1969

Representations of Discriminantal Divisors by Binary Quadratic Forms.

Ezra Allan Brown

Louisiana State University and Agricultural & Mechanical College

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

Recommended Citation

https://digitalcommons.lsu.edu/gradschool_disstheses/1641

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
BROWN, Ezra Allan, 1944-
REPRESENTATIONS OF DISCRIMINANTAL
DIVISORS BY BINARY QUADRATIC FORMS.

The Louisiana State University and Agricultural
and Mechanical College, Ph.D., 1969
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan
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

Ezra Allan Brown
B.A., Rice University, 1965
M.S., Louisiana State University, 1967
August, 1969
ACKNOWLEDGMENT

I would like to express my appreciation to Professor Gordon Pall, under whose direction this dissertation was written, for his advice and encouragement.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</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>CHAPTER I</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER II</td>
<td>35</td>
</tr>
<tr>
<td>CHAPTER III</td>
<td>57</td>
</tr>
<tr>
<td>CHAPTER IV</td>
<td>69</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>79</td>
</tr>
<tr>
<td>AUTOBIOGRAPHY</td>
<td>80</td>
</tr>
</tbody>
</table>
ABSTRACT

An ancipital form is a binary quadratic form \([a, b, c]\) for which \(b = a\) or \(b = 0\). The set of leading coefficients of the primitive ancipital forms of discriminant \(d\) is called the set of discriminantal divisors of \(d\). The principal form of discriminant \(d\) is the form \(f_1 = [1, \epsilon, (\epsilon^2 - d)/4]\), where \(\epsilon = 0\) or \(1\) according as \(d\) is even or odd. The following question is asked: given a discriminant \(d\), which discriminantal divisors of \(d\) are represented by \(f_1\)?

In Chapter I, the question is discussed in detail in the cases \(d = 5p\) and \(d = 20p\), where \(p\) is an odd prime. Certain algebraic invariants discovered by Cantor are used to obtain necessary conditions that \(f_1\) represent the appropriate discriminantal divisors (-1, 5, and -5). The arithmetic theory of generalized quaternions is used to formulate a theorem which gives sufficient conditions that \(f_1\) represent -1, 5, or -5.

In Chapter II, the Cantor invariants are used to generalize the necessary conditions for representing discriminantal divisors, obtained in Chapter I, to discriminants of the form \(pq\) or \(4pq\). The cases \(d = 13p\) and \(d = 52p\) are studied in detail, again with the use of generalized quaternions. In the process, we obtain a complete parametric
solution of the following system of Diophantine equations:

\[ p = x_1^2 + x_2^2 = -x_3^2 + qx_4^2 = x_5^2 + qx_6^2 \]

Here, \( p \) and \( q \) are primes such that \( p \) is representable by \( x_1^2 + x_2^2 \) and \( x_5^2 + qx_6^2 \).

Chapters III and IV are devoted to the study of the cases \( d = pq \) and \( 4pq \), for \( q = 17, 29, 53, \) and \( 61 \); we obtain partial results in these cases.
An integral binary quadratic form (hereinafter called a form) is a homogeneous quadratic polynomial in two variables, \(ax^2 + bxy + cy^2 = [a,b,c]\), in which \(a, b,\) and \(c\) are ordinary integers. A class of forms is a set of forms which are transformable into one another by linear transformations with integral coefficients and determinant \(1\); such transformations are called unimodular. Write \(f \sim g\) (\(f\) is equivalent to \(g\)) to mean that the forms \(f\) and \(g\) are in the same class. The discriminant of the form \([a,b,c]\) is the integer \(d = b^2 - 4ac\); the determinant of the form \([a,b,c]\) is the number \(ac - b^2/4 = -d/4\) (which may or may not be an integer). An ambiguous form is a form \([a,b,c]\) in which \(a\) divides \(b\); an ambiguous class is a class of forms containing an ambiguous form. The form \([a,b,c]\) is primitive if \((a,b,c)\), the g.c.d. of coefficients, is \(1\); a primitive class is a class of forms consisting of primitive forms. We will write class and form hereafter to mean primitive class and form, unless otherwise specified. An ancipital form is a form \([a,b,c]\) in which \(b = 0\) or \(b = a\). To find the ancipital forms of a given discriminant \(d\) we must find all pairs of coprime integers \(a,c\) satisfying \(4ac = -d\) or \(a(4c - a) = -d\). The ancipital forms fall into equivalent
pairs of associates 

\[ [a,0,c] \text{ and } [c,0,a], \ [a,a,c] \text{ and } [4c-a,4c-a,c]. \]

(To see that \([a,a,c] \sim [4c-a,4c-a,c]\), apply to the first form the unimodular transformation \(x = -x' - y', y = 2x' + y'\)).

If \(d\) is a positive, non-square discriminant, then the first coefficients of two associates have opposite signs, and the smaller of the two satisfies \((2a)^2 < d\), or \(a^2 < d\), in the respective cases, while the larger satisfies \((2a)^2 > d\), or \(a^2 > d\).

For any non-zero discriminant \(d\), the set of first coefficients of (primitive) ancipital forms \([a,0,c]\) which satisfy \((2a)^2 < d\) will be denoted by \(S_1(d)\); those coefficients of the forms \([a,a,c]\) satisfying \(a^2 < d\) will be denoted by \(S_2(d)\). We will call those elements of either \(S_1(d)\) or \(S_2(d)\) discriminantal divisors of \(d\) of type 1 or type 2, respectively.

From the Gaussian theory of reduction of forms, the following can be deduced (we will postpone the proof for the time being):

**PROPOSITION 1.2.** Every primitive ambiguous class of positive non-square discriminant contains exactly two ancipital forms with positive first coefficient, and hence exactly two pairs of associate ancipital forms in all.

In view of this result, it is natural to ask the
following questions: given an ambiguous class of a positive non-square discriminant $d$, which two discriminantal divisors (that is, elements of $S_1(d)$ and $S_2(d)$) are represented (primitively) by that class? Which, besides 1, is represented by the principal class (i.e., the class containing the principal form, $[1, e, (e^2 - d)/4]$, where $e = 0$ or 1 according as $d \equiv 0$ or 1(mod 4))? A special case of this was considered by Dirichlet, who studied the equation $X^2 - AY^2 = -1$. He asserted that the problem of characterizing all values of $A$ for which the equation is solvable in integers $X$ and $Y$ is quite difficult [4, p. 223].

