教育학석사학위請求論文

$x^2 + ny^2$ 형태의 소수들에 관하여

<Primes of the form $x^2 + ny^2$>

2002年 2月

仁何大學校 教育大學院

數學教育專攻

金 幸 石
教育학석사학위請求論文

\[ x^2 + ny^2 \] 형태의 소수들에 관하여

<Primes of the form \( x^2 + ny^2 \)>

2002年 2月

指導教授 金載文

이論文을碩士學位論文으로提出함.
本論文은 김정호의碩士學位論文으로
認定함.

2002年2月日

主審

副審

副審
Abstract

In this paper, we study primes of the form $x^2 + ny^2$ for $n = 1, 2, 3, 5$ and 7. The cases when $n = 1, 2$ and 3 can be taken care of by using the quadratic reciprocity law. For the remaining two cases, we first review basic theory of quadratic forms. Then as an application, we investigate the cases $n = 5$ and 7.
국문要約

이 논문은 $\nu = 1, 2, 3, 5, 7$ 일 때 $x^2 + \nu y^2$ 형태의 소수들을 연구하는데 목적이 있다.

$\nu = 1, 2, 3$ 인 경우에는 이차형여상호법칙을 사용하여 비교적 쉽게 해결할 수 있다. 나머지 두 가지 경우는 이차형태에 관한 이론을 이용한다. 이 논문의 3절에서는 이차형태의 기본적인 이론을 소개하고 마지막 4절에서 $\nu = 5, 7$ 인 경우에 대한 답을 제시한다.
CONTENTS

I. Introduction

II. Quadratic reciprocity law and primes of the form $x^2 + ny^2$ for $n = 1, 2$ and $3$

III. Quadratic form

IV. Primes of the form $x^2 + ny^2$ for $n = 5$ and $7$

Abstract

Korean Abstract

References
§ 1. Introduction

The basic question we are concerned about in this paper is the following: Given a positive integer \( n \), which primes \( p \) can be expressed in the form \( p = x^2 + ny^2 \), where \( x \) and \( y \) are integers? The history of this problem goes back to Fermat, who examined the cases when \( n = 1, 2 \) and \( 3 \). Fermat's assertion on these cases says, without proofs, that

\[
\begin{align*}
p &= x^2 + y^2, \quad x, y \in \mathbb{Z} \quad \iff \quad p \equiv 1 \mod 4, \\
p &= x^2 + 2y^2, \quad x, y \in \mathbb{Z} \quad \iff \quad p \equiv 1 \text{ or } 3 \mod 8, \\
p &= x^2 + 3y^2, \quad x, y \in \mathbb{Z} \quad \iff \quad p = 3 \text{ or } p \equiv 1 \mod 3.
\end{align*}
\]

Later in 18th century, Euler studied these problems again and found a proof by using the quadratic reciprocity law. Of course, he did not know the quadratic reciprocity law in full generality which was discovered after Legendre. However, he had enough information on the reciprocity law to take care of the cases \( n = 1, 2 \) and \( 3 \). Moreover his method generalized to the case when \( n > 3 \) and gave partial, but important results. And he made several conjectures:

\[
\begin{align*}
p &= x^2 + 5y^2 \iff p \equiv 1, 9 \mod 20, \\
p &= \begin{cases} 
  x^2 + 14y^2 
  & \iff p \equiv 1, 9, 15, 23, 25, 39 \mod 56, \\
  2x^2 + 7y^2 
  & \end{cases} \\
p &= x^2 + 2(3y)^2 \iff p \equiv 1 \mod 3 \text{ and } 2 \text{ is a cubic residue modulo } p.
\end{align*}
\]
Proofs for \( n = 5 \) and 14 on Euler's conjecture were available only after Lagrange introduced the theory of positive definite quadratic forms. A proof for \( n = 27 \) came out even later. It had been unsettled until Gauss found cubic reciprocity law. A complete answer to this problem for general \( n \) was only possible in the 20th century when class field theory and elliptic curve theory were developed.

