 집합을 $Q(f)$라 하자. 1938년 Delone은 동형이 아닌 두 이차형식 f,g가 $Q(f)=Q(g)$을 만족할 필요충분조건이 $(f,g)\simeq(x^2+xy+y^2,x^2+3y^2)$임을 증명하였다. 최근에 Oh는 소수 p에 대하여, $Q(f)\cap p\mathbb{Z}=Q(g)\cap p\mathbb{Z}$을 만족하는 이차형식 f,g를 구하는 간단한 판정법을 제시하였다. 이 논문에서는 Oh의 판정법을 이용하여 13이하의 소수p에 대하여 $Q(f)\cap p\mathbb{Z}=Q(g)\cap p\mathbb{Z}$, $D_f\equiv 5 \pmod 8$, $4D_f=D_g$, $\left(\frac{D_f}{p}\right)=1$을 만족하는 (f,g)를 모두 구하였다.

주요어휘: 소수의 배수, 이변수 이차형식 표현
학번: 2007-20287