The purpose of this paper is to study the above questions for discriminants $d = pq$ and $d = 4pq$, where $p$ and $q$ are odd primes; the results obtained are similar to results obtained by Pall for discriminants $d = 2p$ and $d = 8p$, $p$ an odd prime, in [7]. We obtain necessary conditions that the principal class of such discriminants represent a given discriminantal divisor. Then we use results from the theory of generalized quaternions (see [8]) to obtain complete parametric solutions of systems of diophantine equations such as

$$p = x_1^2 + x_2^2 = -x_3^2 + qx_4^2 = x_5^2 + qx_6^2$$

(with appropriate restrictions on $p, q, x_1, \ldots, x_6$). Finally, we use these solutions in conjunction with the aforementioned
necessary conditions to prove representation theorems like

THEOREM 1.10. Let \((p|5) = 1\), \(p \equiv 1 \pmod{4}\), and \(f_1 = [1,0,-5p]\). Then:
(a) If \(p = x_5^2 + 5x_6^2\), with \(x_5\) even, then \(f_1\) never represents \(-1\); it represents 5 or \(-5\), according as \((p|5)_4 = 1\) or \(-1\).
(b) If \(p = a^2 + 25b^2\), with \(a\) even, then \(f_1\) never represents \(-5\); it represents 5 or \(-1\), according as \((p|5)_4 = 1\) or \(-1\).
(c) If \((p|5)_4 = -1\), then \(f_1\) never represents 5; it represents \(-1\) or \(-5\), according as \(p = x_5^2 + 5x_6^2\) with \(x_5\) odd, or \(p = x_5^2 + 5x_6^2\) with \(x_5\) even.
(d) If \((p|5)_4 = 1\), then \(f_1\) represents 5 if \(p = x_5^2 + 5x_6^2\) with \(x_5\) even; otherwise, any of the possibilities (that \(f_1\) represents \(-1,5,-5\)) can occur.

At this point, several comments are in order. From reading the statement of the preceding theorem, one infers that \(S_1(20p) = \{1,-1,5,-5\}\); this is true, and we shall prove that, if \(p \equiv q \pmod{4}\) and \(p > q\), then \(S_2(pq) = S_1(4pq) = \{1,-1,q,-q\}\). Throughout this discussion, the letters \(p\) and \(q\) will denote odd primes, the letter \(d\) will denote a discriminant, and the letters \(f,g\) and \(h\) will denote forms. We shall assume knowledge of the definitions, theorems and notations of elementary number theory (see [6]) and of
elementary theory of quadratic forms (see [1] or [9]).

Further, the symbol \((p|q)_4\) is defined, when \((p|q) = 1\), by

\[
(p|q)_4 = \begin{cases} 
1, & \text{if } p \equiv x^4 \pmod{q} \text{ has a solution;} \\
-1, & \text{if } p \equiv x^4 \pmod{q} \text{ has no solution.}
\end{cases}
\]

**Lemma 1.1.** Every ambiguous form \(f\) of positive non-square discriminant \(d\) is equivalent, by a translation \((x = x' + hy', y = y')\) to an unique ancipital form \(g\). Moreover, if \(f\) is primitive, so is \(g\).

**Proof.** Suppose \(f = [a, ka, z]\) is an ambiguous form for which \(d = a(k^2a - 4z)\) is positive and not a square. Let \(n = [k/2]\); applying the translation \((x = x' - ny', y = y')\) yields the form \(g = [a, (k - 2n)a, an^2 - kan + z]\). If \(\epsilon = 0\) or 1, according as \(k\) is even or odd, then \(k = 2n + \epsilon\); and \(g = [a, \epsilon a, an^2 - \epsilon an + z]\) is an ancipital form of type 1 or 2, according as \(\epsilon = 0\) or 1. Now \(g\) is unique, since any translation applied to \(f\) yields a form with middle coefficient \((k + 2m)a\): letting \(m = -n + s\), we see that \((k + 2m)a = (k - 2n + 2s)a = (\epsilon + 2s)a = 0\) or \(a\) if and only if \(s = 0\). Finally, since \(f \sim g\), \(f\) primitive implies \(g\) primitive, because the g.c.d. of a form is invariant under unimodular transformation.

Q.E.D.

**Proposition 1.2.** Every primitive ambiguous class of positive non-square discriminant contains exactly two
ancipital forms with positive first coefficient, and hence exactly two pairs of associate ancipital forms in all.

**PROOF.** This follows from Gauss's theorem that the chain of reduced forms of a primitive ambiguous class with a positive non-square discriminant contains exactly two ambiguous forms. By Lemma 1.1, each of these is translatable into an unique ancipital form; moreover, the two resulting ancipital forms are not associates. To see this, observe that exactly one of a pair of associate ancipital forms is translatable to a reduced ambiguous form. In the case of forms of type 1, this is proved by assuming, for instance, that for $a > 0$, $c > 0$, there exist integers $k, k' > 0$ for which both $[a, 2ka, ak^2 - c]$ and $[-c, 2k'c, -ck'^2 + a]$ are reduced (these are translates of $[a, 0, -c]$ and $[-c, 0, a]$ respectively). Since these forms are reduced, we must have $ak^2 - c < 0$ and $-ck'^2 + a > 0$; this implies that $c > ak^2$, $a > ck'^2$, and hence $c > ck^2k'^2$, or $1 > k^2k'^2$; since $k, k' > 0$, this is a contradiction. Analogous results hold for forms of type 2. Hence, in the given ambiguous class, there are two non-associate ancipital forms and their associates, making four in all. Two of these have positive first coefficients and two have negative first coefficients; they are all primitive, since the class is primitive.

Q.E.D.

Another result from Gauss is that the number of
primitive ambiguous classes of a non-zero discriminant $d$ is equal to the number of primitive genera of $d$. We then deduce, from Proposition 1.2, that the total number of pairs of primitive ancipital forms of a positive non-square discriminant $d$ is equal to twice the number of primitive genera of $d$, and is equal to the cardinality of $S_1(d) \cup S_2(d)$.

Let $p = q \pmod{4}$, $p \neq q$. For $d = pq$ or $d = 4pq$, there are the generic characters $(f|p)$ and $(f|q)$; by the Gaussian theory of forms, their product is 1, so there are two genera, and four pairs of associate ancipital forms, which we enumerate here ($f_1$ and $g_1$ are associates):

For $d = pq$:

$f_1 = [1,1,(1-pq)/4]$, $g_1 = [-pq,-pq,(1-pq)/4]$;
$f_2 = [-1,-1,(pq-1)/4]$, $g_2 = [pq,pq,(pq-1)/4]$;

(1.2.1)

$f_3 = [q,q,(q-p)/4]$, $g_3 = [-p,-p,(q-p)/4]$;
$f_4 = [-q,-q,(p-q)/4]$, $g_4 = [p,p,(p-q)/4]$.