This paper is a survey article on this subject. In this paper, we will study primes of the form \( p = x^2 + n_{32}^2 \) for a first few \( n \)'s. Section 2 takes care of the cases when \( n = 1, 2 \) and 3. We will follow Euler's method, but use modern languages such as Legendre symbol and the quadratic reciprocity law which were unavailable in his era. In section 3, we introduce basic concepts from the theory of quadratic forms briefly. And in section 4, by using the theory of quadratic forms, we determine primes of the form \( p = x^2 + n_{32}^2 \) for \( n = 5 \) and \( n = 7 \).
§ 2. Quadratic reciprocity law and primes of the form \( x^2 + n3^2 \) when \( n = 1, 2 \) and \( 3 \)

**Definition 2.1.** Let \( p \) be an odd prime and \( a \) an integer such that \((a, p) = 1\). If \( x^2 \equiv a \mod p \) has a solution, then \( a \) is called a quadratic residue of \( p \). Otherwise \( a \) is called a quadratic nonresidue of \( p \).

**Definition 2.2.** For an odd prime \( p \) and an integer \( a \) relatively prime to \( p \), the Legendre symbol \((\frac{a}{p})\) is defined as follows:

\[
(\frac{a}{p}) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue of } p \\
-1 & \text{if } a \text{ is a quadratic nonresidue of } p.
\end{cases}
\]

**Proposition 2.3.** Legendre symbol satisfies the following properties:

(i) \((\frac{a^2}{p}) = 1\)

(ii) If \( a \equiv b \mod p \), then \((\frac{a}{p}) = (\frac{b}{p})\)

(iii) \((\frac{a}{p}) = a^{\frac{p-1}{2}} \mod p\)

(iv) \((\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})\)

(v) \((\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4 \\
-1 & \text{if } p \equiv 3 \mod 4
\end{cases}\)

(vi) \((\frac{2}{p}) = (-1)^{\frac{p-1}{8}}\).

- 4 -
Theorem 2.4. (Quadratic Reciprocity Law) If $p$ and $q$ are distinct odd primes, then

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/2}.$$  

(Proof) See [2], Chapter IV.

Example 1. $x^2 = 3 \mod 13$ has a solution.

(Proof) By the quadratic reciprocity law,

$$(\frac{3}{13}) = (\frac{13}{3}) = (\frac{1}{3}) = 1.$$  

Thus $x^2 = 3 \mod 13$ has a solution.

Example 2. $x^2 = 21064 \mod 1999$ does not have a solution.

(Proof) Since $21064 \equiv 1094 \mod 1999$, $1094 = 2 \cdot 547$ and $1999 = -1 \mod 8$, we have 

$$(\frac{21064}{1999}) = (\frac{1094}{1999}) = (\frac{2}{1999})(\frac{547}{1999}) = (\frac{547}{1999}).$$

By using the quadratic reciprocity law and the properties in Proposition 2.3, we have 

$$(\frac{547}{1999}) = -(\frac{1999}{547}) = -(\frac{58}{547}) = -\left(\frac{2}{547}\right)(\frac{29}{547}) = (\frac{547}{179}) = (\frac{10}{179}) = (\frac{10 \cdot 5}{179}) = (\frac{5^2}{179}) = -1.$$  

Therefore the congruence does not have a solution.
Example 3. Quadratic reciprocity law can also be used to prove the following kinds of statements:

\[
\left( \frac{3}{p} \right) = 1 \iff p \equiv \pm 1 \mod 12.
\]

\[
\left( \frac{5}{p} \right) = 1 \iff p \equiv \pm 1, \pm 9 \mod 20.
\]

\[
\left( \frac{7}{p} \right) = 1 \iff p \equiv \pm 1, \pm 9, \pm 25 \mod 28.
\]

(Proof) We will prove the first one. The remaining two can be handled similarly. By the quadratic reciprocity law, we have \(\left( \frac{3}{p} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{p}{3} \right)\). Note that \(p \equiv 1 \mod 4\) if and only if \((-1)^{\frac{p-1}{2}} = 1\), and that \(p \equiv 1 \mod 3\) if and only if \(\left( \frac{p}{3} \right) = 1\). Therefore \((-1)^{\frac{p-1}{2}} \left( \frac{p}{3} \right) = 1\) if and only if \(p \equiv 1 \mod 12\). Thus \(\left( \frac{3}{p} \right) = 1\) if and only if \(p \equiv \pm 1 \mod 12\).

