Class Numbers and Sums of Squares in a Quadratic Field.

George Warthen Lofquist
Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation
https://repository.lsu.edu/gradschool_disstheses/1348

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
LOFQUIST, George Warthen, 1930-
CLASS NUMBERS AND SUMS OF SQUARES IN A QUADRATIC FIELD.

Louisiana State University and Agricultural and Mechanical College, Ph.D., 1967
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan
CLASS NUMBERS AND SUMS OF SQUARES IN A QUADRATIC FIELD

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

George Warthen Lofquist
B.S., University of North Carolina, 1952
M.Ed., University of North Carolina, 1959
M.S., Louisiana State University, 1963
August, 1967
ACKNOWLEDGMENT

The author acknowledges with gratitude the assistance, encouragement, and patience of Professor Gordon Pall during his direction of the writing of this dissertation.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION AND NOTATION</td>
<td>1</td>
</tr>
<tr>
<td>I</td>
<td>FACTORIZATION OF QUATERNIONS AND SUMS OF FOUR SQUARES</td>
</tr>
<tr>
<td>II</td>
<td>CLASS-NUMBERS AND SUMS OF THREE SQUARES</td>
</tr>
<tr>
<td></td>
<td>SELECTED BIBLIOGRAPHY</td>
</tr>
<tr>
<td></td>
<td>VITA</td>
</tr>
</tbody>
</table>
ABSTRACT

This paper is a study of the relationship between the number of classes of primitive totally positive binary quadratic forms of a given determinant and the number of certain quaternions of a given norm where the coefficients of the forms and the components of the quaternions are from the integral elements in the field $\mathbb{R}(\sqrt{2})$. The related problem of finding the number of representations of an integer as a sum of squares is also considered.

An integer $\eta = a_0 + a_1\sqrt{2}$ in $\mathbb{R}(\sqrt{2})$ is called odd if $n(\eta) = \eta\overline{\eta}$ is an odd rational integer, and $\eta$ is called evenish if $a_1$ is even. The two major results of Chapter I are the two independent theorems:

Theorem 1.1. If $v = v_0 + v_1i_1 + v_2i_2 + v_3i_3$ is a primitive (mod $\eta$) quaternion such that $\eta$ divides $N(v)$, $\eta$ is evenish and $n(\eta)$ is odd and positive, then $v$ has exactly eight right divisors $t$ with $N(t) = \eta$. The divisors are the eight left-associates $\pm t, \pm i_1t$.

Theorem 1.2. If $\xi = \pi_1^1 \cdots \pi_k^k$ where $\pi_1$ is an odd evenish and totally positive prime in $\mathbb{Z}(\sqrt{2})$, then

$$r_4(\xi) = 8 \prod_{i=1}^{k} \left( \sum_{j=0}^{h_i} [n(\pi_i)]^j \right)$$
where $r_4(\delta)$ is the number of representations of $\delta$ as a sum of four squares.

Let $h(\delta)$ be the number of classes of primitive totally positive binary quadratic forms of determinant $\delta$. The principal result of Chapter II is:

**Theorem 2.1.** The number of classes of primitive totally positive binary quadratic forms of determinant $\delta$ where $\delta$ is odd evenish totally positive and $\neq 1$ and is given by

$$h(\delta) = \frac{1}{12} r_1(\delta) + \frac{1}{24} r_{ii}(\delta) + \frac{1}{8} r_{iii}(\delta) + \frac{1}{24} r_{iv}(\delta)$$

where $r_\alpha(\delta)$ is the number of primitive pure quaternions

$$x = x_1^1 + x_2^2 + x_3^3$$

of norm $\delta$ satisfying the following conditions for $\alpha = i, ii, iii, iv$.

i) $n(x_1) = n(x_2) = n(x_3)$ fails and exactly two of $x_1, x_2, x_3$ are congruent,

ii) $n(x_1) = n(x_2) = n(x_3)$ fails and no two of $x_1, x_2, x_3$ are congruent,

iii) $n(x_1) = n(x_2) = n(x_3) = 1$ and $x_1 = x_2 = x_3$,

iv) $n(x_1) = n(x_2) = n(x_3) = 1$ and exactly two of $x_1, x_2, x_3$ are congruent. All congruences are modulo two.
By utilizing theorem 1.2 and some of the results preliminary to the theorem just stated we obtain:

**Theorem 2.2.** If \( \xi = \pi_1^{k_1} \pi_2^{k_2} \cdots \pi_m^{k_m} \) where \( \pi_i \) is an odd evenish totally positive prime with \( (\pi_i, \pi_j) = 1 \) for \( i \neq j \) and \( \eta \) is an odd evenish totally positive square free integer, then

\[
r_3(\xi^2 \eta) = r_3(\eta) \prod_{i=1}^{m} T_i
\]

where

\[
T_i = \frac{n(\pi_i)^{k_i+2}}{n(\pi_i) - 1} - \frac{\eta}{\pi_i} \frac{n(\pi_i)^{k_i+1}}{n(\pi_i) - 1}
\]

and

\[r_3(\eta)\] is the number of representations of \( \eta \) as the sum of three squares.
INTRODUCTION AND NOTATION

In his paper 'On the Arithmetic of Quaternions' [5] Professor Gordon Pall obtained formulae for the number of classes of primitive positive binary quadratic forms with rational integral coefficients and of a given determinant by using properties of Lipschitz quaternions. The methods involved lend themselves to a consideration of the problem of counting the number of classes of primitive totally positive binary quadratic forms of a given determinant but having as coefficients integral elements of a quadratic extension of the rational numbers. In Chapter II we obtain a theorem which gives a representation for the number of classes of such forms in terms of the numbers of quaternions of certain types.

In Chapter I we prove a basic theorem on the factorization of quaternions and also obtain a result on the number of representations of certain numbers in \( \mathbb{R}(\sqrt{2}) \) as a sum of four squares.

Throughout this paper we will restrict the word integer to mean an algebraic integer in the field \( \mathbb{R}(\sqrt{2}) \). Lower case Greek letters will be used to designate

---

1 Pairs of numbers in brackets refer to correspondingly numbered references in the Selected Bibliography and page numbers, respectively. A single number refers to the similarly numbered reference in the Selected Bibliography.
these integers and \( \mathbb{Z}(\sqrt{2}) \) will be used to denote the ring of integral elements in \( \mathbb{R}(\sqrt{2}) \). The norm of an integer \( \eta = a_0 + a_1\sqrt{2} \) will be denoted by \( n(\eta) = (a_0 + a_1\sqrt{2})(a_0 - a_1\sqrt{2}) = a_0^2 - 2a_1^2 \). If \( \eta = a_0 + a_1\sqrt{2} \), then the conjugate of \( \eta \) is \( \bar{\eta} = a_0 - a_1\sqrt{2} \). \( \eta \) will be called totally positive if \( a_0 > |a_1\sqrt{2}| \). In case \( \eta = a_0 + 2a_1\sqrt{2} \), then \( \eta \) will be called evenish. We note that the square of any integer is evenish. An integer \( \eta \) will be referred to as odd if \( n(\eta) \) is an odd rational integer. We note further that an integer can be both odd and evenish.

The ring of quaternions considered will be the collection of all expressions of the form \( x = x_0 + x_1i_1 + x_2i_2 + x_3i_3 \) where \( x_j \) is in \( \mathbb{Z}(\sqrt{2}) \) and the multiplication of the symbols \( i_1, i_2, i_3 \) is the usual one

\[
i_1^2 = i_2^2 = i_3^2 = -1, \quad i_1i_2 = i_3, \quad i_2i_3 = i_1, \quad i_3i_1 = i_2.
\]

If \( x = x_0 + x_1i_1 + x_2i_2 + x_3i_3 \), then the conjugate of \( x \) is \( \bar{x} = x_0 - x_1i_1 - x_2i_2 - x_3i_3 \) and the norm of \( x \) is \( N(x) = xx = x_0^2 + x_1^2 + x_2^2 + x_3^2 \). If \( x_0 = 0 \), then \( x \) is called pure, and if \( (x_0,x_1,x_2,x_3) = 1 \), then \( x \) is said to be primitive. Further, if \( x_0 \equiv 0 \, (\text{mod } \eta) \), then \( x \) is called pure \( (\text{mod } \eta) \), and if \( (x_0,x_1,x_2,x_3,\eta) = 1 \), then
$x$ is said to be **primitive** $(\text{mod } \eta)$. If $\pi$ is a prime different from $\sqrt{2}$ and $\pi \not| \eta$, then $(\frac{\eta}{\pi}) = 1$ if $\eta$ is a quadratic residue $(\text{mod } \pi)$ and $-1$ otherwise.
CHAPTER I

FACTORIZATION OF QUATERNIONS AND
SUMS OF FOUR SQUARES

The following basic theorem was proved in its original form by Lipschitz [2] for quaternions with rational integral coefficients and a prime as the divisor of the norm of the quaternion.

We note that if \( x, u, t \) are quaternions such that \( x = ut \), then \( \pm t, \pm i_j t \) for \( j = 1, 2, 3 \) are also right divisors of \( x \) with the same norm as \( t \). Also if \( \eta \) is the norm of a quaternion \( t \), then \( \eta \) is a sum of four squares and hence must be evenish.

**Theorem 1.1.** If \( v = v_0 + v_1 i_1 + v_2 i_2 + v_3 i_3 \) is a primitive \(( \text{mod } \eta)\) quaternion such that \( \eta \) divides \( N(v) \), \( \eta \) is evenish and \( n(\eta) \) is odd and totally positive, then \( v \) has exactly eight right divisors \( t \) with \( N(t) = \eta \). The divisors are the eight left-associates \( \pm t, \pm i_j t \).

In the following lemmata \( \eta \) is assumed to be odd, evenish, and totally positive.

**Lemma 1.2.** If \( x \) and \( y \) are two quaternions such that \( x \equiv y \pmod{\eta} \), then \( x \) and \( y \) have the same right divisors of norm \( \eta \).
PROOF: If the quaternion $t$ is a right divisor of $y$ such that $N(t) = \eta$, then $y = ut$. Thus $x = y + z\eta = ut + z\bar{t}t = (u + zt)t$. A similar argument holds if $t$ is a right divisor of $x$.

Lemma 1.3. If $(N(x), \eta) = 1$, then $v$ and $xv$ have the same right divisors $t$ such that $N(t) = \eta$.

PROOF: If $v = ut$ and $N(t) = \eta$, then $xv = (xu)t$. If, conversely, $xv = ut$ and $(N(x), \eta) = 1$, then there exist two integers $\xi$ and $\theta$ such that $\xi N(x) + \theta \eta = 1$ and $\xi N(x) = 1 \pmod{\eta}$. Thus $1 \cdot v = \xi N(x) \cdot v = \xi \bar{x}xv = (\xi \bar{x}u)t \pmod{\eta}$. Since $v = (\xi \bar{x}u)t \pmod{\eta}$, $t$ is a right divisor of $v$.

Lemma 1.4. If theorem 1.1 holds for every product $\eta$ of $r - 1$ or less primes of odd norm ($r > 1$), then it holds for products $\eta$ of $r$ primes of odd norm.

PROOF: Assume the theorem holds for products $\eta$ of $r - 1$ or fewer primes of odd norm. Assume further that $\pi$ is a prime of odd norm which is positive and such that $\pi \eta$ is a divisor of $N(v)$ and $v$ is primitive $\pmod{\pi \eta}$.

From $v = ut$ with $N(t) = \eta$ and $\pi \eta \xi = N(v) = N(u)N(t)$, it follows that $\pi$ is a factor of $N(u)$. Since $v$ is primitive $\pmod{\pi \eta}$, $u$ must be primitive $\pmod{\pi}$, and the theorem applies to $u$ and $\pi$ so that $u = wx$, where $N(x) = \pi$. Thus $v = w(xt)$ and $N(xt) = \pi \eta$ so $v$ has a right divisor of norm $\pi \eta$.

To show that any two such right divisors are left-associates suppose $v = ux = wy$ with $N(x) = N(y) = \pi \eta$. Then $x = st$ and $y = s't'$ where $N(t) = N(t') = \eta$ and since $t$, $t'$ are right divisors of $v$, by the induction assumption they are left-associates. Thus $t = \theta t'$ where $\theta = \pm i \alpha$, so that
\(N(x) = N(y)\) and \(N(t) = N(t')\) imply that \(N(s\theta) = N(s')\).

Also \(x = s\theta t'\) and \(v = us\theta t' = ws't'\) imply that \(us\theta = ws' = q\) and \(N(s\theta) = N(s') = \pi\). Since \(v\) is primitive (mod \(\pi\)), \(q\) is primitive (mod \(\pi\)), so \(s\theta\) and \(s'\) are left-associates. Thus we have \(s\theta = \varphi s'\) with \(\varphi\) a unit and \(x = st = s\theta t' = \varphi s't = \varphi y\), so \(x\) and \(y\) are left associates.