For $d = 4pq$:

$f_1 = [1,0,-pq]$, $g_1 = [-pq,0,1]$;
$f_2 = [-1,0,pq]$, $g_2 = [pq,0,-1]$;

(1.2.2)

$f_3 = [q,0,-p]$, $g_3 = [-p,0,q]$;
$f_4 = [-q,0,p]$, $g_4 = [p,0,-q]$.

It is clear that, if $p < q$, then $S_2(pq) = S_1(4pq) = \ldots$
\{l,-l,p,-p\}, and if \( p > q \), then \( S_2(pq) = S_1(4pq) = \{l,-l,q,-q\} \).

It is also evident that in either case, \( f_1 \) represents \( p \) implies \( f_1 \) represents \(-q\), and if \( f_1 \) represents \(-p\), then it also represents \( q \). Since our strategy is to fix a prime \( q \), and examine the forms \( f_1 \) and \( g_1 \) for varying \( p \), we lose no generality in changing our main question to: which two elements of \( T(pq) = T(4pq) = \{l,-l,q,-q\} \) do each of the forms \( f_1 \) represent? We remark here that all representations of primes and of \( \pm 1 \) must be primitive, so that we will write "representation" to mean "primitive representation" (unless otherwise specified). The following proposition will enable us to work with \( d = 4pq \), and at the same time, obtain representability data on \( d = pq \).

**PROPOSITION 1.3.** Let \( p \) and \( q \) be as above. The form \([l,0,-pq]\) represents one of \(-l,q,-q\) if and only if the same one is represented by \([l,l,(1-pq)/4]\).

**PROOF.** If there exist integers \( x,y \) such that 
\[
x^2 - pqy^2 = -l,q,\text{ or } -q,
\]
then by letting \( u = x - y, v = 2y \), we have 
\[
u^2 + uv + (1-pq)v^2/4 = x^2 - 2xy + y^2 + 2xy - 2y^2 + \frac{1}{4}(4y^2) - pqy^2 = x^2 - pqy^2 = (\text{the same}) - l,q,\text{ or } -q.
\]
Conversely, if \([l,l,(1-pq)/4]\) represents \( k \), and \([l,0,-pq]\) represents \( n \), where \( k,n \in \{-l,q,-q\} \), then \([l,l,(1-pq)/4]\) represents \( n \), by the above argument. Since \([l,l,(1-pq)/4]\) represents exactly one of \(-l,q,-q\), we deduce that \( k = n \).

Q.E.D.
As mentioned above, we shall derive necessary conditions that $f_1 = [1, 0, -pq]$ represents $-1, q$, or $-q$; obviously necessary is that the forms $f_2 = [-1, 0, pq], f_3 = [q, 0, -p], \text{ or } f_4 = [-q, 0, p]$ be in the genus of $f_1$ if $f_1$ is to represent $-1, q$, or $-q$ respectively. This is put to use in the following proposition, which, by virtue of Proposition 1.3, is true also for $d = pq$:

**PROPOSITION 1.4.** Let $p \equiv q \equiv 3 (\text{mod } 4)$. Then $f_1 = [1, 0, -pq]$ never represents $-1$; it represents $q$ if $(q|p) = 1$, and $-q$ if $(q|p) = -1$.

**PROOF.** There are two genera for $d = 4pq$, and the forms $f_1, f_2, f_3, f_4$ are distributed between these genera according to the following table of generic characters:

<table>
<thead>
<tr>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
<th>$f_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$-1$</td>
<td>$(q</td>
<td>p)$</td>
</tr>
</tbody>
</table>

From this table, the conclusion follows.

Q.E.D.

Now let $d = 4pq$, where $p \equiv q \equiv 1 (\text{mod } 4)$. By examining the table of generic characters for the antepenultimate
forms given below, we deduce that \( f_1 \) represents \(-1\) if \((p|q) = (q|p) = -1:\)

\[
\begin{array}{ccc}
(f|p) & (f|q) \\
\hline
f_1 & 1 & 1 \\
f_2 & 1 & 1 \\
f_3 & (q|p) & (q|p) \\
f_4 & (q|p) & (q|p)
\end{array}
\]

To discover more information when \((q|p) = 1\), we start with a specific case, namely \(q = 5\). Then the pertinent divisors are \(T(5p) = T(20p) = \{1, -1, 5, -5\}\). We now digress to develop a piece of algebraic machinery that will shorten later arguments and enable us to connect the form \([1, 0, -pq]\) with forms of determinants \(1, -q,\) and \(q\). We recall that the determinant of the form \(f = [a, b, c]\) is the determinant of

\[
\begin{vmatrix}
a & b/2 \\
b/2 & c
\end{vmatrix}
\]

which is called the matrix of the form \(f\).

**DEFINITION.** A Cantor diagram is a diagram of the form

\[
h_1 \xrightarrow{T} h_2
\]

\[
h_4 \xleftarrow{T'} h_3
\]
where the $h_i$ are binary quadratic forms, $T$ is a $2 \times 2$ matrix which transforms $h_1$ into $h_2$, and $T'$ is the transpose of $T$, and carries $h_3$ into $h_4$. (This idea originated with Georg Cantor in 1868).

**PROPOSITION 1.5.** If $h_1 \xrightarrow{T} h_2$ is a Cantor diagram, then $a_1 a_4 + 2b_1 b_4 + c_1 c_4 = a_2 a_3 + 2b_2 b_3 + c_2 c_3$ where $h_1 = [a_i, b_i, c_i], 1 \leq i \leq 4$.

**PROOF.** Let $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$; since $h_1 \xrightarrow{T} h_2$, we have

\[
(a_1 ax + b_1 by)^2 + 2b_1 (ax + by)(cx + dy) + c_1 (cx + dy)^2 = a_2 x^2 + 2b_2 xy + c_2 y^2,
\]

where: $a_2 = a_1 a^2 + 2b_1 ac + c_1 c^2$,

$2b_2 = 2a_1 ab + 2b_1 (ad + bc) + 2c_1 cd$, and

$c_1 = a_1 b^2 + 2b_1 bd + c_1 d^2$. Since $h_4 \xleftarrow{T'} h_3$,

we have, by replacing 1 by 3 and 2 by 4 in the above, the following:

\[
a_4 = a_3 a^2 + 2b_3 ab + c_3 b^2,
2b_4 = 2a_3 ac + 2b_3 (ad + bc) + 2c_3 bd, \text{ and}
\]

$c_4 = a_3 c^2 + 2b_3 cd + c_3 d^2$. Hence

\[
a_1 a_4 + 2b_1 b_4 + c_1 c_4 = a_1 (a_3 a^2 + 2b_3 ab + c_3 b^2) + 2b_1 (a_3 ac + b_3 (ad + bc) + c_3 bd) + c_1 (a_3 c^2 + 2b_3 cd + c_3 d^2)
\]
\[ a_3 (a_1 a^2 + 2b_1 a c + c_1 c^2) + 2b_3 (a_1 a b + b_1 (a d + b c) + c_1 c d) + c_3 (a_1 b^2 + 2b_1 b d + c_1 d^2) = a_2 a_3 + 2b_2 b_3 + c_2 c_3. \]

Q.E.D.