Remark 2.5. From Example 3, one can see a pattern: if \(p\) and \(q\) are distinct odd primes, then \(\left( \frac{q}{p} \right) = 1\) if and only if \(p \equiv \pm q^2 \mod 4q\) for some odd integer \(\beta\). We will prove that this is indeed the case.

(Proof) We will prove only if part only. The converse can be justified similarly. We examine two cases separately:

(i) \(p \equiv 1 \mod 4\) or \(q \equiv 1 \mod 4\)

(ii) \(p \equiv 3 \mod 4\) and \(q \equiv 3 \mod 4\).
(i) $p \equiv 1$ or $q \equiv 1 \mod 4$

By the quadratic reciprocity law, $(\frac{q}{p}) = 1$ implies that $(\frac{p}{q}) = 1$. Thus $p \equiv a^2 \mod q$. If $a$ is odd, then we have $p \equiv a^2 \mod 4q$. If $a$ is even, then $a + q$ is odd and $p \equiv (a + q)^2 \mod 4q$.

(ii) $p \equiv 3$ and $q \equiv 3 \mod 4$

By the quadratic reciprocity law, if $(\frac{q}{p}) = 1$, then $(\frac{p}{q}) = -1$. Since $(\frac{-1}{q}) = -1$, we have $(\frac{-p}{q}) = 1$. Therefore $-p \equiv b^2 \mod q$, from which we can conclude $p \equiv -b^2 \mod 4q$ as in case (i).

Now we use Legendre symbol and quadratic reciprocity law to study primes of the form $x^2 + ny^2$. We begin with a lemma.

**Lemma 2.6.** Let $n$ be a nonzero integer, and $p$ an odd prime not dividing $n$. Then $p \mid x^2 + ny^2$ for some integers $x$ and $y$ such that $\gcd(x, y) = 1$ if and only if $(\frac{-n}{p}) = 1$.

(Proof) The lemma is immediate from the definition of the Legendre symbol $(\frac{-n}{p})$. 
**Theorem 2.7.** We have the following theorems:

\[ p = x^2 + y^2 \quad \iff \quad p \equiv 1 \pmod{4} \]
\[ p = x^2 + 2y^2 \quad \iff \quad p \equiv 1, 3 \pmod{8} \]
\[ p = x^2 + 3y^2 \quad \iff \quad p \equiv 1, 7 \pmod{12} \text{ or } p = 3 \]

To prove above theorems, we need a lemma.

**Lemma 2.8.** Suppose that an integer \( N \) is of the form \( N = x^2 + ny^2 \) for some relatively prime integers \( a \) and \( b \). If \( q = x^2 + ny^2 \) is a prime divisor of \( N \), then \( \frac{N}{q} \) is also of the form \( \frac{N}{q} = c^2 + nd^2 \) with \( (c, d) = 1 \).

(Proof) Note that \( q \) divides

\[ x^2N - a^2q = x^2(a^2 + nb^2) - a^2(x^2 + ny^2) \]
\[ = n(xb - ac)(xb + ac) \]

Since \( q \) is a prime, it divides either \( xb - ac \) or \( xb + ac \).

By changing the sign of \( a \) if necessary, we may assume that \( q \mid xb - ac \), thus \( xb - ac = dq \) for some integer \( d \).

Note that \( x \mid (a + ndb)y \), since

\[ (a + ndb)y = ac + ndb^2 \]
\[ = xb - dq + ndb^2 \]
\[ = xb - db^2. \]

Since \( (x, y) = 1 \), we have \( x \mid a + ndb \). Set \( a + ndb = cx \).