**Lemma 1.5.** If \(v\) is primitive (mod \(\pi\)), there is a pure quaternion \(x\) with \(N(x)\) prime to \(\pi\) such that \(xv\) is pure (mod \(\pi\)).

**PROOF:** If \(v_0 \neq 0\) (mod \(\pi\)), \(v_1 = v_2 = v_3 = 0\) (mod \(\pi\)), and \(x\) is any pure quaternion such that \(N(x) \neq 0\) (mod \(\pi\)), then \(x_1v_1 + x_2v_2 + x_3v_3 = 0\) (mod \(\pi\)). That is, \(xv\) is pure (mod \(\pi\)).

If at least one of \(v_1, v_2, v_3\), say \(v_1\), is not divisible by \(\pi\), then \((v_1, \pi) = 1\) and \(v_1\xi + \pi\lambda = 1\) for some \(\xi\) and \(\lambda\). Hence \(v_1\xi = 1\) (mod \(\pi\)) and the congruence \(x_1v_1 + x_2v_2 + x_3v_3 = 0\) (mod \(\pi\)) can be rewritten as \(x_1 \equiv \xi v_1 x_1 = -\xi x_2v_2 - \xi x_3v_3 \equiv \eta x_2 + \mu x_3\) (mod \(\pi\)). Substituting \(x_1 \equiv \eta x_2 + \mu x_3\) (mod \(\pi\)) in \(x_1^2 + x_2^2 + x_3^2 \neq 0\) (mod \(\pi\)) yields

\[(1) \quad (1 + \eta^2)x_2^2 + 2\eta\mu x_2 x_3 + (1 + \mu^2)x_3^2 \neq 0\) (mod \(\pi\)).

A solution \(x_2, x_3\) to this incongruence will exist unless all of \(1 + \eta^2\), \(\eta\mu\), \(1 + \mu^2\) \(\neq 0\) (mod \(\pi\)). But \(\eta\mu = 0\) (mod \(\pi\)) implies \(\eta = 0\) or \(\mu = 0\) (mod \(\pi\)) so that \(1 + \eta^2 \neq 0\) or \(1 + \mu^2 \neq 0\) (mod \(\pi\)).
Thus a solution to (1) and the corresponding
\[ x_1 v_1 + x_2 v_2 + x_3 v_3 \equiv 0 \pmod{\pi} \]
and
\[ x_1^2 + x_2^2 + x_3^2 \not\equiv 0 \pmod{\pi} \]
so that \( x \) is of norm prime to \( \pi \) and \( xv \) is pure \((\pmod{t^j})\).

Consider two quaternions \( v \) and \( x \) which satisfy
lemma 1.5. Then if \( w = xv \), \( w \) is pure \((\pmod{\pi})\); and if
\( w' = w - w_0 \), then \( w' \equiv xv \pmod{\pi} \). By lemma 1.2 and 1.3,
\( w' \) and \( v \) have the same right divisors of norm \( \pi \). If
\( \pi \mid xv \), then \( \pi \mid \tilde{x}v = N(x)v \), and from \( (N(x),\pi) = 1 \)
it follows that \( \pi \nmid v \) contrary to the assumption that
\( v \) is primitive \((\pmod{\pi})\). Hence \( \pi \nmid xv \) and \( xv \equiv w' \)
primitive \((\pmod{\pi})\). For some \( j \), \( w'_j \) is not divisible by \( \pi \),
say \( w'_1 \). Then there exists an integer \( \eta \) such that
\[ \eta w'_1 \equiv 1 \pmod{\pi}. \]
Let \( w'' \) be a pure quaternion such that
\( w'' \equiv \eta w' \pmod{\pi} \). But \( (\eta,\pi) = 1 \) implies, by lemma 1.3,
that \( \eta w' \) and \( w' \) have the same right divisors of norm \( \pi \),
and lemma 1.2 implies \( w'' \) and \( \eta w' \) have the same right
divisors of norm \( \pi \). Hence \( w'' \) and \( v \) have the same right
divisors of norm \( \pi \). Taking \( w'' = i_1 - i_2 w_2 - i_3 w_3 \), \( w'' \)
is pure and primitive and from the congruences above we
have \( N(w'') \equiv N(w') \equiv N(xv) \equiv N(v) \pmod{\pi} \) or
\[ 1 + w_2^2 + w_3^2 = \pi \xi \]
for some integer \( \xi \).

By the considerations above we are able to
reduce the proof of the theorem to the case of a
quaternion \( v = i_1 - i_2 v_2 - i_3 v_3 \) such that \( 1 + v_2^2 + v_3^2 = \pi^2 \) for some integer \( \pi \). For such a quaternion \( v \), to find the quaternions \( t \) which satisfy \( v = ut \) and \( N(t) = \pi \) we consider \( v \bar{t} \equiv 0 \) (mod \( \pi \)) with \( N(t) = \pi \). For \( t = t_0 + t_1 i_1 + t_2 i_2 + t_3 i_3 \) this yields

\[
\begin{align*}
\mu_1 &= t_0 + v_2 t_3 - v_3 t_2 \equiv 0 \\
\mu_2 &= t_1 - v_2 t_2 - v_3 t_3 \equiv 0 \\
\mu_3 &= -v_2 t_0 + v_3 t_1 + t_3 \equiv 0 \\
\mu_4 &= -v_3 t_0 - v_2 t_1 - t_2 \equiv 0
\end{align*}
\]

From \( 1 + v_2^2 + v_3^2 \equiv 0 \) (mod \( \pi \)) and (2) we have

\[-v_2 \mu_1 + v_3 \mu_2 \equiv \mu_3 \text{ (mod } \pi \text{)} \text{ and } -v_3 \mu_1 - v_2 \mu_2 \equiv \mu_4 \text{ (mod } \pi \text{)}, \]

so \( \mu_3 \) and \( \mu_4 \) are linear combinations of \( \mu_1 \) and \( \mu_2 \). Thus we need to consider only the conditions

\[
\begin{align*}
t_0 &\equiv v_3 t_2 - v_2 t_3 \pmod{\pi} \\
t_1 &\equiv v_2 t_2 + v_3 t_3 \pmod{\pi}
\end{align*}
\]

Thus every quaternion \( t \) satisfying \( v = ut \) can be found using

\[
(3) \quad t_0 = \pi y_0 + v_3 y_2 - v_2 y_3, \quad t_1 = \pi y_1 + v_2 y_2 + v_3 y_3, \\
t_2 = y_2, \quad t_3 = y_3
\]
where $y_0$, $y_1$, $y_2$, $y_3$ are integers subject to the condition
$\Sigma t_j^2 = \pi$. Upon substitution of the values of $t_j$ this
condition becomes
\[
\pi^2(y_0^2 + y_1^2) + 2\pi v_3(y_0 y_2 + y_1 y_3) - 2\pi v_2(y_1 y_2 - y_0 y_3) + (1 + v_2^2 + v_3^2)(y_2^2 + y_3^2) = \pi.
\]

Since $N(v) = \pi^2$, this reduces to
\[
(4) \quad \pi(y_0^2 + y_1^2) + 2v_3(y_0 y_2 + y_1 y_3) - 2v_2(y_1 y_2 - y_0 y_3) + \pi(y_2^2 + y_3^2) = 1.
\]

The principal third order minor determinant of (4) is
\[
\pi^2 \pi - \pi v_2^2 - \pi v_3^2 = \pi
\]
and the determinant of (4) is
\[
(\pi^2 - v_2^2 - v_3^2)^2 = 1. \quad \text{Since the form in (4) represents}
\]
integers of odd norm and is of determinant 1 it is in
the genus of the sum of four squares. Since there is
only one class [1] in that genus, the form in (4) is
therefore equivalent to the form
\[
(5) \quad u_0^2 + u_1^2 + u_2^2 + u_3^2.
\]

Thus each representation of 1 by the form (4) corresponds
biuniquely to a representation of 1 by (5) of which
there are exactly eight. If $t$ is a quaternion of norm $\pi$
satisfying $v = ut$, then each of the quaternions $\pm t$, $\pm i \pm t$
also is of norm π and satisfies v = ut. Since there are only eight such quaternions, this set includes all possible right divisors of v of norm π.

**Corollary 1.6.** If v is a primitive quaternion, \( \eta \mid N(v) \), \( n(\eta) \) is even and \( n(\frac{N(v)}{\eta}) \) is odd, evenish, and positive, then v has exactly one set of right divisors of norm \( \eta \).

**PROOF:** By the theorem, if \( v = ut \) and \( n(N(u)) \) is odd and positive, then u is determined to within a right unit factor, hence t is determined to within a left unit factor.

In the remainder of this chapter, \( \pi \) will represent an odd prime in \( \mathbb{Z}(\sqrt{2}) \) and \( p \) an odd rational prime.

**Lemma 1.7.** If \( \pi = a_0 + a_1\sqrt{2} \) is a prime in \( \mathbb{Z}(\sqrt{2}) \), and if \( n(\pi) = p \), an odd rational prime, then \( \pi \) is a factor of \( \xi = b_0 + b_1\sqrt{2} \) if and only if

\[
a_0b_1 \equiv a_1b_0 \pmod{p}
\]

**PROOF:** Since \( p = n(\pi) = a_0^2 - 2a_1^2 \), if \( a_1 \) is odd, then \( p \equiv -1 \pmod{8} \); and if \( a_1 \) is even, \( p \equiv 1 \pmod{8} \) so that in either case we have \( p = 8k \pm 1 \).

Dividing \( \xi \) by \( \pi \) we get

\[
\frac{\xi}{\pi} = \frac{\xi - \pi}{\pi} = \frac{(a_0b_0 - 2a_1b_1) + (a_0b_1 - a_1b_0)\sqrt{2}}{p}
\]
and \( \pi \) is seen to be a divisor of \( \xi \) if and only if
\[
a_0b_0 - 2a_1b_1 \equiv 0 \pmod{p} \quad \text{and} \quad a_0b_1 - a_1b_0 \equiv 0 \pmod{p}
\]
both hold. However, if \( a_0b_1 - a_1b_0 = 0 \pmod{p} \), then
\[
a_0b_1 \equiv a_0a_1b_0 \pmod{p}.
\]
Hence from \( a_0^2 - 2a_1^2 \equiv 0 \pmod{p} \) it follows that
\[
2a_1^2b_1 \equiv a_0a_1b_0 \pmod{p}
\]
and hence
\[
a_0b_1 \equiv a_0b_0 \pmod{p}.
\]
Thus the one condition
\[
a_0b_1 \equiv a_1b_0 \pmod{p}
\]
is both necessary and sufficient for \( \pi \) to be a divisor of \( \xi \).

**Lemma 1.8.** If \( \pi \) is an odd prime in \( \mathbb{Z}(\sqrt{2}) \), then
-1 is a quadratic non-residue \( \pmod{\pi} \) if and only if \( n(\pi) \) is a rational prime congruent to -1 \( \pmod{8} \).

**PROOF:** Suppose \( n(\pi) \equiv \pm 1 \pmod{8} \). Then
\[
\xi^2 \equiv -1 \pmod{\pi}
\]
has a solution \( \xi = b_0 + b_1\sqrt{2} \) if and only if
\[
1 + b_0^2 + 2b_1^2 + 2b_0b_1\sqrt{2} \equiv 0 \pmod{\pi}.
\]
If \( \pi = a_0 + a_1\sqrt{2} \) with \( n(\pi) = p \), then \( a_1 \neq 0 \) and the last congruence holds if and only if
\[
2b_0b_1a_0 = a_1 + a_1b_0 + 2a_1b_1^2 \pmod{p}
\]
by lemma 1.7. That is, if \( a_1b_0^2 - 2a_0b_0b_1 + 2a_1b_1^2 \equiv -a_1 \pmod{p} \).
Since the determinant of the form on the left in this congruence is
\[
2a_1^2 - a_0^2 = -p
\]
and the form represents \( a_1 \), the form represents \( -a_1 \) if and only if \( \left( \frac{a_1}{p} \right) = \left( \frac{-a_1}{p} \right) \) or if and only if
\[
p = 4k + 1.\]
Thus for \( n(\pi) \equiv \pm 1 \pmod{8} \), -1 is a quadratic
non-residue if and only if \( n(\pi) \equiv -1 \pmod{8} \).