THEOREM 1.6. Let \((p \mid 5) = 1, p \equiv 1 \mod 4\), and \(f_1 = [1,0,-5p]\).

Then:

(a) A necessary condition that \(f_1\) represent \(-1\) is that there exist integers \(x_1\) odd, \(x_2\) even such that \(p = x_1^2 + x_2^2\), with either \((x_1 + 2x_2 \mid 5) = 1\) and \((2x_1 - x_2 \mid 5) = -1\), or \((x_1 - 2x_2 \mid 5) = 1\) and \((2x_1 + x_2 \mid 5) = -1\).

(b) A necessary condition that \(f_1\) represent \(5\) is that there exist integers \(x_3\) even, \(x_4\) odd such that \(p = -x_3^2 + 5x_4^2\), with \((x_3 \mid 5) = -1\); or, equivalently, that there exist integers \(y_3\) even, \(y_4\) odd such that \(p = y_4^2 - 5y_3^2\), with \((y_4 \mid 5) = 1\).

(c) A necessary condition that \(f_1\) represent \(-5\) is either (1) there exist integers \(x_5\) odd, \(x_6\) even such that \(p = x_5^2 + 5x_6^2\) and \((x_5 \mid 5) = (p \mid 5)_4 = 1\); or (2) there exist integers \(x_5\) even, \(x_6\) odd such that \(p = x_5^2 + 5x_6^2\) and \((x_5 \mid 5) = (p \mid 5)_4 = -1\).

PROOF. (a) If there exist integers \(u,v\) \((v > 0, \text{ since } (-v)^2 = v^2)\) such that \(u^2 - 5pv^2 = -1\), then there exists a form \(g = [5pv,2u,v]\) of determinant \(1\). Hence \(g \sim [1,0,1]\), since there is only one class of positive definite forms of
determinant 1. We form the following Cantor diagram:

\[ [1,0,1] \xrightarrow{T} [5pv,2u,v] = g \]

\[ h = [z_1,2z_2,z] \xleftarrow{T'} [1,0,-5p] = f_1 \]

From here on, we will denote by \( h \) the image of \( f_1 \) under \( T' \). By Proposition 1.5, \( z_1 + z = 5pv - 5pv = 0 \), so that \( z_1 = -z \), and there is a form \( h = [z_1,2z_2,-z_1] \approx f_1 \). Comparing determinants, we find that \( 5p = z_1^2 + z_2^2 \). Since \( h \) is primitive, \( z_1 \) must be odd, so \( z_2 \) is even. Since \( h \) is in the genus of \( f_1 \), we must have \( 1 = (z_1|5) = (2z_2|5) \), because both \( z_1 \) and \( 2z_2 \) are represented (primitive) by \( h \). Hence \( (z_1|5) = 1, (z_2|5) = -1 \). Now \( p \) is a prime \( \equiv 1 \pmod{4} \), and so has a representation \( p = x_1^2 + x_2^2 \) as a sum of two squares. This representation is unique up to change of signs and order, so we may assume \( x_1 \) is odd, \( x_2 \) is even, and both are positive, with no loss in generality. Then

\[ 5p = (1^2 + 2^2)(x_1^2 + x_2^2) = (x_1 + 2x_2)^2 + (2x_1 \mp x_2)^2 = z_1^2 + z_2^2 ; \]

since \( z_1 \) is odd and \( z_2 \) even, we have \( z_1 = x_1 + 2x_2 \) and \( z_2 = 2x_1 \mp x_2 \) (this notation means that if we choose \( z_1 = x_1 + 2x_2 \), we must choose \( z_2 = 2x_1 - x_2 \), etc). Hence, either (1) \( (x_1 + 2x_2|5) = 1 \) and \( (2x_1-x_2|5) = -1 \), or (2) \( (x_1-2x_2|5) = 1 \) and \( (2x_1+x_2|5) = -1 \). This proves (a).

(b) If there exist integers \( u,v \) (again, we may assume \( v > 0 \)) such that \( u^2 - 5pv^2 = 5 \), then there exists a form \( g = [5pv,2u,v] \) of determinant \(-5\). Now
\[ u^2 - 5pv^2 = u^2 - \nu^2 \pmod{4}, \] so that in this case, \[ u^2 = 5 + \nu^2 \equiv 1 + \nu^2 \pmod{4} \] implies that \( u \) is odd and \( \nu \) is even.

Hence \( g \) is imprimitive, with \( \gcd = 2 \), since \((5pv, 2u, \nu) = (5pv, (2u, \nu)) = (5pv, 2) = (\nu, 2) = 2. \) Hence \( g \sim [2, 2, -2] \), the latter representing the only class of determinant \(-5, \gcd = 2.\) We then form the following Cantor diagram:

\[
[2, 2, -2] \xrightarrow{T} [5pv, 2u, \nu] = g
\]

\[
h = [a, 2b, c] \xleftarrow{T'} [1, 0, -5p] = f_1
\]

By Proposition 1.5, \( 2a + 2b - 2c = 0, \) so \( c = a + b, \) and hence there is a form \( h = [a, 2b, a+b] \sim f_1. \) Equating determinants yields the equation \( 5p = b^2 - ba - a^2. \) Since \( h \) is primitive, either \( a \) or \( a+b \) is odd; however, \( b^2 - ba - a^2 = (-b)^2 - (-b)(a+b) - (a+b)^2, \) so we may replace \( a \) by \( a+b \) and \( b \) by \(-b, \) and change nothing. Hence, we may assume that \( a \) is odd. It is easy to verify that we may also replace \( b \) by \( b - a \) and \( a \) by \(-a, \) so we may also assume that \( b \) is even. Hence \( b = 2y_4, \) and we have

\[
5p = 4y_4^2 - 2ay_4 - a^2 = 5y_4^2 - (y_4 + a)^2; \quad 5 \text{ must therefore divide } y_4 + a, \text{ so we write } y_4 + a = 5y_3, \text{ and so } 5p = 5y_4^2 - 25y_3^2.
\]