Then the equation \( (a + ndb)y = x(b - dx) \) implies that \( b = dx + cy \). So we have \( a = cx - ndy \) and \( b = dx + cy \).
Then
\[ N = a^2 + nb^2 \]
\[ = (cx - ndy)^2 + n(dx + cy)^2 \]
\[ = c^2x^2 - 2ncdxy + n^2d^2y^2 + nd^2x^2 + 2nacdy + nc^2y^2 \]
\[ = c^2(x^2 + ndy^2) + nd^2(x^2 + ndy^2) \]
\[ = (x^2 + ndy^2)(c^2 + nd^2) \]
\[ = q(c^2 + nd^2) . \]

Therefore \( \frac{N}{q} = c^2 + nd^2 \) as desired and \( c \) and \( d \) must be relatively prime since \( a \) and \( b \) are so. This proves the lemma.

(Proof of Theorem 2.7) We will show the theorem when \( n = 2 \) only. A similar argument works for \( n = 1 \) and 3.
Suppose that \( p = x^2 + 2y^2 \) for some integers \( x \) and \( y \). Then
\( \left( \frac{-2}{p} \right) = 1 \) by Lemma 2.6. Therefore \( p = 1 \) or 3 mod 8.

Conversely, suppose that \( p = 1 \) or 3 mod 8. Then
\( \left( \frac{-2}{p} \right) = 1 \) and so \( p \mid a^2 + 2b^2 \) for some \( a \) and \( b \) with \( (a, b) = 1 \). We claim that \( p \mid a^2 + 2b^2 \) implies that \( p = c^2 + 2d^2 \). Put \( N = a^2 + 2b^2 \), with \( (a, b) = 1 \). By subtracting suitable multiples of \( p \) from \( a \) and \( b \), we may assume \( a \) and \( b \) satisfy \( |a| < \frac{p}{2} \) and \( |b| < \frac{p}{2} \). The new \( a, b \) may not be relatively prime. However \( (a, b) \) is not divisible by \( p \). Thus we may further assume that our new...
\(a, b\) are relatively prime. Note that \(N = a^2 + 2b^2 < \frac{5}{4} p^2\), which means that \(p\) is the largest prime divisor of \(N\). If \(p\) is not of the form \(x^2 + 2y^2\), then \(N\) has another prime divisor \(q\) with \(q < p\) which is not of this form by Lemma 2.8. This process can be repeated infinitely, which is impossible. Therefore \(p\) is of the form \(p = c^2 + 2d^2\).
§ 3. Quadratic form

Definition 3.1. An (integral) quadratic form in two variables $x$ and $y$ or simply a quadratic form is a polynomial $f(x, y)$ of the form $f(x, y) = ax^2 + bx y + cy^2$ with $a, b$ and $c \in \mathbb{Z}$. A quadratic form $ax^2 + bx y + cy^2$ is called primitive if the coefficients $a$, $b$ and $c$ are relatively prime. We say a quadratic form $f(x, y)$ represents $m$ if the equation $m = f(x, y)$ has an integer solution in $x$ and $y$, and say $f(x, y)$ represents $m$ properly if $m = f(x, y)$ has a solution with relatively prime integers.

Example 4. The primitive quadratic form $x^2 + 5y^2$ represents 29 properly since $29 = 3^2 + 5 \cdot 2^2$.

Definition 3.2. Two quadratic forms $f(x, y)$ and $g(x, y)$ are said to be equivalent if $f(x, y) = g(px + qy, rx + sy)$ for some integers $p, q, r$ and $s$ satisfying $ps - qr = \pm 1$. We say that an equivalence is a proper equivalence if $ps - qr = 1$, and improper equivalence if $ps - qr = -1$.

Lemma 3.3. (1) Equivalence (proper equivalence) of quadratic forms is an equivalence relation.

(2) Equivalent forms represent (properly) the same numbers.
(Proof) (1) Reflexiveness is obvious by taking $p = s = 1$ and $q = r = 0$. To prove symmetry suppose that $f(x, y) = g(px + qy, rx + sy)$ for some $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$ with $ps - qr = \pm 1$.

