J. Chosun Natural Sci.
Vol. 14, No. 4 (2021) pp. 159 – 161
https://doi.org/10.13160/ricns.2021.14.4.159

Remarks of Primes of the Form

Kwang-Seob Kim†
Department of mathematics, Chosun University, Gwangju, Korea

Abstract

In this article, we will study which prime numbers are represented by the principal form. $p = x^2 + ny^2$. We will also give some results related to the form of primes of the form $x^2 + axy + y^2$.

Keywords: Primes of the form, Class number, Unramified extension

(Recceived November 26, 2021 Revised December 17, 2021 Accepted December 29, 2021)

1. Introduction

One of the important topic of algebraic number theory is to study primes p of the form $p = x^2 + ny^2$ for given integer n. The answers for the question was widely studied by various authors. In this paper, we will study the several prims represented by quadratic forms

2. Preliminary

We will review some basic facts from algebraic number theory, including Dedekind domain, factorization of ideals, and ramification. To begin, we define a number field K to be a subfield of the complex numbers C which has finite degree over Q. The degree of K over Q is denoted $[K : Q]$. Given such a field K, we let O_K denote the algebraic integers of K, i.e., the set of all $\alpha \in K$ which are roots of a monic integer polynomial. The basic structure of O_K is given in the following proposition.

Proposition 2.1. (See proposition 5.3 of [1])
Let K be a number field.
(i) O_K is a subring of C whose field of fraction is K.
(ii) O_K is a free Z-module of rank $[K : Q]$.

We will often call O_K the number ring of K. To begin our study of O_K, we note that part (ii) of Proposition 2.1 has the following useful consequence concering the ideals of O_K:

Corollary 2.2.
If K is a number field and a is a nonzero ideals of O_K, then the quotient ring O_K/a is finite.

Given an order O, let $I(O)$ denote the set of proper fractional O-ideals. Then $I(O)$ is a group under multiplication; the crucial issues are closure and the existence of inverses, both of which follow from the inevitability of proper ideals, The principal O-ideals give a subgroup $P(O) \subset I(O)$, and thus we can form the quotient

$$C(O) = I(O) / P(O)$$

which is the ideal class group of the order O. When O is the maximal order O_K, $I(O_K)$ and $P(O_K)$ will be denoted I_K and P_K, respectively. We can relate the ideal class group $C(O)$ to the form class group $C(D)$.

†Corresponding author : kwang12@chosun.ac.kr

Theorem 2.3. (Theorem 7.7 in [1])

Let O be the order of discriminant D in an imaginary quadratic field K.

(i) If $f(x, y) = ax^2 + bxy + cy^2$ is a primitive definite quadratic form of discriminant D, then $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ is a proper ideal of O.

(ii) The map sending $f(x, y)$ to $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ induces an isomorphism between the form class group $C(D)$ and the ideal class group $C(O)$. Hence the order of $C(O)$ is the class number $h(D)$.

(iii) A positive integer m is represented by a form $f(x, y)$ if and only if m is the norm $N(a)$ of some ideal a in the corresponding ideal class in $C(O)$.

Let L be the ring class field of $Z[\sqrt{-n}\,]$. We start by relating

Theorem 2.4. (See Theorem 9.4 in [1])

Let $n>0$ be an integer, and L be the ring class field of the order $Z[\sqrt{-n}\,]$ in the imaginary quadratic field $K = Q(\sqrt{-n}\,)$. If p is an odd prime not dividing n, then $p = x^2 + ny^2 \Leftrightarrow p$ splits completely in L.

3. Primes of the form $x^2 + axy + by^2$

Theorem 3.1.

Let n be a positive integer greater than k^2. A rational prime p is represented by a binary quadratic form $f(x, y) = x^2 + 2kxy + ny^2$ if and only if p is represented by $x^2 + (n - k^2)y^2$.

Proof)

Let $K = Q(\sqrt{k^2-n}\,)$, $O = Z[\sqrt{k^2-n}\,]$. The discriminant of quadratic form f and order O is both $4(k^2 - n)$. Let L be ring class field of O, $a_0 = \left(1, \frac{-2k+\sqrt{4(k^2-n)}}{2}\right)$ $= (1, \sqrt{k^2-n}\,) = O$ and σ_0 be a corresponding element of a_0 in $Gal(L/K)$. We can regard σ_0 as an element in $Gal(L/Q)$, and suppose $<\sigma_0>$ be a conjugacy class of σ_0 in $Gal(L/Q)$. By Theorem 2.3, a rational prime p is represented by f if and only if p satisfies following two conditions.

1) p is unramified in L.

2) $\left(\frac{L/Q}{p}\right) = <\sigma_0>$

Since $a_0 = 0$, the ideal class containing a_0 is the identity element of $C(O)$ and hence σ_0 is identity. Also $\left(\frac{L/Q}{p}\right) = 1$ if and only if p splits completely in L. Thus a rational prime p is represented by f if and only if p splits completely in L. By Theorem 2.4, f representing p is equivalent to $x^2 + (n - k^2)y^2$ representing p.

Theorem 3.2.

Let n be a positive integer greater than $\frac{(2k+1)^2}{4}$. A rational prime p is represented by a binary quadratic form $g(x, y) = x^2 + (2k + 1)xy + ny^2$ if and only if p is represented by $x^2 + (4n - (2k + 1)^2)y^2$.