Hence \( p = y_4^2 - 5y_3^2, \) and since \( 5 \neq p \equiv 1 \pmod{4}, \) we have \( y_4 \) odd, \( (y_4, 5) = 1, \) and \( y_3 \) even. Since \( h = [5y_3 - y_4, 4y_4, 5y_3 + y_4] \) is in the genus of \( f_1, \) we have

\[
l = (5y_3 + y_4) \mid 5 = (y_4 \mid 5). \quad \text{We observe that the unimodular substitution } y_3 = x_3 - 2x_4, y_4 = -2x_3 + 5x_4, \text{ yields}
\]
\[ p = -x_3^2 + 5x_4^2, \] with \( x_3 \) even and \( x_4 \) odd holding in order that \( y_3 \) be even and \( y_4 \) odd. Finally, \( l = (-2x_3 + 5x_4 | 5) = (-2x_3 | 5) \), so that \( (x_3 | 5) = -1 \). The conditions involving the pair \( x_3 \) and \( x_4 \) are equivalent to those involving the pair \( y_3 \) and \( y_4 \), since the unimodular substitution
\[ x_3 = 5y_3 + 2y_4, \ x_4 = 2y_3 + y_4, \] transforms \( -x_3^2 + 5x_4^2 \) back into \( y_4^2 - 5y_3^2 \). This proves (b).

(c) If there exist integers \( u,v \) (again, with \( v > 0 \)) such that \( u^2 - 5pv^2 = -5 \), then there is a form \( g = [5pv, 2u, v] \) of determinant 5. There are two classes of positive definite forms of determinant 5, represented by \([1,0,5]\) and \([2,2,3]\). Hence there are two cases:

1. \( g \sim [1,0,5] \). We form the following Cantor diagram:

\[ [1,0,5] \xrightarrow{T} [5pv, 2u, v] = g \]
\[ h = [w, 2z, x_5] \xleftarrow{T'} [1,0,-5p] = f_1 \]

By Proposition 1.5, \( w + 5x_5 = 0 \), so \( w = -5x_5 \), and there is a form \( h = [-5x_5, 2z, x_5] \sim f_1 \). Equating determinants, we find that \( 5p = 5x_5^2 + z^2 \). Hence \( z = 5x_6 \), and we have \( p = x_5^2 + 5x_6^2 \). Since \( h \) is primitive, \( x_5 \) is odd, so \( x_6 \) is even; since \( h \) is in the genus of \( f_1 \), we have \( (x_5 | 5) = 1 \). Finally, \( p \equiv x_5^2 \pmod{5} \) implies that \( (p|5)_4 = (x_5^2|5)_4 = (x_5|5)_2 = 1 \).
(2) \[ g \sim [2,2,3]. \] We form the following Cantor diagram:

\[
[2,2,3] \xrightarrow{T} [5pv,2u,v] = g
\]

\[
h = [a,2b,c] \xleftarrow{T'} [1,0,-5p] = f_1
\]

By Proposition 1.5, \(2a + 2b + 3c = 0\), so that \(c = 2x_5\) is even. Hence \(a + b + 3x_5 = 0\), \(a = -b - 3x_5\), and there is a form \(h = [-b-3x_5,2b,2x_5] \sim f_1\). Equating determinants, we have \(5p = b^2 + 2bx_5 + 6x_5^2 = (b+x_5)^2 + 5x_5^2\). Hence \(b\) is odd, so \(x_5\) is even (since \(h\) is primitive) and \(b+x_5\) is odd, and is divisible by 5. Writing \(b+x_5 = 5x_6\), we obtain \(p = x_5^2 + 5x_6^2\). Since \(h\) is the genus of \(f_1\), we find that \(l = (2x_5|5)\), so \((x_5|5) = -1\). Hence \((x^2|5)_4 = -1\), and \(p \equiv x_5^2 \pmod{5}\) implies that \((p|5)_4 = -1\). This proves (c), and completes the proof of Theorem 1.6.

Q.E.D.

Since we are concerned with the representations of a prime by the forms \(x^2+y^2\), \(-x^2+5y^2\) and \(x^2+5y^2\), any relationships among such representations could be more easily discerned by obtaining a complete solution of

\[(1.6.1) \quad p = x_1^2 + x_2^2 = -x_3^2 + 5x_4^2 = x_5^2 + 5x_6^2\]

by expressions for \(x_1, \ldots, x_6\) with integral-valued parameters. We propose to obtain such a solution, for
x_1, x_3, x_5 odd, and x_2, x_4, x_6 even; also a solution for x_1, x_3, x_6 odd, and x_2, x_4, x_5 even will be obtained. In each case, p will denote a prime representable by the forms x^2 + y^2 and x^2 + 5y^2 (i.e. (p | 5) = 1, p ≡ 1 (mod 4)). To accomplish this, we will study the solutions of
x_1^2 + x_2^2 = -x_3^2 + 5x_4^2 in integral parameters t_0, t_1, t_2, t_3, the solutions of -x_3^2 + 5x_4^2 = x_5^2 + 5x_6^2 in integral parameters s_0, s_1, s_2, s_3, and the solutions of x_5^2 + 5x_6^2 = x_1^2 + x_2^2 in integral parameters u_0, u_1, u_2, u_3. Then we will adjust the parameters t_1 and s_1 to make the two expressions of x_3 and of x_4 equal, obtaining a complete parametric solution of (1.6.1) when x_5 is odd, x_6 is even, and p is a prime. Finally, we will adjust the parameters t_1 and u_1 to make the two expressions of x_1 and of x_2 equal, obtaining a complete parametric solution of (1.6.1) when x_5 is even, x_6 is odd, and p is a prime.

THEOREM 1.7. Let p be a prime which is representable by the forms x^2 + y^2 and x^2 + 5y^2. Then every solution in integers x_1, ..., x_6 with x_1 and x_4 odd, x_2 and x_3 even of the system of equations

\begin{align*}
(1.6.1) \quad p &= x_1^2 + x_2^2 = -x_3^2 + 5x_4^2 = x_5^2 + 5x_6^2
\end{align*}

is given (except for sign), for integral values of t_0, t_1, t_2, t_3 (one or three of which may be odd), by the following
expressions:

\[ x_1 = t_0^2 + t_1^2 - t_2^2 - t_3^2 + 4(-t_0 t_2 + t_1 t_3) \]
\[ x_2 = 2(-t_0 t_3 + t_1 t_2) + 4(t_0 t_1 + t_2 t_3) \]
\[ x_3 = 2(t_0 t_2 + t_1 t_3) + 2(t_0^2 + t_3^2 - t_1^2 - t_2^2) \]