Let $\begin{pmatrix} p' & r' \\ q' & s' \end{pmatrix}$ be the inverse of $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$. Then $p's' - q'r' = \pm 1$ and $g(x, y) = f(p'x + q'y, r'x + s'y)$. Finally to show transitivity, suppose that $f(x, y) = g((x, y)A)$ and $g(x, y) = h((x, y)B)$, where $A = \begin{pmatrix} p_1 & r_1 \\ q_1 & s_1 \end{pmatrix}$ and $B = \begin{pmatrix} p_2 & r_2 \\ q_2 & s_2 \end{pmatrix}$ with $\det A$ and $\det B = \pm 1$. Then $f(x, y) = g((x, y)A) = h((x, y)AB)$ and $\det AB = \pm 1$.

(2) Let $f(x, y) = g((x, y)A)$, with $\det A = \pm 1$. If $f(s, t) = m$ then $g(s_1, t_1) = m$, where $(s_1, t_1) = (s, t)A$. Conversely, if $g(u, v) = m$, then $f(u', v') = m$, where $(u', v') = (u, v)A^{-1}$.

Lemma 3.4. A quadratic form $f(x, y)$ properly represents an integer $m$ if and only if $f(x, y)$ is properly equivalent to the form $mx^2 + bxy + cy^2$ for some $b, c \in Z$.

(Proof) Put $f(x, y) = ax^2 + bxy + cy^2$ and suppose that $f(p, q) = m$, where $p$ and $q$ are relatively prime. We can find integers $r$ and $s$ such that $ps - qr = 1$. Then $f(px + qy, rx + sy)$
\[ f(x, y) = (a' x^2 + b' xy + c' y^2) \]

The converse is obvious by Lemma 3.3.

**Definition 3.5.** We define the discriminant \( D \) of \( f(x, y) = ax^2 + bxy + cy^2 \) by \( D = b'^2 - 4ac' \).

**Lemma 3.6.** Suppose \( f \) and \( g \) satisfy \( f(x, y) = g(px + qy, mx + ny) \). Let \( D \) and \( D' \) be the discriminants of \( f \) and \( g \) respectively. Then \( D = (px - qy)^2 D' \).

*(Proof)* Let \( f(x, y) = ax^2 + bxy + cy^2 \) and \( g(x, y) = a' x^2 + b' xy + c' y^2 \). Then from the equation \( f(x, y) = g(px + qy, mx + ny) \), we have

\[
\begin{align*}
a &= a' p^2 + b' pq + c' q^2, \\
b &= 2a' pq + b' (ps + qr) + c' rs, \\
c &= a' q^2 + b' qs + c' s^2.
\end{align*}
\]

Hence

\[
b'^2 - 4ac' = (2a' pq + b' (ps + qr) + c' rs)^2 - 4(a' p^2 + b' pq + c' q^2) (a' q^2 + b' qs + c' s^2) = (ps - qr)^2 (b'^2 - 4ac').
\]

**Corollary 3.7.** Equivalent forms have the same discriminants.
Lemma 3.8. Let \( D \) be the discriminant of \( ax^2 + bx + cy^2 \).
Then
(i) \( D \equiv 0, 1 \mod 4 \)
(ii) \( D \equiv 0 \iff b = \text{even} \)
\( D \equiv 1 \iff b = \text{odd} \)

(Proof) Since \( D = b^2 - 4ac \) we have \( D \equiv b^2 \equiv 0 \) or 1 mod 4. And obviously \( b \) is even if and only if \( D \equiv 0 \mod 4 \) and \( b \) is odd if and only if \( D \equiv 1 \mod 4 \).

Definition 3.9. A quadratic form \( f(x, y) = ax^2 + bxy + cy^2 \) with discriminant \( D \) is called indefinite if \( D > 0 \) and definite if \( D < 0 \). When \( f \) is definite (i.e., \( D < 0 \)), we say it is positive (negative, respectively) definite if \( a > 0 \) (\( a < 0 \), respectively).

Remark 3.10. From the identity \( 4acf(x, y) = (2ax + by)^2 - Dy^2 \), we see that:
(i) if \( f \) is indefinite, \( f(x, y) \) represents both positive and negative integers,
(ii) if \( f \) is positive definite, \( f(x, y) \) represents only positive integers,
(iii) if \( f \) is negative definite, \( f(x, y) \) represents only negative integers.