In case \( \pi = 8m + 3 \) is also a rational prime, then
\[
\xi = b_0 + b_1\sqrt{2} \text{ is a solution to } \xi^2 \equiv -1 \pmod{\pi} \text{ if and only if } \]
\[b_0^2 + 2b_1^2 \equiv -1 \pmod{\pi} \text{ and } b_0b_1 \equiv 0 \pmod{\pi}.\]
Taking \( b_0 \equiv 0 \pmod{\pi} \) reduces these last conditions to \( 2b_1^2 \equiv -1 \pmod{\pi} \).
From this we have \( 16b_1^2 + 8 \equiv 0 \pmod{\pi} \) or \( (4b_1)^2 \equiv -8 \pmod{\pi} \).
Thus there is a solution to \( \xi^2 \equiv -1 \pmod{\pi} \) if there is a solution to \( \eta^2 \equiv -8 \pmod{\pi} \). Since \( \pi = 3 \pmod{8} \),
\[
\left(\frac{-8}{\pi}\right) = (\frac{-1}{\pi})(\frac{2}{\pi})^3 = (-1)^4 = 1 \text{ so that } -1 \text{ is a quadratic residue } \pmod{\pi} \text{ if } \pi = 8m + 3.

Similarly, if \( \pi = 8m - 3 \) is a rational prime, then
\( \xi^2 \equiv -1 \pmod{\pi} \) has a solution if and only if \( b_0^2 + 2b_1^2 \equiv -1 \)
and \( b_0b_1 \equiv 0 \pmod{\pi} \). Letting \( b_1 = 0 \), these last conditions reduce to \( b_0^2 \equiv -1 \pmod{\pi} \); but since \( \pi = 1 \pmod{4} \), \( -1 \) is a quadratic residue and \( \xi^2 \equiv -1 \pmod{\pi} \) has a solution.

**Lemma 1.9.** If \( \pi \) is a prime in \( \mathbb{Z}(/2) \), then for any integer \( \gamma \) in \( \mathbb{Z}(/2) \) there exist \( \xi, \eta \) in \( \mathbb{Z}(/2) \) which satisfy \( \xi^2 + \eta^2 \equiv \gamma \pmod{\pi} \).

**PROOF:** Consider first a prime \( \pi \) with \( n(\pi) \) odd. The ideal \( (\pi) \) in \( \mathbb{Z}(/2) \) is maximal so that \( \mathbb{Z}(/2)/(\pi) \) is a
field containing \( n(\pi) \) elements. Hence there are either \( p \) or \( p^2 \) elements in \( \mathbb{Z}(\sqrt{2})/(\pi) \) for a rational prime \( p \).

Now in any finite field with \( p^k \) elements exactly \( \frac{p^k + 1}{2} \) of them are squares. For if \( x^2 = y^2 \), then

\[
x^2 - y^2 = (x + y)(x - y) = 0 \implies x = y \text{ or } x = -y.
\]

Thus there are \( \frac{p^k - 1}{2} \) non-zero squares or \( \frac{p^k + 1}{2} \) squares altogether.

Similarly, there exist \( \frac{p^k + 1}{2} \) elements of the field of the form \(-y^2 + m\) for a fixed element \( m \) of the field. Since

\[
2 \cdot \frac{p^k + 1}{2} > p^k,
\]

there is an element in common from the two sets so there exist \( x, y \) in the field satisfying \( x^2 + y^2 = m \). Thus for \( \gamma \), the residue class in \( \mathbb{Z}(\sqrt{2})/(\pi) \) which contains \( \gamma \), there is a solution to \( \bar{x}^2 + \bar{y}^2 = \bar{\gamma} \) in \( \mathbb{Z}(\sqrt{2})/(\pi) \). Let \( \xi \) and \( \eta \) be elements of the residue classes \( \bar{x} \) and \( \bar{y} \) which satisfy the last equation, then \( \xi^2 + \eta^2 \equiv \gamma \pmod{\pi} \).

If \( \pi = \sqrt{2} \) and \( \gamma = a_0 + a_1\sqrt{2} \), let \( \xi = a_0 \) and \( \eta = 0 \).

**Lemma 1.10.** If \( \pi \) is a prime in \( \mathbb{Z}(\sqrt{2}) \) of odd norm, then the congruence \( u^2 + v^2 \equiv 1 \pmod{\pi} \) has \( n(\pi) - \left( \frac{-1}{\pi} \right) \) solutions.
PROOF: Let \( \gamma \) be a non-zero element of \( \mathbb{Z}(\sqrt{2}) \) of which \( \pi \) is not a factor. By lemma 1.9 there exists at least one solution to \( x^2 + y^2 \equiv \gamma \pmod{\pi} \), say \( \xi, \eta \). Using Gaussian integers with coefficients from \( \mathbb{Z}(\sqrt{2}) \), consider the congruence

\[
(6) \quad (\xi + i\eta)(u + iv) \equiv x + iy \pmod{\pi}
\]

or equivalently, the pair of congruences

\[
(7) \quad \begin{array}{c}
\xi u + \eta v \equiv x \\
-\eta u + \xi v \equiv y
\end{array} \pmod{\pi}
\]

Since \( \xi^2 + \eta^2 \equiv \gamma \not\equiv 0 \pmod{\pi} \), there is a one to one correspondence between the pairs \( x, y \) and \( u, v \) satisfying the congruences in (7). Taking the norms of the Gaussian integers in (6) yields \((\xi^2 + \eta^2)(u^2 + v^2) \equiv x^2 + y^2 \pmod{\pi}\)
or \( \gamma(u^2 + v^2) \equiv x^2 + y^2 \pmod{\pi} \). Thus there is a one to one correspondence between the pairs \( x, y \) and \( u, v \) such that \( x^2 + y^2 \equiv \gamma \pmod{\pi} \) and \( u^2 + v^2 \equiv 1 \pmod{\pi} \).

Let \( a \) be the number of solutions to \( u^2 + v^2 \equiv 1 \pmod{\pi} \) and \( b \) the number of solutions to \( x^2 + y^2 \equiv 0 \pmod{\pi} \). If \( (-1)^{\frac{1}{\pi}} = -1 \), then \( x^2 \equiv -y^2 \pmod{\pi} \) and thus \( x^2 + y^2 \equiv 0 \pmod{\pi} \) has no solution except \( x \equiv y \equiv 0 \pmod{\pi} \). If \( (-1)^{\frac{1}{\pi}} = 1 \), then for each \( x \) from a complete set of \( n(\pi) - 1 \) non-zero
residues modulo $\pi$ there are two numbers $\pm y$ for which the congruence $x^2 \equiv -y^2 \pmod{\pi}$ is satisfied. In either case we have $b = 1 + [n(\pi) - 1][1 + (\pi^{-1})]$ where the $1$ is obtained in counting the solution $x \equiv y \equiv 0 \pmod{\pi}$.

Since there are $n(\pi) - 1$ non-zero residues in a complete residue system modulo $\pi$, the second paragraph above implies there are $a[n(\pi) - 1]$ total ways of representing them modulo $\pi$ by $x^2 + y^2$. Hence there are $b + a[n(\pi) - 1]$ ways of evaluating $x^2 + y^2 \pmod{\pi}$, but with $n(\pi)$ choices for each of $x$ and $y$ we have

$$b + a[n(\pi) - 1] = [n(\pi)]^2$$

$$a = \frac{[n(\pi)]^2 - 1 - [n(\pi) - 1][1 + (\pi^{-1})]}{n(\pi) - 1}$$

$$= \frac{[n(\pi) - 1][n(\pi) + 1 - [1 + (\pi^{-1})]]}{n(\pi) - 1}$$

$$= n(\pi) - (\pi^{-1})$$.

Thus $u^2 + v^2 \equiv 1 \pmod{\pi}$ has $n(\pi) - (\pi^{-1})$ solutions.

In explanation of the hypothesis of the following theorem we note that the square of any number in $Z(\sqrt{2})$ is totally positive and the sum of two or more totally positive numbers is again a totally positive number. Further, since $(a_0 + a_1\sqrt{2})^2 = (a_0^2 + 2a_1^2) + 2a_0a_1\sqrt{2}$, we see that the
coefficient of $\sqrt{2}$ in a sum of squares must be even. If 
\[ \eta = a_0 + 2a_1\sqrt{2} \]
is a sum of four squares with odd norm and has an odd prime \( \pi = p_0 + p_1\sqrt{2} \) as a factor such that the other factor is \( \xi = b_0 + 2b_1\sqrt{2} \), then 
\[ a_0 = p_0b_0 + 4p_1b_1 \]
and 
\[ 2a_1 = 2p_0b_1 + p_1b_0. \]
From the last two relations it follows that since \( a_0 \) is odd, \( p_0b_0 \) and hence \( b_0 \) is odd so \( p_1 \) is even. Thus we can write \( \eta = p_0 + 2p_1\sqrt{2} \). The symbol \( r_4(\eta) \) denotes the number of representations of \( \eta \) as a sum of four squares.

Theorem 1.11. If \( \eta = p_0 + 2p_1\sqrt{2} \) is an odd prime in \( \mathbb{Z}(\sqrt{2}) \) which is totally positive and \( \eta = a_0 + 2a_1\sqrt{2} \) is odd and totally positive, then

\[ r_4(\eta) = (n(\pi) + 1)r_4(\eta) - n(\pi)r_4(\frac{\eta}{\pi}) \]

where \( r_4(\frac{\eta}{\pi}) = 0 \) if \( \frac{\eta}{\pi} \) is not an integer.

PROOF: We first note that \( n(\pi) = p_0^2 - 8p_1^2 = 1 \)
so that we need consider no primes of norm congruent to 
\(-1 \pmod{8}\).

We will consider sets of vectors \( \{x, y, z, w\} \) with elements in \( \mathbb{Z}(\sqrt{2}) \) which satisfy

\[ x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{\pi} \]

and which have the property that any two of the sets have
only the vector \([0, 0, 0, 0]\) in common.

If \([x, y, z, w]\) is a vector satisfying (9) and \(\pi\) is not a factor of \(x^2 + y^2\), then by the use of Gaussian integers with coefficients from \(\mathbb{Z}(\sqrt{2})\), the congruence

\[
(x + iy)(u + iv) \equiv z + iw \pmod{\pi}
\]

has a solution \(u, v\). For

\[(x - iy)(x + iy)(u + iv) \equiv (x - iy)(z + iw) \pmod{\pi}\]

reduces to

\[(x^2 + y^2)(u + iv) \equiv (xz + yw) + i(xw - yz) \pmod{\pi}\]

which is equivalent to the pair of congruences

\[
(x^2 + y^2)u \equiv xz + yw \pmod{\pi}
\]

\[
(x^2 + y^2)v \equiv xw - yz
\]

for which a solution \(u, v\) exists which is unique \(\pmod{\pi}\).

Taking the norms of the Gaussian integers in (10) yields

\[(x^2 + y^2)(u^2 + v^2) \equiv z^2 + w^2 \pmod{\pi}.
\]

Since \(x^2 + y^2 \equiv -(z^2 + w^2) \pmod{\pi}\) it follows that

\[(11) \quad u^2 + v^2 \equiv -1 \pmod{\pi}.
\]

Expanding (10) yields

\[
xu - yv \equiv z \pmod{\pi}.
\]

\[
xv + yu \equiv w
\]
If a pair \( u, v \) satisfies (11), then any vector \( \{x, y, z, w\} \) which for the pair \( u, v \) satisfies (10) will also satisfy (9). For each pair satisfying (11) we define the space
\[
S(u,v) = \{ \{x, y, z, w\} \mid \{x, y, z, w\} \text{ satisfies (10)} \}.
\]
From the above, if \( \{x, y, z, w\} \) satisfies (9) and \( \pi \) is not a factor of \( x^2 + y^2 \), then \( \{x, y, z, w\} \) belongs to an unique space \( S(u,v) \).

If \( \{x, y, z, w\} \) is in \( S(u,v) \) and \( x \equiv y \equiv 0 \pmod{\pi} \), then (10), or (12), shows that \( z \equiv w \equiv 0 \pmod{\pi} \). Conversely, if \( z \equiv w \equiv 0 \pmod{\pi} \), \( u^2 + v^2 \equiv -1 \pmod{\pi} \) and (12) show that \( x \equiv y \equiv 0 \pmod{\pi} \).

In case \( \{x, y, z, w\} \) satisfies (9) and belongs to \( S(u,v) \) and is such that \( x^2 + y^2 \equiv 0 \pmod{\pi} \) with \( y \not\equiv 0 \pmod{\pi} \), then \( x \equiv \tau y \pmod{\pi} \) where \( \tau \) is a solution to \( \tau^2 \equiv -1 \pmod{\pi} \). For a fixed \( \tau \) such that \( \tau^2 \equiv -1 \pmod{\pi} \) and a given \( y \) prime to \( \pi \), if \( x \equiv \tau y \pmod{\pi} \), then \( \tau x \equiv -y \pmod{\pi} \) and since (12) holds for vectors in \( S(u,v) \) we have \( xu - yv \equiv z \pmod{\pi} \) and hence \( \tau xu + \tau xv \equiv z \pmod{\pi} \) or \( \tau(yu + xv) \equiv z \pmod{\pi} \). Thus from the other congruence in (12), \( \tau w \equiv z \pmod{\pi} \).