\((1.7.1)\)

\[ x_4 = t_0^2 + t_1^2 + t_2^2 + t_3^2 \]
\[ x_5 = t_0^2 + t_3^2 - t_1^2 - t_2^2 + 4(t_0 t_3 + t_1 t_2) \]
\[ x_6 = 2(-t_0 t_1 + t_2 t_3) \quad (x_5 \text{ odd}, x_6 \text{ even}) \]

and

\[ x_1 = t_0^2 + t_1^2 - t_2^2 - t_3^2 + 4(t_0 t_3 + t_1 t_2) \]
\[ x_2 = 2(-t_0 t_3 + t_1 t_2) + 2(t_0^2 + t_2^2 - t_1^2 - t_3^2) \]
\[ x_3 = 2(t_0 t_2 + t_1 t_3) + 4(-t_0 t_1 + t_2 t_3) \]

\((1.7.2)\)

\[ x_4 = t_0^2 + t_1^2 + t_2^2 + t_3^2 \]
\[ x_5 = 2(t_0 t_1 - t_2 t_3) + 4(t_0 t_2 + t_1 t_3) \]
\[ x_6 = t_0^2 + t_3^2 - t_1^2 - t_2^2 \quad (x_5 \text{ even}, x_6 \text{ odd}) \]

PROOF. The proof is based on the properties of certain quaternary quadratic forms, called norm-forms, and their relationship to the theory of factorization of generalized
quaternions. For details beyond this paper, see [8].

With each integral ternary quadratic form \( f \) of matrix \([a_{\alpha\beta}]\) is associated a certain quaternion ring. The quaternary quadratic form \( F \) associated with this ring and defined by

\[
(1.7.3) \quad F = (x_0 + \epsilon_1 x_1/2 + \epsilon_2 x_2/2 + \epsilon_3 x_3/2)^2 + \sum_{\alpha, \beta} A_{\alpha\beta} x_\alpha x_\beta
\]

where \( A = [A_{\alpha\beta}] \) is the adjoint matrix of \([a_{\alpha\beta}]\) and the \( \epsilon_i \) are chosen to make \( F \) an integral form, is called the norm-form of the ring. We denote by \( Q^* \) the conjugate of the quaternion \( Q \), and by \( N(Q) \) the norm of \( Q \); a quaternion \( Q \) is pure if \( Q^* = -Q \).

We state the following without proof:

**Lemma 1.8.** (essentially Theorem 3 of [8]). Let \( m \) be a non-zero integer represented by some form in the genus of the norm-form \( F \); assume \( m \) is not divisible by any prime \( p \) such that \( p^2 \mid d \) \((d = -4 \cdot \text{det}[a_{\alpha\beta}])\) or such that \( p \parallel d \) and \( c_p = +1 \) (see [9]); assume \( Q \) is a primitive quaternion such that \( m \mid N(Q) \), and that the genus of \( F \) contains only one class. Then there exists a right-divisor \( \sigma \) of \( Q \), of norm \( m \) and unique up to a left unit factor.

To study the solutions of

\[
(1.7.4) \quad x_1^2 + x_1^2 = -x_3^2 + 5x_4^2
\]

in integral parameters, for \( x_1 \) and \( x_4 \) odd, \( x_2 \) and \( x_3 \) even,
we examine the equation \(5x_4^2 = x_2^2 + x_3^2\), and we observe that \(Q = i_1x_1 + i_2x_2 + i_3x_3\) is a quaternion of norm \(5x_4^2\) in the ring of quaternions with the following multiplication table (the so-called Lipschitz quaternions): \(i_1^2 = i_2^2 = i_3^2 = -1\), \(i_1i_2 = i_3 = -i_2i_1, i_2i_3 = i_1 = -i_3i_2\), and \(i_3i_1 = i_2 = -i_1i_3\).

The norm-form of this ring is the form \(F = t_0^2 + t_1^2 + t_2^2 + t_3^2\), which is in a genus of one class [8,p.329]. Since we assume \(x_4\) odd, the hypotheses of Lemma 1.8 are satisfied, so we may write \(Q = \beta\sigma\), where \(\sigma = t_0 + t_1i_1 + t_2i_2i_3\) is unique up to a left-unit factor, and \(N(\sigma) = \sum_{i=0}^{3} t_i^2 = x_4\).

Now \(Q\) is pure, so \(-\beta\sigma = -Q = Q^* = \sigma^*\beta^*\). Hence \(\sigma^*\) is a left-divisor of \(\beta\), and we may write \(Q = \sigma^*\tau\sigma\), where \(N(\tau) = 5\).

**Lemma 1.9.** If \(Q, \sigma\) and \(\tau\) are quaternions (in any quaternion ring) satisfying \(Q = \sigma^*\tau\sigma\), if \(\sigma \neq 0\), and if \(Q\) is pure, then \(\tau\) is pure.

**Proof.** If \(Q = \sigma^*\tau\sigma\), then \(Q^* = \sigma^*\tau^*\sigma\). \(Q\) is pure, so \(0 = Q + Q^* = \sigma^*(\tau + \tau^*)\sigma\); these rings contain no zero divisors, so \(\tau + \tau^* = 0\) (recall \(\sigma \neq 0\)); hence \(\tau\) is pure.

By the above lemma, \(\tau\) is pure; if we write \(\tau = ai_1 + bi_2 + ci_3\) (\(a,b,c\) to be determined), then

\(Q = \sigma^*\tau\sigma = (t_0 + t_1i_1 - t_2i_2 - t_3i_3)(ai_1 + bi_2 + ci_3)(t_0 + t_1i_1 + t_2i_2 + t_3i_3)\)
\[ \begin{align*}
&= a(t_0 - t_1 i_1 - t_2 i_2 - t_3 i_3) + a(t_0 + t_1 i_1 + t_2 i_2 + t_3 i_3) + b(t_0 - t_1 i_1 - t_2 i_2 - t_3 i_3) + b(t_0 + t_1 i_1 + t_2 i_2 + t_3 i_3) + c(t_0 - t_1 i_1 - t_2 i_2 - t_3 i_3) + c(t_0 + t_1 i_1 + t_2 i_2 + t_3 i_3) \\
&= x_1^2 + x_2^2 + x_3^2. \text{ Collecting coefficients of} \ i_1, i_2, i_3, \text{ we have} \]

\[ \begin{align*}
x_1 &= a(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2b(t_0 t_3 + t_1 t_2) + 2c(-t_0 t_2 + t_1 t_3) \\
x_2 &= 2a(-t_0 t_3 + t_1 t_2) + b(t_0^2 + t_2^2 - t_1^2 - t_3^2) + 2c(t_0 t_1 + t_2 t_3) \\
x_3 &= 2a(t_0 t_2 - t_1 t_3) + 2b(-t_0 t_1 + t_2 t_3) + c(t_0^2 + t_3^2 - t_1^2 - t_2^2) \\
x_4 &= N(\sigma) = t_0^2 + t_1^2 + t_2^2 + t_3^2.
\end{align*} \]

We observe that \( x_1 = a, \ x_2 = b, \ x_3 = c \) (mod 2), so that \( a \) is odd, and \( b \) and \( c \) are even. The possibilities for \( \tau \) are \( \pm(i_1 + 2i_2) \) and \( \pm(i_1 + 2i_3) \), for any other pure quaternion of norm 5 has \( a \) even. We now show that all parametric solutions of \( (1.7.4) \), except possibly for changes of the sign of \( x_3 \) and \( x_4 \), can be obtained by using \( \tau_1 = i_1 + 2i_2 \) and \( \tau_2 = i_1 + 2i_3 \). (We would need to use only \( \tau_1 \) were we interested only in the equation \( 5x_4^2 = x_1^2 + x_2^2 + x_3^2 \), for replacing \( \tau_1 \) by \( \tau_2 \) has the effect of permuting \( x_2 \) and \( x_3 \)).