Definition 3.11. A primitive positive definite form \( f(x, y) = ax^2 + bxy + cy^2 \) is said to be reduced if \( |b| \leq a \leq c \), and \( b \geq 0 \) if either \( |b| = a \) or \( a = c \).
Example 5. Both $3x^2+2xy+5y^2$ and $3x^2-2xy+5y^2$ are reduced forms of discriminant $-56$. On the other hand, of two forms $2x^2+2xy+3y^2$ of discriminant $-20$, only $2x^2+2xy+3y^2$ is reduced.

Theorem 3.12. Every primitive positive definite form is properly equivalent to a unique reduced form.

(Proof) We will only show the existence. For the uniqueness, refer [1], Chapter one.

(i) The first step is to show that a given form is properly equivalent to one satisfying $|b|\leq a \leq c$. Among all forms properly equivalent to the given one, pick $f(x, y) = ax^2 + bxy + cy^2$ so that $|b|$ is as small as possible. If $a < |b|$, then $g(x, y) = f(x + ny, y) = ax^2 + (2am + b)xy + cy^2$ is properly equivalent to $f(x, y)$. Since $a < |b|$, we can choose $m = \mathbb{Z}$ so that $|2am + b| < |b|$, which contradicts our choice of $f(x, y)$. Thus $a \geq |b|$, and $c \geq |b|$ follows similarly. If $a > c$, the proper equivalence $(x, y) \mapsto (-y, x)$ results in a form satisfying $|b| \leq a \leq c$.

(ii) The next step is to show that such a form is properly equivalent to a reduced one. By definition 3.11, the form is already reduced unless $b > 0$ and $a = -b$ or $a = c$. In these exceptional cases $ax^2 - bxy + cy^2$ is reduced, so that we need only show that the two forms
\[ \alpha x^2 + \beta xy + \gamma y^2 \] are properly equivalent. This can be done as follows:

\[ a = -b : (x, y) \mapsto (x + y, y) \text{ takes } \alpha x^2 - \alpha y^2 + \gamma y^2 \text{ to } \alpha x^2 + \alpha xy + \gamma y^2 \]

\[ a = c : (x, y) \mapsto (-y, x) \text{ takes } \alpha x^2 + \beta xy + \gamma y^2 \text{ to } \alpha x^2 - \beta xy + \gamma y^2. \]

**Example 6.** The form \( 2x^2 - 2xy + 3y^2 \) which is not reduced is equivalent to the reduced form \( 2x^2 + 2xy + 3y^2 \) under the substitution \((x, y) \mapsto (x + y, y)\).

**Remark 3.13.** In each class of primitive positive definite forms of discriminant \( D \), there is a unique reduced form \( \alpha x^2 + \beta xy + \gamma y^2 \) of discriminant \( D \) by Theorem 3.12. Note that \( b^2 \leq a^2 \) and \( a \leq c \) so that \( -D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \) and thus \( a \leq \sqrt{\frac{-D}{3}} \). Since \( |b| \leq a \), \( a \) and \( b \) are bounded, and so there are finitely many choices for \( a, b \). Since \( b^2 - 4ac = D \), the same is true for \( c \). Hence there are only a finite number of reduced forms of discriminant \( D \). We denote this number by \( h(D) \), which is called the class number of \( D \).

**Examples 7.** In this example, we find all reduced forms of discriminant \( D = -20 \). Let \( \alpha x^2 + \beta xy + \gamma y^2 \) be a reduced form of discriminant \( D = -20 \). Since \( a \leq \sqrt{\frac{-D}{3}} = \sqrt{\frac{-20}{3}} = 2.5 \ldots \),
\( a = 1 \) or 2

(i) \( a = 1 \). In this case \( b = 0 \) or 1. But if \( b = 1 \), then \( 4c = 21 \), which is impossible. If \( b = 0 \), then \( c = 5 \). Hence we get a reduced form \( x^2 + 5y^2 \).