We now show that each space \( S(u,v) \) contains one and only one vector \( \{x, y, z, w\} \) satisfying (9) for a given \( y \not\equiv 0 \pmod{\pi} \) and for a fixed \( \tau \) satisfying \( \tau^2 \equiv -1 \pmod{\pi} \) and such that \( x \equiv \tau y \) and \( z \equiv \tau w \pmod{\pi} \). Each space \( S(u,v) \) contains one such vector since for such a
given \( y \), we can take

\[
x = \tau y, \quad z = \tau yu - yv, \quad \text{and} \quad w = -\tau [\tau yu - yv] \pmod{\tau}
\]

for which (12) will hold. The uniqueness of the vector is seen by noting that since \( u^2 + v^2 \equiv -1 \pmod{\tau} \), for a given pair \( x, y \), there is an unique solution to (12) \pmod{\tau}.

Conversely, if \( y \not\equiv 0 \pmod{\tau} \), \( x \equiv \tau y \pmod{\tau} \) and \( z \equiv \tau w \pmod{\tau} \) for a fixed \( \tau \) satisfying \( \tau^2 \equiv -1 \pmod{\tau} \), then solving for \( u, v \) in \( xu - yv = z \) and \( u^2 + v^2 \equiv -1 \pmod{\tau} \) shows that the pair \( u, v \) is unique \pmod{\tau}. Hence again the only vector common to two of the spaces \( S(u,v) \) is the zero vector \([0, 0, 0, 0]\).

We have seen that each vector \([x, y, z, w]\) satisfying (9) with \( x^2 + y^2 \not\equiv 0 \pmod{\tau} \) belongs to an unique space \( S(u,v) \) and each such vector satisfying (9) with \( x^2 + y^2 \equiv 0 \pmod{\tau} \) and \( y \not\equiv 0 \pmod{\tau} \) belongs to one and only one space \( S(u,v) \). Moreover for each pair \( u, v \) satisfying (11), \( S(u,v) \) is non-empty. Hence there exist as many spaces \( S(u,v) \) as there are solutions to (11). Since \( n(\pi) \equiv 1 \pmod{8} \), by lemmata 1.8, 1.9, 1.10, there are \( n(\pi) - (\frac{-1}{\pi}) \) solutions to (11). Since \( (\frac{-1}{\pi}) = 1 \), we have \( n(\pi) - 1 \) spaces \( S(u,v) \) which have only \([0, 0, 0, 0]\) in common for any two of them.

For a fixed \( y \) such that \( y \not\equiv 0 \pmod{\tau} \) and a fixed \( \tau \) such that \( \tau^2 \equiv -1 \pmod{\tau} \), the relations
yield a vector satisfying (9) which is not in any of the previous \( n(\pi) - 1 \) spaces. For from (10), \( xu - yv = z \) and \( yu + xv = w \) (mod \( \pi \)). Hence if \( z \equiv -\tau w \) (mod \( \pi \)) we have
\[
xu - yv = -\tau yu - \tau xv \quad \text{(mod \( \pi \))}
\]
which, using \( x \equiv \tau y \) yields
\[
xu + \tau xv = -\tau yu + yv \quad \text{(mod \( \pi \))}
\]
so that \( x(u + \tau v) \equiv -\tau y(u + \tau v) \) (mod \( \pi \)) and thus \( x \equiv -\tau y \), a contradiction. This exhausts all cases in which \( x^2 + y^2 \equiv 0 \) (mod \( \pi \)) so that for the two signs of \( \tau \) we get two additional spaces of vectors satisfying (9) for a total of \( n(\pi) + 1 \) spaces.

If \( S \) is a space determined by a given \( y \) and \( \tau \) such that \( y \not\equiv 0 \) and \( \tau \equiv -1 \) (mod \( \pi \)) and (13), then for \( \{x, y, z, w\} \) in \( S \), \( \{x, y, z, -w\} \) satisfies (9). For \( u = -\tau, v = 0 \), this latter vector satisfies (10) since \( (x + iz)(-\tau) = y - iw \) (mod \( \pi \)) if and only if \(-x\tau = y \) and \( \tau z = w \) or \( x \equiv \tau y, z \equiv -\tau w \) (mod \( \pi \)). Hence for each \( \{x, y, z, w\} \) in \( S \) there is a vector \( \{x, z, y, -w\} \) in \( S(-\tau,0) \). The converse argument is similar so that the number of vectors in \( S \) is the same as the number of vectors in \( S(-\tau,0) \).

Thus the number of vectors in each of the \( n(\pi) + 1 \) spaces can be found by the substitution
\[
x = x_1, \ y = y_1, \ z = \pi z_1 + x_1 u - y_1 v, \ w = \pi w_1 + x_1 v + y_1 u
\]
in \( x^2 + y^2 + z^2 + w^2 = \pi r \), where \( x_1, y_1, z_1, w_1 \) are
arbitrary integers in $Z(\sqrt{2})$. The substitution yields

$$x_1^2 + y_1^2 + \pi^2 z_1^2 + x_1^2 u_1^2 + y_1^2 v_1^2 + \pi^2 w_1^2 + x_1^2 v_1^2 + y_1^2 u_1^2$$

$$+ 2(\pi z_1 x_1 u - \pi z_1 y_1 v + \pi w_1 x_1 v + \pi w_1 y_1 u) = \pi \eta.$$  

Hence

$$(u^2 + v^2 + 1)(x_1^2 + y_1^2) + 2(ux_1 z_1 + vx_1 w_1 - vy_1 z_1 + uy_1 w_1)$$

$$+ \pi^2 (z_1^2 + w_1^2) = \pi \eta.$$  

Letting $q = \frac{u^2 + v^2 + 1}{\pi}$, this last equality reduces to (14)

$$q(x_1^2 + y_1^2) + 2(ux_1 z_1 + vx_1 w_1 - vy_1 z_1 + uy_1 w_1) + \pi(z_1^2 + w_1^2) = \eta.$$  

The determinant of this form is $(\pi q - u^2 - v^2)^2$ which, when the value of $q$ is substituted, is seen to be 1. The principal third order minor determinant of this form is $q^2 \pi - u^2 q - v^2 q = q$ which is positive since $q$ is totally positive. Thus the form (14) is positive definite and of determinant 1 and represents integers of odd norm so it is in the same genus as a sum of four squares. Since the form $x^2 + y^2 + z^2 + w^2$ is in a genus of one class [1], (14) must be equivalent to the sum of four squares under an integral transformation of determinant 1. Hence the number of representations of $\eta$ by the form (14) is the same as $r_4(\eta)$. 
If \( \pi \) is a factor of \( \eta \), then the vectors in which each of \( x, y, z, \) and \( w \) is divisible by \( \pi \) have been included in each of the \( n(\pi) + 1 \) spaces. Note that in this case we have

\[
(15) \quad \pi^2 x_2^2 + \pi^2 y_2^2 + \pi^2 z_2^2 + \pi^2 w_2^2 = \pi(\eta_1)
\]

where \( \pi x_2 = x, \ldots, \pi \eta_1 = \eta \), which reduces to

\[
x_2^2 + y_2^2 + z_2^2 + w_2^2 = \eta_1.
\]

Thus we must delete \( n(\pi) r_4(\frac{\eta}{\pi}) \) of the representations in order to count each such representation (15) only once. If \( \pi \) is not a factor of \( \eta \), \( r_4(\frac{\eta}{\pi}) \) is taken to be zero. Hence we have (8).

From (8) we have

\[
r_4(\pi \eta) = (1 + n(\pi))r_4(\eta)
\]

in case \( (\pi, \eta) = 1 \), \( \pi \) is an odd and evenish totally positive prime and \( \eta \) is odd and evenish and totally positive. Assume that for such \( \pi \) and \( \eta \) and \( h \geq 1 \) that

\[
r_4(\pi^h \eta) = [1 + n(\pi) + \ldots + n^h(\pi)]r_4(\eta).
\]

By theorem 1.11

\[
r_4(\pi^{h+1} \eta) = [1 + n(\pi)]r_4(\pi^h \eta) - n(\pi)r_4(\pi^h \frac{\eta}{\pi})
\]

\[
= (1 + n(\pi))(1 + \ldots + n^h(\pi))r_4(\eta)
\]

\[
- n(\pi)(1 + \ldots + n^{h-1}(\pi))r_4(\eta)
\]

\[
= (1 + \ldots + n^{h+1}(\pi))r_4(\eta).
\]

Also \( r_4(1) = 8 \) by inspection.
Thus we have

**Theorem 1.12.** If \( \xi = \pi_1 \cdots \pi_k \) where \( \pi_i \) is an odd, evenish, and totally positive prime in \( \mathbb{Z}(\sqrt{2}) \), then

\[
\text{r}_4(\xi) = 8 \prod_{i=1}^{k} \left( \sum_{j=0}^{h_i} \lfloor \pi_i \rfloor^j \right).
\]
CHAPTER II

CLASS-NUMBERS AND SUMS OF THREE SQUARES

Throughout this chapter we will denote the primitive totally positive binary quadratic form
\[ \Phi = \eta x^2 + 2x_0xy + \xi y^2 \] where \( \xi, x_0, \) and \( \eta \) are in \( \mathbb{Z}(\sqrt{2}) \) by

(1) \[ \Phi = [\eta, 2x_0, \xi]. \]

The determinant \( \delta = \eta \xi - x_0^2 \) we restrict to be totally positive and evenish so that it will be possible for \( \delta \) to be the sum of three squares. \( \eta \) also will be expressible as a sum of squares so it too must be evenish. This in turn implies that \( \xi \) also is evenish. Further, let \( r(\delta) \) be the number of primitive pure quaternions \( x \) of norm \( \delta \). Let \( h(\delta) \) be the number of classes of primitive totally positive binary quadratic forms of determinant \( \delta \).

If \( x = x_1i_1 + x_2i_2 + x_3i_3 \) is a primitive pure quaternion in which \( x_1, x_2, x_3 \) are in \( \mathbb{Z}(\sqrt{2}) \), then by \([x]\) we mean the set of quaternions
\[
x = x_1^1 + x_2^2 + x_3^3
\]
\[
-x_1^1 x_1^1 = x_1^1 x_1^1 - x_2^2 x_2^2 - x_3^3 x_3^3
\]
\[
-x_2^2 x_2^2 = -x_1^1 x_1^1 + x_2^2 x_2^2 - x_3^3 x_3^3
\]
\[
-x_3^3 x_3^3 = -x_1^1 x_1^1 - x_2^2 x_2^2 + x_3^3 x_3^3.
\]

In case \(N(x) = 1\), then for \(x_1 = a_0 + a_1 \sqrt{2}\), \(x_2 = b_0 + b_1 \sqrt{2}\), and \(x_3 = c_0 + c_1 \sqrt{2}\), it follows from \(x_1^2 + x_2^2 + x_3^2 = 1\) that \(a_1 = b_1 = c_1 = 0\). Hence only one \(x_j \neq 0\), say \(x_1\), so that \([x] = \{i, -i\}\). Otherwise there will be four quaternions in \([x]\). To insure this last case we take \(x\) such that \(N(x) \neq 1\).

If \(x\) is a primitive pure quaternion of norm \(\delta \neq 1\) and \(\phi\) is a form as in (1), with determinant \(\delta\), then the quaternion \(v = x_0 + x\) satisfies the condition

\[
N(v) = x_0^2 + N(x) = x_0^2 + \delta = \delta \eta. \quad \text{Since } v \text{ is primitive (see theorem 1.1 or corollary 1.6), if } n(N(\eta)) \text{ is odd, or if } n(N(\eta)) \text{ is even and } n(N(\xi)) \text{ is odd, then } v \text{ has exactly eight right divisors of norm } \eta, \text{ which are of the form } \pm t \text{ or } \pm ij. \text{ Thus we are able to take } v = ut \text{ where } N(u) = \xi \text{ and } N(t) = \eta. \text{ Let } S \text{ be the set of all primitive } [x] \text{ for which } N(x) = \delta. \text{ For each form } \phi \text{ as in (1), we will define a function } F_\phi \text{ from } S \text{ onto } S.
\]
Since \( x = ut - x_0 \), we have \( txt = tut - tx_0 \eta = tu\eta - x_0\eta \). Set
\[
y = \frac{txt}{\eta} = tu - x_0.
\]
Since \( \bar{y} = \frac{tx\bar{t}}{\eta} = -\frac{txt}{\eta} \), \( -y = \bar{y} \) and hence \( y \) is pure. Also \( N(y) = \delta \) so \( [y] \) is in \( S \) if \( y \) is primitive.