Using \( \tau^{(1)}_1 = \tau_1 \), we obtain

\[ \begin{align*}
x_1^{(1)} &= t_0^2 + t_1^2 - t_2^2 - t_3^2 + 4(t_0 t_3 + t_1 t_2) \\
x_2^{(1)} &= 2(-t_0 t_3 + t_1 t_2) + 2(t_0^2 + t_2^2 - t_1^2 - t_3^2)
\end{align*} \]
(1.7.5)
\[ x_3^{(1)} = 2(t_0 t_2 + t_1 t_3) + 4(-t_0 t_1 + t_2 t_3) \]
\[ x_4^{(1)} = t_0^2 + t_1^2 + t_2^2 + t_3^2 \quad \text{(one or three of the } t_i \text{ are odd)} \]

Using \( \tau_1^{(2)} = i_1 - 2i_2 \), we obtain
\[ x_1^{(2)} = t_0^2 + t_1^2 - t_2^2 - t_3^2 + 4(-t_0 t_3 - t_1 t_2) \]
\[ x_2^{(2)} = 2(-t_0 t_3 + t_1 t_2) + 2(-t_0 - t_2 + t_1 + t_3) \]

(1.7.6)
\[ x_3^{(2)} = 2(t_0 t_2 + t_1 t_3) + 4(t_0 t_1 - t_2 t_3) \]
\[ x_4^{(2)} = x_4^{(1)} \quad \text{(one or three of the } t_i \text{ are odd)} \]

If we use \( \tau_1^{(3)} = -\tau_1^{(2)} \), we obtain \( x_1^{(3)} = -x_1^{(2)} \), \( x_2^{(3)} = -x_2^{(2)} \), \( x_3^{(3)} = -x_3^{(2)} \), and \( x_4^{(3)} = x_4^{(2)} \). If we use \( \tau_1^{(4)} = -\tau_1^{(1)} \), we obtain \( x_1^{(4)} = -x_1^{(1)} \), \( x_2^{(4)} = -x_2^{(1)} \), \( x_3^{(4)} = -x_3^{(1)} \), and \( x_4^{(4)} = x_4^{(1)} \). Replacing
\[ t_0 \] by \( -t_1 \), \( t_1 \) by \( -t_0 \), \( t_2 \) by \( t_3 \) and \( t_3 \) by \( t_2 \) (we may do this, since we may choose any values for the \( t_i \) subject to the restriction that one or three of them must be odd)
changes \( x_1^{(2)} \) to \( x_1^{(1)} \), \( x_2^{(2)} \) to \( x_2^{(1)} \), and \( x_3^{(2)} \) to \( -x_3^{(1)} \).

Replacing \( t_0 \) by \( -t_2 \), \( t_1 \) by \( -t_3 \), \( t_2 \) by \( -t_0 \), and \( t_3 \) by \( -t_1 \)
changes \( x_1^{(3)} \) to \( x_1^{(1)} \), \( x_2^{(3)} \) to \( x_2^{(1)} \), and \( x_3^{(3)} \) to \( -x_3^{(1)} \).

Finally, replacing \( t_0 \) by \( -t_3 \), \( t_1 \) by \( -t_2 \), \( t_2 \) by \( t_1 \), and \( t_3 \) by \( t_0 \) changes \( x_1^{(4)} \) to \( x_1^{(1)} \), \( x_2^{(4)} \) to \( x_2^{(1)} \) and
$x_3^{(4)}$ to $x_3^{(1)}$. Note that $x_4 \geq 0$ in all cases.

Hence, except for alteration of the sign of $x_3$, we lose no solutions of (1.7.4) by restricting our choice of the $\tau_1^{(1)}$ to $\tau_1^{(1)} = \tau_1$. A similar argument shows the same thing for $\tau_2$; if we use $\tau_2 = i_1 + 2i_3$, we obtain

$$x_1 = t_0^2 + t_1^2 - t_2^2 - t_3^2 + 4(-t_0 t_2 + t_1 t_3)$$

$$x_2 = 2(-t_0 t_3 + t_1 t_2) + 4(t_0 t_1 + t_2 t_3)$$

(1.7.7)

$$x_3 = 2(t_0 t_2 + t_1 t_3) + 2(t_0^2 + t_2^2 - t_1^2 - t_3^2)$$

$$x_4 = t_0^2 + t_1^2 + t_2^2 + t_3^2 \quad \text{(where one or three of the $t_i$ are odd)}$$

Since by Lemma 1.8 the factorization of $Q$ is unique, the expressions in (1.7.5) and (1.7.7) yield all solutions (except for changes of the sign of $x_3$ and $x_4$) of (1.7.4) in independent parameters $t_0, t_1, t_2, t_3$ with $x_1$ and $x_4$ odd, and $x_2$ and $x_3$ even.

To study the solutions of

(1.7.8) $-x_3^2 + 5x_4^2 = x_5^2 + 5x_6^2$

in integral parameters, in the case where $x_4$ and $x_5$ are odd, and $x_3$ and $x_6$ are even, we study the equation

(1.7.9) $y_4^2 - 5y_3^2 = x_5^2 + 5x_6^2$
in the case that $y_4$ and $x_5$ are odd, and $y_3$ and $x_6$ are even. Using the parametric solutions of (1.7.9) and the unimodular substitution $y_4 = 5x_4 - x_3$, $y_3 = -2x_4 + x_3$, we will be able to find parametric solutions of (1.7.8).