(ii) \( a = 2 \). By a similar analysis, we have two forms \( 2x^2 \pm 2xy + 3y^2 \). But \( 2x^2 - 2xy + 3y^2 \) is not reduced and is equivalent to the reduced form \( 2x^2 + 2xy + 3y^2 \) as was explained in Example 6.

From (i), (ii), \( \mathcal{H}(-20) = 2 \) and \( x^2 + 5y^2, 2x^2 + 2xy + 3y^2 \) are the only reduced forms of discriminant \(-20\).

**Examples 8.** By a similar argument as in Examples 7, we can check that \( x^2 + 7y^2 \) is the only reduced form of discriminant \(-28\). Thus \( \mathcal{H}(-28) = 1 \).
§ 4. Primes of the form \( x^2 + \nu y^2 \) for \( \nu = 5 \) and \( \nu = 7 \)

**Proposition 4.1.** Let \( \nu \) be a positive integer and \( p \) be an odd prime not dividing \( \nu \). Then \( \left( \frac{-\nu}{p} \right) = 1 \) if and only if \( p \) is represented by one of the \( h(-4\nu) \) reduced forms of discriminant \( -4\nu \).

(Proof) Suppose that \( p \) is represented by a reduced form \( f \) of discriminant \( -4\nu \). Then \( f \) is equivalent to a form \( px^2 + bx + cy^2 \) by Lemma 3.4 and \( b^2 - 4ac = -4\nu \). Thus \( b^2 \equiv -4\nu \pmod{p} \). Hence \( \left( \frac{-\nu}{p} \right) = \left( \frac{-4\nu}{p} \right) = \left( \frac{b^2}{p} \right) = 1 \).

Conversely, suppose that \( \left( \frac{-\nu}{p} \right) = 1 \). Then \( -\nu \) and thus \( -4\nu \) is a square \( \pmod{p} \), i.e., \( -4\nu \equiv b^2 \pmod{p} \) for some \( b \). We may assume that \( b \) is even, for otherwise we replace \( b \) by \( b + p \). Thus \( -4\nu \equiv b^2 \pmod{4p} \). Therefore \( -4\nu \equiv b^2 - 4pc \) for some \( c \). Then \( px^2 + bx + cy^2 \) has discriminant \( -4\nu \). Let \( f(x, y) \) be the reduced form equivalent to \( px^2 + bx + cy^2 \). Then \( f \) represents \( p \) and the discriminant of \( f \) is \( -4\nu \).

**Theorem 4.2.** For \( \nu \neq 7 \), we have \( p = x^2 + 7y^2 \) if and only if \( p \equiv 1, 9, 11, 15, 23, 25 \pmod{28} \).

(Proof) By Example 8, \( x^2 + 7y^2 \) is the only reduced form of
discriminant $-28$. Hence by Proposition 41, $p$ is represented by $x^2 + 7y^2$ if and only if $(\frac{-7}{p}) = 1$. By using the quadratic reciprocity law, we can check that $(\frac{-7}{p}) = 1$ if and only if $p = 1, 9, 11, 15, 23, 25 \mod 28$.

**Theorem 4.3.** For $p \neq 5$, we have

$$p = x^2 + 5y^2 \iff p = 1, 9 \mod 20.$$  
$$p = 2x^2 + 2xy + 3y^2 \iff p = 3, 7 \mod 20.$$  

(Proof) By Example 7, $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are the only reduced forms of discriminant $-20$. Hence, by Proposition 41, $p$ is represented by either $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ if and only if $(\frac{-5}{p}) = 1$, i.e., $p = 1, 3, 7, 9 \mod 20$. If $p = 3, 7 \mod 20$, then by reading the equation $p = x^2 + 5y^2 \mod 5$, we see that it is impossible. Thus if $p = 3, 7$, then $p$ must be represented by $2x^2 + 2xy + 3y^2$. On the other hand, if $p = 1, 9 \mod 20$, then by reading the equation $p = 2x^2 + 2xy + 3y^2 \mod 4$, we get a contradiction. Thus these primes should be represented by $x^2 + 5y^2$. Therefore we have the theorem.
References