Lemma 2.1. \( y \) is primitive.

PROOF: If \( \pi \) is a factor of each component of \( y \), then \( \pi \) is a factor of \( N(y) = \delta \). Also, by (2), \( \eta x = \bar{t}yt \).

Since \( x \) is primitive, if \( \pi \) divides \( y \), then \( \pi \) is a factor of \( \eta \). Now \( \delta = \eta\xi - x_0^2 \), so that \( \pi \) is also a factor of \( x_0 \) and thus a factor of \( y + x_0 = tu \). If \( \pi \) is a divisor of \( t \), then since \( x = ut - x_0 \) we would have \( x \) non-primitive. Hence \( \pi \) is not a divisor of \( t \). Thus if \( \pi \) is a factor of \( tu\bar{u} = tN(u) \) so that \( \pi \) divides \( N(u) = \xi \). Hence \( \pi \) is a factor of \( \xi, x_0 \), and \( \eta \) so that \( \xi \) is not primitive, contrary to assumption.

In (2) if \( t \) is replaced by \(-t\), then
\[
\frac{-tx(-t)}{\eta} = \frac{-tx(-\bar{t})}{\eta} = \frac{txt}{\eta} = y.
\]
Replacing \( t \) by \( i\alpha t \) gives
\[
\frac{t_{\alpha} x \bar{t}_{\alpha}}{\eta} = \frac{i_{\alpha} t x \bar{t} (-i_{\alpha})}{\eta} = \frac{-i_{\alpha} t x \bar{t} i_{\alpha}}{\eta} = -i_{\alpha} y i_{\alpha} \quad \text{which is again in } [y].
\]

Also if \( x \) is replaced by \( x' = -i_{\alpha} x i_{\alpha} \), then
\[
x_{0} + x' = x_{0} - i_{\alpha} x i_{\alpha} = -i_{\alpha} u t i_{\alpha} \quad \text{where } N(ti_{\alpha}) = -\eta.
\]

Thus
\[
y' = (ti_{\alpha})(-i_{\alpha} u) - x_{0} = tu - x_{0} = y \quad \text{and again we get } [y].
\]

Hence the mapping \( F_{\phi} \) from \( S \) into \( S \) which takes \([x]\) onto \([y]\) by (2) is a function.

**Lemma 2.2.** \( F_{\phi} \) is one to one and onto.

**PROOF:** We show that if \( \phi = [\eta, 2x_{0}, \xi] \), and \( \psi = [\eta, -2x_{0}, \xi] \), then \( F_{\psi} = F_{\phi}^{-1} \). Let \( F_{\phi}([x]) = [y] \).

Then \( x_{0} + x = ut \) where \( \frac{t x \bar{t}}{\eta} = y = tu - x_{0} \). Hence \( x_{0} - y = \bar{u}t \)
or \( -x_{0} + y = -\bar{u}t \) so that \( F_{\psi}([y]) = [x] \).

**Lemma 2.3.** If \( \phi = [\eta, 2x_{0}, \xi] \) and \( \psi \) is any one of the three forms \([\xi, -2x_{0}, \eta], [\eta, 2(x_{0} + \mu \eta), (\eta \mu^{2} + 2x_{0} \mu + \xi)]\)
or, for a unit \( \theta \), \([\eta \theta^{2}, 2x_{0}, \xi \theta^{-2}]\), then \( F_{\psi} = F_{\phi} \).

**PROOF:** If \( F_{\phi}([x]) = [y] \), then from \( x_{0} + x = ut \), follows \( (x_{0} + \mu \eta) + x = ut + \mu \eta = (u + \mu \bar{t})t \) so that
\[
y = t(u + \mu \bar{t}) - (x_{0} + \mu \eta) = tu + \mu \eta - x_{0} - \mu \eta = tu - x_{0}.
\]
Hence \( F_{\psi}([x]) = F_{\phi}([x]) \) for \( \psi = [\eta, 2(x_{0} + \mu \eta), \ldots] \).
Now consider $\psi = [\xi, -2x_0, \eta]$. Since $x = ut - x_0$, $\bar{x} = tu - x_0$, and $x = -\bar{x} = -tu + x_0$ which gives $\bar{u}x = u(-tu + x_0)u = -\bar{u}tu + x_0\bar{u} = -\bar{u}tu + x_0\bar{u} = x_0\bar{u}$. But $y = tu - x_0$ implies $-y = \bar{y} = -tu - x_0$ or $\bar{u}x = \xi y$ and thus $y = \frac{\bar{u}x}{\xi}$ so again $F_\psi = F_\xi$.

If $\psi = [\eta\theta^2, 2x_0, \xi\theta^{-2}]$ for a unit $\theta$, again from $x_0 + x = ut$ it follows that $x_0 + x = u\theta^{-1}t$ and

$$\frac{\theta tx\theta t}{\eta\theta^2} = \frac{\theta tx\theta t}{\eta\theta^2} = y \text{ or } F_\psi = F_\xi.$$

**Corollary 2.4.** If $\phi$ and $\psi$ are equivalent forms under integral transformations of determinant one, then $F_\psi = F_\phi$.

**PROOF:** If $\phi$ and $\psi$ are equivalent forms, either can be obtained from the other by a finite number of transformations of the types used in lemma 2.3 to give the equivalent forms.

If $\phi$ is a binary quadratic form, then the class $C$ of forms containing $\phi$ is the set of all forms which can be obtained from $\phi$ by a linear transformation of determinant 1. A class is called primitive if the greatest common divisor of the coefficients in any form in the class is 1. If $\phi = [\eta_1, \xi, \eta_2\gamma]$ and $\psi = [\eta_2, \xi, \eta_1\gamma]$ are two forms in two primitive classes, $C_1$ and $C_2$ respectively, of the same determinant (the classes not necessarily distinct), they are called united forms. The form $\Omega = [\eta_1\eta_2, \xi, \gamma]$ of the same determinant is called the compound of $\phi$ and $\psi$ and the class
$C_3$ containing $\Omega$ is called the **product class under composition**. We write $C_1 C_2 = C_3$.

The following two lemmas appear in [3] where the forms have rational integral coefficients. Since the results and proofs carry over to forms with coefficients in $\mathbb{Z}(\sqrt{2})$ without change, we state the lemmas without proof.

**Lemma 2.5.** For any primitive binary quadratic forms $\phi_1, \ldots, \phi_k$ of the same determinant $\delta$, there can be found integers $\xi, \gamma, \eta_1, \eta_2, \ldots, \eta_k$ such that

$$\phi_i \text{ is equivalent to } [\eta_1 \xi, \gamma \eta_1 \ldots \eta_k / \eta_i] \quad (i = 1, \ldots, k).$$

Furthermore, these integers can be chosen so that $\eta_1, \ldots, \eta_k$ and $2\delta$ are prime in pairs.

**Lemma 2.6.** Let the divisors of the classes $C_1$ and $C_2$ of determinant $\delta$ be assumed coprime. Then for all choices of united forms $\phi$ and $\psi$ in $C_1$ and $C_2$ respectively, the compound of $\phi$ and $\psi$ belongs to a unique class.

It is possible by extending the results in [3] as is done in [4,2.18] to obtain the following lemma. The proof again carries over to $\mathbb{Z}(\sqrt{2})$ without change.

**Lemma 2.7.** The classes of primitive binary quadratic forms of a given determinant $\delta$ constitute an abelian group under composition.
Lemma 2.8. If $C$ and $D$ are primitive totally positive classes of binary quadratic forms of determinant $\delta \neq 1$ and if, for $\phi$ in $C$ and $\psi$ in $D$, $F_\phi([x]) = [y]$ and $F_\psi([y]) = [z]$, then for $\Omega$ in $CD$, the product class under composition, $F_\Omega([x]) = [z]$.

PROOF: By lemmas 2.5 and 2.6 we can choose representative forms $\phi = [\eta, 2x_0, \mu \xi]$ and $\psi = [\mu, 2x_0, \eta \xi]$ in $C$ and $D$ respectively so that $(\eta, \mu) = 1$. Since $F_\phi([x]) = [y]$ and $F_\psi([y]) = [z]$ we have

$$x_0 + x = ut, \quad N(t) = \eta, \quad \frac{tx\tilde{t}}{\eta} = y = tu - x_0,$$

and

$$x_0 + y = vt', \quad N(t') = \mu, \quad \frac{t'yt'}{\mu} = z = t'v - x_0.$$

Therefore $x_0 + y = x_0 + tu - x_0 = vt'$ or $tu = vt'$. Also $\tilde{\phi}tu = \tilde{\psi}vt'$ implies $\eta u = (\tilde{\psi}v)t'$. Letting $w = \tilde{\psi}v$, then $\eta u \tilde{t'} = N(t')w$ so that $\eta$ is a factor of $N(t')w_1$ for $i = 0, 1, 2, 3$. By assumption $(\eta, N(t')) = (\eta, \mu) = 1$ so that $\eta$ divides $w_1$ for each $i$. Hence $w = \eta r$ or $\eta u = (\tilde{\psi}v)t'$ implies $\eta u = \eta rt'$. Thus $u = rt'$ and $x_0 + x = r(t't)$ with

$$N(t't) = \mu \eta$$

and

$$\frac{(t't)x(t't)}{\eta \mu} = \frac{t'}{\eta} \cdot \frac{tx\tilde{t}}{\mu} \cdot \frac{t'}{\eta} = \frac{t'yt'}{\mu} = z.$$
Thus $F_\Omega([x]) = [z]$ where $\Omega = [\eta \mu, 2x_0, \xi]$, the compound of $\eta$ and $\mu$.

If $x = x_1i_1 + x_2i_2 + x_3i_3$ is a pure quaternion, we denote by $T(x)$ the set of all quaternions obtainable from $x$ by permuting the $x_j$ or by changing signs.

**Lemma 2.9.** If $N(v) = 2^r$, then $\frac{\bar{v}v}{N(v)}$ is in $T(y)$.

**Proof:** First we show that if $N(v) = 2^r$, then $v$ is a product of factors of the form $\pm i_\alpha$, $1 + i_\alpha$, or $\sqrt{2} i_\alpha$.

The proof is by induction on $r$.

If $r = 0$, then $v = \pm 1$ or $\pm i_\alpha$ give the only possibilities for $v$ such that $N(v) = 1$. If $r = 1$ we consider $v = x_0 + x_1i_1 + x_2i_2 + x_3i_3$ where $x_0 = a_0 + a_1\sqrt{2}$, $x_1 = b_0 + b_1\sqrt{2}$, $x_2 = c_0 + c_1\sqrt{2}$, and $x_3 = d_0 + d_1\sqrt{2}$ so that

$$N(v) = a_0^2 + b_0^2 + c_0^2 + d_0^2 + 2(a_1^2 + b_1^2 + c_1^2 + d_1^2)$$

$$+ 2\sqrt{2}(a_0a_1 + b_0b_1 + c_0c_1 + d_0d_1).$$

Hence for $N(v) = 2$, clearly the only possibilities are for two of $a_0$, $b_0$, $c_0$, $d_0$ equal to $\pm 1$ and all else zero or one of $a_1$, $b_1$, $c_1$, $d_1$ equal $\pm 1$ and all else zero. Thus $v = 1 + i_\alpha$, $\pm i_\alpha(1 + i_\beta)$, $\sqrt{2} i_\alpha$ or $\pm i_\alpha(\sqrt{2} i_\beta)$.

If $\xi = a_0 + a_1\sqrt{2}$, we note that $\xi^2 = a_0^2 + 2a_1^2 + 2\sqrt{2} a_0a_1$ and $n(\xi) = a_0^2 - 2a_1^2$ so that $\xi^2 \equiv n(x) = a_0^2 \pmod{2}$. 
Hence \( v = x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 \) and

\[
N(v) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 2^{k+1}
\]

imply that either none, two or four of the \( x_a \) have \( n(x_a) \) odd. Grouping the \( x_a \) of such odd norm in pairs we have, for example, in case \( x_0, x_1 \) are of odd norm,

\[
N(v) = 2\left(\frac{x_0 - x_1}{2}\right)^2 + 2\left(\frac{x_0 + x_1}{2}\right)^2 + 2\left(\frac{x_2 - x_3}{2}\right)^2 + 2\left(\frac{x_2 + x_3}{2}\right)^2
\]

\[= 2^{k+1}.
\]

So \( N(v) = 2(N(v')) \) where

\[
v' = \frac{x_0 - x_1}{2} + \frac{x_0 + x_1}{2} i_1 + \frac{x_2 - x_3}{2} i_2 + \frac{x_2 + x_3}{2} i_3
\]

and \( N(v') = 2^k \). Expanding the product

\[
(-i_1)(1 + i_1)v' = (1 - i_1)v'
\]

\[= \left(\frac{x_0 - x_1}{2} + \frac{x_0 + x_1}{2}\right) + \left(\frac{x_0 + x_1}{2} - \frac{x_0 - x_1}{2}\right) i_1
\]

\[+ \left(\frac{x_2 - x_3}{2} + \frac{x_2 + x_3}{2}\right) i_2
\]

\[+ \left(\frac{x_2 + x_3}{2} - \frac{x_2 - x_3}{2}\right) i_3
\]

\[= v
\]
and by the induction assumption $v'$ and hence $v$ is a product of factors of the given form.