Proof)

Let $K = Q(\sqrt{(2k+1)^2-4n}\,)$, $O = Z\left[\frac{-1+\sqrt{(2k+1)^2-4n}}{2}\right]$.

The discriminant of quadratic form g and order O is both $(2k + 1)^2 - 4n$. Let L be the ring class field of O, $a_0 = \left(1, \frac{-(2k+1)+\sqrt{(2k+1)^2-4n}}{2}\right) = (1, \sqrt{(2k+1)^2-4n})$ $= O$ and σ_0 be a corresponding element of a_0 in $Gal(L/K)$. We can regard σ_0 as an element in $Gal(L/Q)$, and suppose $<\sigma_0>$ be a conjugacy class of σ_0 in $Gal(L/Q)$. Since p is represented by g if and only if p is unramified in L and $\left(\frac{L/Q}{p}\right) = <\sigma_0>$, a rational prime p is represented by g if and only if p splits completely in L. By Theorem 2.4, f representing p is equivalent to $x^2 + (4n - (2k + 1)^2)y^2$ representing p.

4. Primes of the form $ax^2 + by^2$

Theorem 4.1.

Let k be a positive integer, n be a positive integer coprime with a such that class number of $Q(\sqrt{-an}\,)$ is odd. A rational prime p is represented by a binary quadratic form $f(x, y) = ax^2 + ny^2$ if and only if p is represented by $x^2 + (an)y^2$.

Proof)

Let $K = Q(\sqrt{-an})$, $O = Z[\sqrt{-an}]$. The discriminant of quadratic form f and order O is both $-4an$. Let L be ring class field of O, $a_0 = \left(a, \frac{-\sqrt{-4an}}{2}\right) = (a, \sqrt{-an}) = O$.

$$a_0^2 = (a^2, a\sqrt{-an}, a\sqrt{-an}, -an) = (a, a\sqrt{-an}) = (a)$$

hence $[a_0]^2 = 1$. Since we suppose $h(K) \equiv 1 \pmod 2$, the order of $C(O)$ is odd and the order of $[a_0]$ is 1. Since $[a_0] = 1$, the corresponding element σ_0 in Gal(L/K) is 1. By Theorem 2.3, a rational prime p is represented by f if and only if p is unramified in L and $\left(\frac{L/Q}{p}\right) = < \sigma_0 \geq 1$. This is equivalent to p completely splitting in L. By Theorem 2.4, f representing p is equivalent to $x^2 + any^2$ representing p.

5. Primes of the form $ax^2 + 2xy + by^2$

Theorem 4.1.

Let q be a odd positive integer, n be a positive integer satisfying $n = \frac{2(kq-1)}{q-1}$ for some k. A rational prime p is represented by a binary quadratic form $f(x, y) = qx^2 + 2xy + ny^2$ if and only if p is represented by $x^2 + (qn - 1)y^2$.

Proof)

Let $K = Q[\sqrt{1-qn}]$, θ be a solution of $qx^2 + 2x + n = 0$ and $O = Z[\sqrt{1-qn}]$. The discriminant of quadratic form f and order O is both $4(1-qn)$. Let L be ring class field of O, $[a_0] = \left(q, \frac{-2+\sqrt{4-4qn}}{2}\right) = (q, q\theta)$.

$$a_0^2 = (q, q\theta)^2 = (q^2, q^2\theta, q^2\theta, q^2\theta^2)$$
$$= (q^2, q^2\theta, -2q\theta - qn)$$
$$= (q^2, -q + q\sqrt{1-qn}, 2 - qn - 2\sqrt{1-qn})$$

a_0^2 is consisted of all number of the form $t + s\sqrt{1-qn}$ which satisfies $t = q^2x - qy + (2-qn)z$, $s\sqrt{1-qn} = (qy - 2z)\sqrt{1-qn}$ for $x, y, z \in Z$. Since q is odd, every integer solution for $qy - 2z = s$ is

$$y = s + 2k, z = s\frac{q-1}{2} + qk, k \in Z$$

by bezout identity. If we substitute this result to real part,

$$t = q^2x - s - qns\frac{q-1}{2} - q^2nk, x, k \in Z$$

It can be all elements of $q^2Z - \left(\frac{nq(q-1)}{2} + 1\right)s$. Hence

$$a_0^2 = \left(q^2, -\left(\frac{nq(q-1)}{2} + 1\right) + \sqrt{1-qn}\right) = \left(q^2, -\frac{nq(q-1)}{2}q\theta\right).$$

Since $n = \frac{2(kq-1)}{q-1}$ for some k,

$$a_0^2 = q^2, \frac{nq(q-1)}{2}q\theta = (q^2, -(kq^2 - q) + q\theta)$$
$$= (q^2, q + q\theta) = (q^2, \sqrt{1-qn})$$

But $a_0^6 = (q^2, \sqrt{1-qn})$. Hence $[a_0] = 1$ and the corresponding element σ_0 in Gal(L/K) is 1. By Theorem 2.3, a rational prime p is represented by f if and only if p is unramified in L and $\left(\frac{L/Q}{p}\right) = < \sigma_0 \geq 1$. This is equivalent to p completely splitting in L. By Theorem 2.4, f representing p is equivalent to $x^2 + (qn - 1)y^2$ representing p.

Acknowledgments

This study was supported by research funds from Chosun University, 2021.

Reference

[1] Cox, David A. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication(1989) JOHN WILEY & SONS, INC.