By the above, we need to show that the lemma is true only in case $v$ is of the form of one of the three possible factor types. Since $[y]$ is contained in $T(y)$, and $-i_\alpha y_\alpha$ is in $[y]$, then $-i_\alpha y_\alpha$ is in $T(y)$. Also

$$(1 - i_1)y(1 + i_1) = (1 - i_1)(y_1 i_1 + y_2 i_2 + y_3 i_3)(1 + i_1)$$

$$= 2(y_1 i_1 - y_3 i_2 - y_2 i_3),$$

so

$$\frac{(1 + i_1) y (1 + i_1)}{N(1 + i_1)}$$

is in $T(y)$ with a similar result holding for $v = 1 + i_B$. Finally,

$$(-\sqrt{2} i_\alpha) y (\sqrt{2} i_\alpha) = 2(-i_\alpha y_\alpha) = 2y' \text{ for } y' \text{ in } [y].$$

Hence

$$\frac{(-\sqrt{2} i_\alpha) y (\sqrt{2} i_\alpha)}{N(\sqrt{2} i_\alpha)}$$

is in $T(y)$.

Lemma 2.10. If $x$ and $y$ are pure and primitive quaternions and $N(x) = N(y)$, then there exists a primitive quaternion $t$ with $N(t) = \eta$ and $n(\eta)$ an odd rational integer, such that for some $y'$ in $T(y)$, $tx\bar{t} = \eta y'$.

PROOF: From $N(x) = N(y)$ and $x$ and $y$ pure it follows that $xx = y\bar{y} = x(-x) = y(-y)$ and $x^2 = y^2$. Thus

$$(x + y)x = y(x + y)$$

and

$$x + y = y N(x + y).$$
If \( y = -x \), take \( y' = x \) and \( t = 1 \).

If \( x + y \neq 0 \), then let \( x + y = \delta vt \) where \( \delta \) is the divisor of \( x + y \), \( vt \) is primitive, \( N(v) = 2^r \) and \( n(N(t)) = n(\eta) \) is odd. This is possible by theorem 1.1. Thus from (2) we have,

\[
\delta vtx\bar{v}\bar{\omega} = yN(x + y) = y\delta vt\bar{v}\bar{\omega},
\]

\[
vtx\bar{v} = yvt\bar{v} = N(v)N(t)y,
\]

and

\[
\bar{v}vtx\bar{v}\bar{v} = N(v)N(t)\bar{v}yv.
\]

Hence, \( N^2(v)(tx\bar{t}) = N(v)N(t)\bar{v}yv \) or \( tx\bar{t} = N(t)\frac{\bar{v}yv}{N(v)} = \eta y' \)

with \( y' \) in \( T(y) \) by lemma 2.9.

**Lemma 2.11.** If \( x \) is a pure quaternion, \( t \) a primitive quaternion such that \( n(N(t)) \) is odd, and \( tx\bar{t} = N(t)y \), then there is an integer \( a \) such that \( a + x = ut \).

**PROOF:** From \( tx\bar{t} = N(t)y \) we have \( txN(t) = N(t)yt \) so that \( tx = yt \). Let \( z = tx = yt \). Then \( z\bar{t} = yN(t) \equiv 0 \pmod{\pi^r} \) for each \( \pi^r \) such that \( \pi \) is prime and \( r \) is the highest power of \( \pi \) for which \( \pi^r \) is a factor of \( N(t) \). Similarly

\( \bar{t}z = N(t)x \equiv 0 \pmod{\pi^r} \) with \( r \) as before. Expanding \( z\bar{t} \) and \( \bar{t}z \) gives

\[
\begin{align*}
z_0t_0 + z_1t_1 + z_2t_2 + z_3t_3 &= 0 \\
(z_0t_1 - z_1t_0) + (z_2t_3 - z_3t_2) &= 0 \quad \pmod{\pi^r} \\
(z_0t_2 - z_2t_0) + (z_3t_1 - z_1t_3) &= 0 \\
(z_0t_3 - z_3t_0) + (z_1t_2 - z_2t_1) &= 0
\end{align*}
\]
and

\[
\begin{align*}
&z_0 + z_1 + z_2 + z_3 = 0 \\
&(z_0 - z_1) - (z_2 - z_3) = 0 \\
&(z_0 - z_2) - (z_3 - z_1) = 0 \\
&(z_0 - z_3) - (z_1 - z_2) = 0
\end{align*}
\]

(5)

Adding and subtracting congruences in (4) and (5) gives

\[
\begin{align*}
2(z_0 - z_1) &= 0 \\
2(z_0 - z_2) &= 0 \\
2(z_0 - z_3) &= 0
\end{align*}
\]

Since \(n(\pi)\) is odd, \(n(\pi^r)\) is odd and 2 can be deleted throughout. Thus \(z_i - z_j = 0 (mod \pi^r)\) for \(i, j = 0, 1, 2, 3\).

Since \(t\) is primitive, there is some \(t_1\), say \(t_1\), such that \((t_1, \pi) = 1\). Therefore

\[
\begin{align*}
z_0 &= (t_1^{-1}z_1)t_0 \\
z_1 &= (t_1^{-1}z_1)t_1 \\
z_2 &= (t_1^{-1}z_1)t_2 \\
z_3 &= (t_1^{-1}z_1)t_3
\end{align*}
\]

(mod \(\pi^r\)).

This can be done for each prime \(\pi\) dividing \(N(t)\), so by the Chinese Remainder Theorem, there is a constant \(a\) such that \(z_i = at_i (mod N(t))\) or \(z = at (mod N(t))\) so that
tx = at(mod N(t)). Thus \((a + x)\overline{t} = at + xt = at - xt\)
where \(at - xt = \overline{xt} - \overline{xt} = 0 (mod N(t))\). That is, \((a + x)\overline{t} = N(t)u\) or \(a + x = ut\).

**Lemma 2.12.** If \(\Phi = [\eta, \mu, \xi]\) is a primitive binary quadratic form, then \(\Phi\) represents a prime integer.

See [8] for a proof of this lemma for forms with rational integral coefficients.

**Lemma 2.13.** If \(x\) and \(y\) are primitive pure quaternions of norm \(\delta \neq 1\) and \(\Phi\) and \(\Psi\) are primitive totally positive binary quadratic forms of determinant \(\delta\) such that \(F_\Phi([x]) = [y]\) and \(F_\Psi([x]) = [y]\), then \(\Phi\) is equivalent to \(\Psi\).

**PROOF:** Suppose \(C\) and \(D\) are the primitive classes of forms which contain \(\Phi\) and \(\Psi\) respectively. Then \(CD^{-1}\) and the principal class \(E\) both contain forms whose associated functions, \(F\), map \([x]\) onto \([x]\). If, however, \(tx\overline{t} = N(t)x\), then \(tx = xt\) implies \(x_2t_3 = x_3t_2\), \(x_3t_1 = x_1t_3\), and \(x_1t_2 = x_2t_1\).

If \(\pi^r\) divides \(x_2\), then \(\pi^r\) divides \(x_3t_2\) and \(x_1t_2\), but \(x\) is primitive so \(\pi\) is not a factor of \(x_1\) and \(x_3\) and hence \(\pi^r\) divides \(t_2\). Thus \(x_2\) is a factor of \(t_2\) and it follows from \(t_3 = x_3 \frac{t_2}{x_2}, t_1 = x_1 \frac{t_2}{x_2}, \) and \(t_2 = x_2 \frac{t_2}{x_2}\) that \(t_i = x_i \alpha\) for \(i = 1, 2, 3\) for some integer \(\alpha\). Thus

\[
(6) \quad N(t) = t_0^2 + N(x)\alpha^2 = t_0^2 + \delta\alpha^2.
\]
By corollary 2.4, any two equivalent forms have the same associated function. If \( \Omega \) is a form in \( CD^{-1} \) and \( \Omega \) represents \( \eta \) primitively, there is an equivalent form, \( \Omega' \), with \( \eta \) as the first coefficient and a corresponding quaternion \( t \) such that \( N(t) = \eta \) and \( txt' = \eta x \). But by (6), \( N(t) = t_0^2 + \delta a^2 \).

Hence the form \( x^2 + \delta y^2 \) represents every integer represented primitively by \( \Omega \).

By lemma 2.9, \( \Omega \) represents a prime \( \pi \). Let \( [\pi, 2\beta, \gamma] \) be equivalent to \( \Omega \) where \( 2\beta \) is reduced so that \( \beta \) is in a reduced residue system \((\text{mod } \pi)\). \([1, 0, \delta]\) also represents \( \pi \) so that it is equivalent to a form \([\pi, 2\rho, \gamma']\) where \( 2\rho \) is also reduced \((\text{mod } \pi)\). But \( \delta = \pi \gamma - \beta^2 = \pi \gamma' - \rho^2 \) implies \( \beta^2 \equiv \delta \equiv \rho^2 \) \((\text{mod } \pi)\) so that \( \beta \equiv \pm \rho \) \((\text{mod } \pi)\). Since \([1, 0, \delta]\) is improperly equivalent to itself, if one of \([\pi, 2\rho, \gamma']\) or \([\pi, -2\rho, \gamma']\) is equivalent to \([1, 0, \delta]\), so is the other. Hence \( \beta \equiv \pm \rho \) \((\text{mod } \pi)\) implies \( \beta = \pm \rho \) so that \([\pi, 2\beta, \gamma]\) is equivalent to \([1, 0, \delta]\) and \( CD^{-1} = E \) or \( C = D \) and thus \( \psi \) is equivalent to \( \psi \).

We note that without using lemma 2.9 it can be shown by the theory of reduction as developed in [7] that if two totally positive forms represent primitively the same integers, then the forms are properly or improperly equivalent.
Lemma 2.14. Let the quaternion $x'$ be obtained from a pure quaternion $x = x_1i_1 + x_2i_2 + x_3i_3$ by $r$ sign changes and $s$ permutations of $x_1, x_2, x_3$. Then a primitive quaternion $t$ with $n(N(t))$ odd and such that $tx' = N(t)x'$ exists if and only if

1) $x' \equiv x \pmod{2}$

and

2) $r$ is even if $1 = n(x_1) = n(x_2) = n(x_3) \pmod{2}$.

PROOF: To show the necessity of 1) and 2), consider the following expansion.

$$tx' = x_1(t_0^2 + t_1^2 - t_2^2 - t_3^2)i_1 + x_2[t_0^2 - t_1^2 + t_2^2 - t_3^2]i_2$$
$$+ x_3(t_0^2 - t_1^2 - t_2^2 + t_3^2)i_3 + 2[(x_2t_1t_2 + x_3t_1t_3 - x_2t_0t_3$$
$$+ x_3t_1t_2)i_1 + (x_1t_1t_2 + x_3t_2t_3 - x_3t_0t_1 + x_1t_0t_3)i_2$$
$$+ (x_2t_0t_1 - x_1t_0t_2 + x_1t_1t_3 + x_2t_2t_3)i_3].$$

If $t_0 = u_0 + u_1\sqrt{2}$, $t_1 = v_0 + v_1\sqrt{2}$, $t_2 = r_0 + r_1\sqrt{2}$, and $t_3 = s_0 + s_1\sqrt{2}$, then $N(t) \equiv u_0^2 + v_0^2 + r_0^2 + s_0^2 \pmod{2}$.

Letting $z = u_0^2 + v_0^2 + r_0^2 + s_0^2$ we see the parity of $z$ would not be changed by changing two signs in $z$. Thus we have $tx' \equiv N(t)x \pmod{2}$. But since $tx' = N(t)x'$, then $N(t)x \equiv N(t)x' \pmod{2}$ or $x \equiv x' \pmod{2}$ and 1) holds.
Suppose \( n(N(t)) \) is odd, \( 1 = n(x_1) = n(x_2) = n(x_3) \) (mod 2), and \( x' = -x \) (i.e. \( r = 3 \)). Then \( txt = N(t)x' \) implies \( txt = -N(t)x \) or \( tx = -xt \). But expanding \( tx = -xt \) implies

\[-x_1t_1 - x_2t_2 - x_3t_3 = x_1t_1 + x_2t_2 + x_3t_3 \text{ or} \]

(7) \[x_1t_1 + x_2t_2 + x_3t_3 = 0.\]

Also from the expansion we get

\[t_0x_1 + t_2x_2 - t_3x_3 = t_0x_1 - t_3x_2 + t_2x_3 \text{ or } t_0x_1 = 0.\]

Similarly \( t_0x_2 = t_0x_3 = 0. \) But \( x \neq 0 \) and the last equalities imply \( t_0 = 0. \) Letting

\[x_1 = a_0 + a_1\sqrt{2}, \quad x_2 = b_0 + b_1\sqrt{2}, \quad x_3 = c_0 + c_1\sqrt{2}\]

(8)

\[t_1 = v_0 + v_1\sqrt{2}, \quad t_2 = r_0 + r_1\sqrt{2}, \quad t_3 = s_0 + s_1\sqrt{2}\]

and expanding (7) gives

\[a_0v_0 + b_0r_0 + c_0s_0 + 2(a_1v_1 + b_1r_1 + c_1s_1) + \sqrt{2}(a_0v_1 + \ldots) = 0\]

or

\[a_0v_0 + b_0r_0 + c_0s_0 + 2(a_1v_1 + b_1r_1 + c_1s_1) = 0 \text{ so that} \]

\[a_0v_0 + b_0r_0 + c_0s_0 \text{ is even. Since } n(x_1) \text{ is odd, } a_0, b_0, \]

and \( c_0 \) are odd and hence either none or two of \( v_0, r_0, \) and \( s_0 \) are odd. If two, say \( v_0, r_0, \) are odd, then with \( t_0 = 0, \)
$t_0^2 + v_0^2 + r_0^2 + s_0^2$ is even so that $n(N(t))$ is even. If all of $v_0$, $r_0$, and $s_0$ are even and $t_0 = 0$, then again $n(N(t))$ is even, a contradiction in both cases.

If $r = 1$ and $n(x_1) = n(x_2) = n(x_3) = 1$ (mod 2), then suppose $x' = -x_1i_1 + x_2i_2 + x_3i_3$ or $x' = x - 2x_1i_1$.

Expanding $tx = x't'$ as before and equating coefficients of $i_j$ yields

$$(9) \quad x_1t_1 = 0, \ t_0x_1 + t_2x_3 - t_3x_2 = 0, \ t_1x_3 = 0, \ t_1x_2 = 0.$$  

Again, with $x \neq 0$, then $t_1 = 0$. Using $(8)$ again with $(9)$ gives

$$a_0v_0 + c_0r_0 - b_0s_0 + 2(a_1v_1 + c_1r_1 - b_1s_1) + \sqrt{2(a_0v_1 + \ldots)} = 0$$

with $a_0$, $b_0$, $c_0$ all odd. But this last equality implies

$$a_0v_0 + c_0r_0 - b_0s_0$$

is even. Hence either two or none of $v_0$, $r_0$, $s_0$ are odd, and in either case $v_0^2 + r_0^2 + s_0^2$ is even so that $n(N(t))$ is even contrary to our assumption. Thus ii) holds.

To show the sufficiency of i) and ii) suppose first that $x'$ is derived from $x$ by sign changes alone.

For $x'$ differing from $x$ by two signs, we note $x'$ is in $[x]$ so that $-i_jx_i_j = x'$. If $x'$ differs from $x$ by exactly one or three signs, it is sufficient to exhibit a $t$ such that
\[ tx^t = N(t)(-x), \]
for then this can be followed by the previous transformation \(-i_j(tx^t)i_j\) to give the desired result. Since \( r \) is even if \( n(x_1) = n(x_2) = n(x_3) = 1 \pmod{2} \)
we need only consider \( n(x_k) \) even for exactly one or two of \( k = 1, 2, 3 \).

To obtain such a \( t \) with \( n(N(t)) \) odd we use either \( x_2i_3 - x_3i_2 = t \) or \( x_3i_1 - x_1i_3 = t \), whichever one satisfies \( x_2^2 + x_3^2 \) is odd, or \( x_3^2 + x_1^2 \) is odd. Expanding \( tx^t = N(t)(-x) \) yields the desired relation, for example

\[
(x_2i_3 - x_3i_2) x (-x_2i_3 + x_3i_2) = (x_2^2 + x_3^2)(-x).
\]

In order to show the existence of a quaternion \( t \) with \( n(N(t)) \) odd in case \( x' \) is derived from \( x \) by an interchange of \( x_i \)'s we note first that 1) implies that if \( x_j \) and \( x_k \) are interchanged we must have \( x_j = x_k \pmod{2} \).

In this case of \( x' = x_ji_k + x_ki_j + x_mi_m \) we will choose

\[
t = \frac{(x_j + x_k)(i_j + i_k)}{2} + x_mi_m.
\]

For clarity suppose \( j = 1, k = 2 \) so that

\[
t = \frac{(x_1 + x_2)(i_1 + i_2)}{2} + x_3i_3.
\]

Expansion of \( tx^t \) gives \( N(t)(x_2i_1 + x_1i_2 + x_3i_3) \) as desired.
We still must show that \( n(N(t)) \) is odd.

If \( x_j \) is as in (8), then

\[
N(t) = \frac{a_0^2 + b_0^2}{2} + a_1^2 + b_1^2 + a_0 b_0 + 2a_1 b_1 + c_0^2 + 2c_1^2 + \sqrt{2}(a_0 a_1 + \ldots).
\]

Now \( n(N(t)) \) is odd unless

\[
z = \frac{a_0^2 + b_0^2}{2} + a_1^2 + b_1^2 + a_0 b_0 + 2a_1 b_1 + c_0^2 + 2c_1^2 \equiv 0 \pmod{2}.
\]

Since \( x_1 = x_2 \pmod{2} \), then \( a_0 = b_0 \) and \( a_1 = b_1 \pmod{2} \).

If it should happen that \( z \) is even then we have three possible cases for \( a_0, b_0, \) and \( c_0 \).

Case 1. \( a_0, b_0 \) even and \( c_0 \) odd which, with \( z \) even, implies \( a_1^2 + b_1^2 + c_0^2 \) is even so \( a_1 \neq b_1 \pmod{2} \).

Case 2. \( a_0, b_0 \) odd and \( c_0 \) odd imply that

\[
a_0^2 = 4n + 1, \quad b_0^2 = 4m + 1, \quad c_0^2 = 4p + 1
\]

so that

\[
z = [2(n + m) + 4p + 2] + 2a_1 b_1 + a_1^2 + b_1^2 + a_0 b_0. \quad \text{Hence}
\]

\( a_1^2 + b_1^2 + a_0 b_0 \) is even and \( a_1 \neq b_1 \pmod{2} \).

Case 3. \( a_0, b_0 \) odd and \( c_0 \) even imply

\[
z = 2(m + n) + 1 + a_1^2 + b_1^2 + a_0 b_0 + c_0^2 + 2c_1^2 \text{ is even, or}
\]

\( 1 + a_1^2 + b_1^2 + a_0 b_0 \) is even so that \( a_1 = b_1 \pmod{2} \).
Cases 1 and 2 contradict \( x_1 \equiv x_2 \pmod{2} \) so
\( n(N(t)) \) is odd unless

\[ (10) \quad a_0 \equiv b_0 \equiv 1, \quad c_0 \equiv 0, \quad a_1 \equiv b_1 \pmod{2}. \]

If (10) holds, we choose

\[ t = -\frac{x_1 + x_2}{2} - \frac{x_1 - x_2}{2} i_3. \]

Then
\[
txt = \left(\frac{x_1 x_3 - x_2 x_3}{2} - \frac{x_1^2 + x_2^2}{2} i_1 - \frac{x_1^2 + x_2^2}{2} i_2 \right)
\]
\[
- \frac{x_1 x_3 + x_2 x_3}{2} i_3 \right) \left( -\frac{x_1 + x_2}{2} + \frac{x_1 - x_2}{2} i_3 \right)
\]
\[= \frac{x_2^2 + x_1 x_2}{2} i_1 + \frac{x_2^2 + x_1 x_2}{2} i_2 + \frac{x_1 x_3 + x_2 x_3}{2} i_3
\]
\[= \left(\frac{x_2^2 + x_1^2}{2}\right) (x_2 i_1 + x_1 i_2 + x_3 i_3) = N(t)x' \text{ as desired.}
\]

For this choice of \( t \) and with the conditions \( a_0 \equiv b_0 \equiv 1 \pmod{2} \) and \( a_1 \equiv b_1 \pmod{2} \), the parity of

\[ N(t) = \frac{a_0^2 + b_0^2 + 2(a_1^2 + b_1^2) + 2(a_0 a_1 + b_0 b_1)}{2} \]

is determined by \( \frac{a_0^2 + b_0^2}{2} \). But \( a_0 = 4n + 1 \) and \( b_0 = 4m + 1 \)
\[ \frac{a_0^2 + b_0^2}{2} = 8(n^2 + m^2) + 4(n \pm m) + 1 \] so that \( n(N(t)) \) is odd.

Thus under the restriction \( x_1 \equiv x_2 \pmod{2} \) we can find a quaternion \( t \) such that \( n(N(t)) \) is odd and \( tx^t = N(t)x' \). If \( t \) is not primitive, we obtain a primitive one merely by removing the common factor. The cases \( x_1 \equiv x_3 \) and \( x_2 \equiv x_3 \pmod{2} \) are handled similarly.

If \( x \) is a pure quaternion and there is a primitive quaternion \( t \) with \( n(N(t)) \) odd and such that \( tx^t = N(t)x' \), we say that \( x \) can be transformed into \( x' \). We note, here, that there are forty-eight quaternions in \( T(x) \).

**Corollary 2.15.** If \( x = x_1i_1 + x_2i_2 + x_3i_3 \) is a primitive pure quaternion, then

1) if \( n(x_1) \equiv n(x_2) \equiv n(x_3) \pmod{2} \) fails and exactly two of \( x_1, x_2, \) and \( x_3 \) are congruent \( \pmod{2} \), then \( x \) can be transformed into one third of the quaternions in \( T(x) \).

ii) if \( n(x_1) \equiv n(x_2) \equiv n(x_3) \pmod{2} \) fails and no two of \( x_1, x_2, \) and \( x_3 \) are congruent \( \pmod{2} \), then \( x \) can be transformed into one sixth of the quaternions in \( T(x) \).

iii) if \( n(x_1) \equiv n(x_2) \equiv n(x_3) \equiv 1 \pmod{2} \) and \( x_1 \equiv x_2 \equiv x_3 \pmod{2} \), then \( x \) can be transformed into
one half of the quaternions in $T(x)$.

iv) if $n(x_1) = n(x_2) = n(x_3) \equiv 1 \pmod{2}$ and exactly two of $x_1, x_2, \text{ and } x_3$ are congruent $\pmod{2}$, then $x$ can be transformed into one sixth of the quaternions in $T(x)$.

**PROOF:** We note first that since $x$ is primitive, $n(x_1) = n(x_2) = n(x_3) \equiv 0 \pmod{2}$ cannot hold.

Suppose $n(x_1) = n(x_2) = n(x_3) \pmod{2}$ fails, say $n(x_1) = n(x_2) \neq n(x_3) \pmod{2}$. Then $x_1 \neq x_3$ and $x_2 \neq x_3 \pmod{2}$. Letting $x_1, x_2,$ and $x_3$ be as in (8), then $a_0 = b_0 \neq c_0 \pmod{2}$ and either

i) $a_1 \equiv b_1 \pmod{2}$ so that $x_1 \equiv x_2 \pmod{2}$

or

ii) $a_1 \not\equiv b_1 \pmod{2}$ and $x_1 \not\equiv x_2 \pmod{2}$.

In case i) holds, by lemma 2.14, the only quaternions $x'$ into which $x$ can be transformed are $x' = \pm x_1i_1 \pm x_2i_2 \pm x_3i_3$ or $x' = \pm x_2i_1 \pm x_1i_2 \pm x_3i_3$. This is a total of sixteen possibilities or one third of the quaternions in $T(x)$. If ii) holds, by lemma 2.14, the only $x'$ into which $x$ can be transformed are

$x' = \pm x_1i_1 \pm x_2i_2 \pm x_3i_3$, a total of eight quaternions or one sixth of the quaternions in $T(x)$. 
If \( n(x_1) = n(x_2) = n(x_3) = 1 \pmod{2} \), then
\[
a_0 = b_0 = c_0 = 1 \pmod{2}
\]
and either

iii) \( x_1 = x_2 = x_3 \pmod{2} \)

or

iv) exactly two of \( x_1, x_2, \) and \( x_3 \) are congruent \( \pmod{2} \).

In case iii), lemma 2.14 implies any quaternion in \( T(x) \) that can be obtained from \( x \) by any permutation of the \( x_j \) and any even number of sign changes is a possible transform of \( x \), hence one half of the quaternions in \( T(x) \) are transforms of \( x \). In the last case iv), suppose

\( x_1 = x_2 \pmod{2} \). Then as in i) the possibilities for \( x' \)

according to lemma 2.14 are \( \pm x_1 i_1 \pm x_2 i_2 \pm x_3 i_3 \) or

\( \pm x_2 i_1 \pm x_1 i_2 \pm x_3 i_3 \) but only an even number of sign changes are possible so there are eight possibilities for \( x' \) or one sixth the number of quaternions in \( T(x) \).

If \( x \) and \( y \) are two primitive pure quaternions such that \( N(x) = N(y) = \delta \neq 1 \), by lemmas 2.10 and 2.11 there is a \( y' \) in \( T(y) \) such that for a class, \( C \), of primitive totally positive binary quadratic forms of determinant \( \delta \), \([x]\) is mapped onto \([y']\) under the associated functions, \( F \), of \( C \). Lemma 2.13 shows the uniqueness of the class \( C \). By corollary 2.15, \( y' \) can be transformed into \( \frac{1}{k} \) of the quaternions in \( T(y') \) where \( k \) depends on the case in the
corollary into which \( y' \) falls. Hence \([y']\) can be mapped onto \( \frac{1}{k} \) of the sets \([y'']\) contained in \( T(y') \). As before, for each such mapping there exists a unique class of associated forms, \( D \), so the number of classes \( D \) is \( \frac{1}{k} \) times the number of sets \([y'']\) contained in \( T(y') \). Since every class of forms whose associated function maps \([x]\) into the sets \([y'']\) in \( T(y) \) can be expressed uniquely as \( CD \), the number of such classes is the same as the number of classes, \( D \), and hence is \( \frac{1}{k} \) times the number of sets \([y'']\) in \( T(y') \).

Let \( r_\alpha(\delta) \), for \( \alpha = i, ii, iii, iv \), be the number of primitive pure quaternions, \( x \), with \( N(x) = \delta \) which satisfy the congruence conditions in case \( \alpha \) of corollary 2.15. A consideration of all possible arrangements \( a_1, a_2, b_0, b_1, c_0, c_1 \) subject to the conditions for each case in the corollary and a subsequent comparison of the corresponding values of \( N(x) \) reduced modulo 8 shows that if \( \delta \) is the norm of a pure and primitive quaternion, then it can be the norm of two different such quaternions \( x \) and \( y \) which satisfy the conditions of two different cases only if they are the cases \( ii \) and \( iii \) or the cases \( ii \) and \( iv \). Otherwise the cases are disjoint.

The number of quaternions in \( T(y) \) is four times the number of sets \([y']\) with \( y' \) in \( T(y) \). Letting \( k(i) \) be the integer given in case \( i \) of corollary 2.15 and \( h(\delta) \)
the number of classes of primitive totally positive binary quadratic forms of determinant $\delta$, from the second paragraph above we have

$$h(\delta) = \frac{1}{3.4} r_1(\delta) + \frac{1}{6.4} r_{ii}(\delta) + \frac{1}{2.4} r_{iii}(\delta) + \frac{1}{6.4} r_{iv}(\delta),$$

where $r_\alpha(\delta) = 0$ if no quaternion satisfying the conditions of case $\alpha$ has norm $\delta$.

Thus we have shown:

**Theorem 2.16.** The number of classes of primitive totally positive binary quadratic forms of determinant $\delta$ where $\delta$ is odd, evenish, totally positive and $\not\equiv 1$ is given by

$$h(\delta) = \frac{1}{12} r_1(\delta) + \frac{1}{24} r_{ii}(\delta) + \frac{1}{8} r_{iii}(\delta) + \frac{1}{24} r_{iv}(\delta)$$

where $r_\alpha(\delta)$ is the number of primitive pure quaternions, $x = x_1^{i_1} + x_2^{i_2} + x_3^{i_3}$, of norm $\delta$ satisfying the following conditions for $\alpha = i, ii, iii, iv$.

1) $n(x_1) \equiv n(x_2) \equiv n(x_3)$ fails and exactly two of $x_1, x_2, x_3$ are congruent,

2) $n(x_1) = n(x_2) = n(x_3)$ fails and no two of $x_1, x_2, x_3$ are congruent,

3) $n(x_1) = n(x_2) = n(x_3) \equiv 1$ and $x_1 \equiv x_2 \equiv x_3$,

4) $n(x_1) = n(x_2) = n(x_3) \equiv 1$ and exactly two of $x_1, x_2, x_3$ are congruent where all congruences are modulo two.
Using the above results we are able to obtain
relations between the representations of \( \eta \) and \( \pi^2\eta \)
as a sum of three squares.

**Lemma 2.17.** If \( y \) is a primitive pure quaternion
with \( N(y) = \pi^2\eta \) where \( \pi \) is an odd evenish and totally positive
prime and \( \eta \) is odd evenish and totally positive, then there
are quaternions \( t, x \) such that \( N(t) = \pi, \ N(x) = \eta \) and
\( y = \overline{t}xt \). \( t \) is unique to within multiplication by
\( \theta = \pm 1, \ \pm ij \), and \( x \) may be replaced only by \( \theta x \theta \). Further, every
primitive set \([y]\) of norm \( \pi^2\eta \) is obtained in this manner
from an unique primitive set \([x]\) of norm \( \eta \).

**PROOF:** By theorem 1.1, \( y = vt \) with \( N(t) = \pi \)
and \( t \) is in an unique set of eight quaternions \( \pm t, \pm ij\).
But \( \pi \) divides \( N(v) \) so \( y \) and \( v \) have the same left divisors
of norm \( \pi \). Since
\( y = -\overline{y} = \overline{tv}, \) then \( v = \overline{tx} \) or \( y = \overline{txt} \).
The uniqueness of \( t \) to within \( \theta t \) implies \( x \) is unique except
for replacement by \( \theta x \theta \). From
\[-ijytj = ijt\overline{txtij} = \overline{ij} \overline{txtij} = (\overline{tij})x(tij) \]
we have
\([y]\) is obtained from an unique \([x]\).

By theorem 1.12 there are \( 8(n(\pi) + 1) \)
representations of \( \pi \) as a sum of four squares. Hence there
exist \( 8(n(\pi) + 1) \) primitive quaternions \( t \) of norm \( \pi \),
that is \( n(\pi) + 1 \) sets of the form \( \pm t, \pm ij \). Thus for
each of these \( n(\pi) + 1 \) sets and a primitive set \([x]\) we
have a primitive $y$ such that $y = \mathfrak{t} x t$ except in the case of those sets of $t$ for which $\mathfrak{t} x t \equiv 0 \pmod{\pi}$. By lemma 2.11, if $t$ is primitive, $N(t) = \pi$, $N(x) = \eta$, and $\mathfrak{t} x t = \pi z$, then there is an integer $a$ such that $a + x = \pi t$. Hence $a^2 + \eta \equiv 0 \pmod{\pi}$.

Thus $\mathfrak{t} x t \equiv 0 \pmod{\pi}$ if and only if $(\frac{-\eta}{\pi}) = 1$. If $(\frac{-\eta}{\pi}) = 1$, then $\mathfrak{t} x t \equiv 0 \pmod{\pi}$ and $\mathfrak{t} x \mathfrak{t} \equiv 0 \pmod{\pi}$ so there are $1 + (\frac{-\eta}{\pi})$ sets $\pm t, \pm i_j t$ with $\mathfrak{t} x \mathfrak{t} \equiv 0 \pmod{\pi}$. Hence there are

$$n(\pi) + 1 - (1 + (\frac{-\eta}{\pi})) = n(\pi) - (\frac{-\eta}{\pi})$$

sets $[y]$ with $n(y) = \pi^2 \eta$ derived from $[x]$ with $n(x) = \eta$. For $t, t'$ in different sets, then $\mathfrak{t} x \mathfrak{t}, t' x t'^{-1}$ are in different $[y]$ by lemma 2.17. Thus

$$r(\pi^2 \eta) = [n(\pi) - (\frac{-\eta}{\pi})] r(\eta).$$

The above argument holds with primitive replaced by primitive $(\mod \pi)$ so we can write

$$r_{\pi}(\pi^2 \eta) = [n(\pi) - (\frac{-\eta}{\pi})] r_{\pi}(\eta)$$

where $r_{\pi}(\eta)$ is the number of representations of $\eta$ as a sum of three squares not all divisible by $\pi$. Hence if $r_3(\eta)$ is the number of all representations of $\eta$ as a sum of three squares, we have

$$r_3(\pi^2 \eta) = r_3(\eta) + r_{\pi}(\pi^2 \eta) = r_3(\eta) + [n(\pi) - (\frac{-\eta}{\pi})] r_{\pi}(\eta)$$

$$= r_3(\eta) + [n(\pi) - (\frac{-\eta}{\pi})][r_3(\eta) - r_3(\pi^2 \eta)].$$
Therefore

\[(12) \quad r_3(\eta^{2}) = [1 + n(\pi) - \left(\frac{n}{\pi}\right)] r_3(\eta) - [n(\pi) - \left(\frac{n}{\pi}\right)] r_3(\eta^{2}).\]

Suppose now that \((\eta, \pi^2) = 1\) or \(\pi\) and for some \(k \geq 1\) that

\[r_3(\eta^{2k}) = r_3(\eta)[\frac{n(\pi)^{k+1}}{n(\pi)} - 1 - \left(\frac{n}{\pi}\right) \frac{n(\pi)^{k}}{n(\pi)} - 1].\]

Then from (12) it follows that

\[r_3(\eta^{2k+2}) = [1 + n(\pi) - \left(\frac{n}{\pi}\right)] r_3(\eta^{2k})\]

\[-[n(\pi) - \left(\frac{n}{\pi}\right)] r_3(\eta^{2k})\]

where \(k > 0\) implies \(\frac{n}{\pi^{2k}} = 0\). Thus

\[r_3(\eta^{2k+2}) = r_3(\eta)[1 + n(\pi)][\frac{n(\pi)^{k+1}}{n(\pi)} - 1 - \left(\frac{n}{\pi}\right) \frac{n(\pi)^{k}}{n(\pi)} - 1] \]

\[- n(\pi)[r_3(\eta)[\frac{n(\pi)^{k}}{n(\pi)} - 1 - \left(\frac{n}{\pi}\right) \frac{n(\pi)^{k-1}}{n(\pi)} - 1]]\]

\[= r_3(\eta)[\frac{n(\pi)^{k+2}}{n(\pi)} - 1 - \left(\frac{n}{\pi}\right) \frac{n(\pi)^{k+1}}{n(\pi)} - 1].\]

Hence by induction we have

**Theorem 2.18.** If \(\mathfrak{g} = \pi_1^{k_1} \pi_2^{k_2} \cdots \pi_m^{k_m}\) where \(\pi_i\) is an odd evenish totally positive prime with \((\pi_i, \pi_j) = 1\) for \(i \neq j\) and \(\eta\) is an odd evenish totally positive square
free integer, then

\[ r_3(g^2 \eta) = r_3(\eta) \prod_{i=1}^{m} T_i \]

where

\[ T_i = \frac{n(\pi_1)_{k_i+2}}{n(\pi_1)_{k_i+1}} - \frac{m \cdot n(\pi_1)_{k_i+1}}{\pi_1 n(\pi_1)_{k_i+1}}. \]
SELECTED BIBLIOGRAPHY


4. _____, Integral Quadratic Forms (To appear).


6. _____, On Sums of Squares (To appear).

7. Pall, G. and Whyburn C. 'Reduction of Totally Positive Binary Quadratic Forms with Coefficients in a Quadratic Ring,' (To appear).

VITA

George Warthen Lofquist was born on October 6, 1930, in Brookhaven, Mississippi. He attended the public schools in that community; Richmond, Virginia; and Asheville, North Carolina. Upon graduation from high school he entered the University of North Carolina from which he received the degree of Bachelor of Science in Mathematics in 1952. He subsequently received the degree of Master of Education from the same institution in 1959. In 1963 he was granted the degree of Master of Science at Louisiana State University. At the present time he is a candidate for the degree of Doctor of Philosophy in the Department of Mathematics.
EXAMINATION AND THESIS REPORT

Candidate: George Warthen Lofquist

Major Field: Mathematics

Title of Thesis: Class Numbers and Sums of Squares in a Quadratic Field

Approved:

[Signatures of Major Professor and Chairman, Dean of the Graduate School, and EXAMINING COMMITTEE members]

Date of Examination: July 18, 1967