Examining the equation $y_4^2 = x_5^2 + 5y_3^2 + 5x_6^2$, we see that the right hand side is the norm of a quaternion $Q = x_5i_1 + y_3i_2 + x_6i_3$ in the ring of quaternions with the multiplication given by the following:

$$i_1^2 = -1, \quad i_2^2 = i_2^2 = -5, \quad i_1i_2 = -i_2i_1 = i_3, \quad i_2i_3 = -i_3i_2 = 5i_1, \quad \text{and} \quad i_3i_1 = -i_1i_3 = i_2.$$ Now the norm-form of this ring is

$$F = s_0^2 + s_1^2 + 5s_2^2 + 5s_3^2,$$ which is not, unfortunately, in a genus of one class. We will show that, for our purposes (namely, studying the equation (1.6.1)), this does not matter; although we may not be able to obtain all solutions of (1.7.8) and (1.7.9), we proceed as above. We write $Q = \sigma^* \tau \sigma$, where $N(\sigma) = N(s_0 + s_1i_1 + s_2i_2 + s_3i_3) = y_4$, and $N(\tau) = 1$. By Lemma 1.9, $\tau$ is pure because $Q$ is pure, so we may take $\tau$ to be $i_1$; hence $Q = x_5i_1 + y_3i_2 + x_6i_3 = (s_0 - s_1i_1 - s_2i_2 - s_3i_3)i_1(s_0 + s_1i_1 + s_2i_2 + s_3i_3)$

$$= i_1(s_0^2 + s_1^2 - 5s_2^2 - 5s_3^2) + 2i_2(-s_0s_3 + s_1s_2) + 2i_3(s_0 + s_1s_3).$$ Comparing coefficients, we have

$$x_5 = s_0^2 + s_1^2 - 5s_2^2 - 5s_3^2$$

$$y_1 = 2(-s_0s_3 + s_1s_2)$$
(1.7.10)

\[ x_5 = 2(s_0s_2 + s_1s_3) \]
\[ y_4 = N(\sigma) = s_0^2 + s_1^2 + 5s_2^2 + 5s_3^2 \]
(\text{where one or three of the } s_i \text{ are odd}).

Since \( x_4 = y_4 + 2y_3 \) and \( x_3 = 2y_4 + 5y_3 \), we have the following:

\[ x_3 = 2(s_0^2 + s_1^2 + 5s_2^2 + 5s_3^2) + 10(-s_0s_3 + s_1s_2) \]
\[ x_4 = s_0^2 + s_1^2 + 5s_2^2 + 5s_3^2 + 4(-s_0s_3 + s_1s_2) \]

(1.7.11)

\[ x_5 = s_0^2 + s_1^2 - 5s_2^2 - 5s_3^2 \]
\[ x_6 = 2(s_0s_2 + s_1s_3) \]
(\text{where one or three } s_i \text{ are odd}).

The expressions in (1.7.11) constitute a solution of (1.7.8), in the case where \( x_3 \) and \( x_6 \) are even and \( x_4 \) and \( x_5 \) are odd, in independent parameters. Since the norm-form is not in a genus of one class, however, no claims can be made regarding uniqueness.

To study the solutions of

(1.7.12) \[ x_1^2 + x_2^2 = x_5^2 + 5x_6^2 \]

in integral parameters in the case that \( x_1 \) and \( x_6 \) are odd, and \( x_2 \) and \( x_5 \) are even, we consider the equation \(-5x_6^2 = -x_1^2 - x_2^2 + x_5^2\), and observe that the right-hand side
is the norm of \( Q = x_1i_1 + x_2i_2 + x_3i_3 \) in the ring of quaternions with the following multiplication: \( i_1^2 = i_2^2 = i_3^2 = 1, \ i_1i_2 = -i_2i_1 = i_3, \ i_2i_3 = -i_3i_2 = i_1, \) and \( i_3i_1 = -i_1i_3 = i_2. \)

We will proceed as above, writing \( Q = \sigma^*\tau\sigma, \) where

\[
N(\sigma) = N(u_0 + u_1i_1 + u_2i_2 + u_3i_3) = u_0^2 + u_1^2 - u_2^2 - u_3^2 = x_6, \quad \text{and}
\]

\[
N(\tau) = -5; \quad \text{for our purposes, it does not matter whether or not the norm-form} \ u_0^2 + u_3^2 - u_1^2 - u_2^2 \ \text{is in a genus of one class.}
\]

By Lemma 1.9, \( \tau \) is pure (since \( Q \) is pure): if we write \( \tau = ai_1 + bi_2 + ci_3, \) then

\[
Q = (u_0 - u_1i_1 - u_2i_2 - u_3i_3)(ai_1 + bi_2 + ci_3)(u_0 + u_1i_1 + u_2i_2 + u_3i_3);
\]

expanding and collecting coefficients of \( i_1, i_2, \) and \( i_3, \) we obtain

\[
x_1 = a(u_0^2 + u_2^2 - u_1^2 - u_3^2) + 2b(u_0u_3 - u_1u_2) + 2c(-u_0u_2 + u_1u_3)
\]

\[
x_2 = 2a(-u_0u_3 - u_1u_2) + b(u_0^2 + u_1^2 - u_2^2 - u_3^2) + 2c(u_0u_1 + u_2u_3)
\]

(1.7.13)

\[
x_5 = 2a(-u_0u_2 - u_1u_3) + 2b(u_0u_1 - u_2u_3) + c(u_0^2 + u_1^2 + u_2^2 + u_3^2)
\]

\[
x_6 = N(\sigma) = u_0^2 + u_3^2 - u_1^2 - u_2^2 \quad \text{(where one or three}
\]

\( u_1 \) \text{ are odd)}

Since \( x_1 \equiv a, \ x_2 \equiv b, \) and \( x_5 \equiv c \) \((\mod 2), \) we must have \( a \) odd, \( b \) and \( c \) even. For our purposes, it is enough to choose \( a = 1, \ b = 2, \ c = 0; \) this may not yield all solutions, but as we shall see, this will not matter. Using these choices, we obtain
\[ x_1 = u_0^2 + u_2^2 - u_1^2 - u_3^2 + 4(u_0 u_3 - u_1 u_2) \]
\[ x_2 = 2(-u_0 u_3 - u_1 u_2) + 2(u_0^2 + u_1^2 - u_2^2 - u_3^2) \]
\[(1.7.14)\]
\[ x_5 = 2(-u_0 u_2 - u_1 u_3) + 4(u_0 u_1 - u_2 u_3) \]
\[ x_6 = u_0^2 + u_3^2 - u_1^2 - u_2^2 \quad \text{(where one or three} \]
\[ u_1 \text{ are odd).} \]

This is a parametric solution of (1.7.12), in the case
that \( x_1 \) and \( x_6 \) are odd, and \( x_2 \) and \( x_5 \) are even. Again,
we make no claims of uniqueness.

To obtain solutions for (1.6.1), we first examine
the expressions for \( x_3 \) and \( x_4 \) in both (1.7.7) and
(1.7.11). These expressions in (1.7.11) can be made to
coincide with the corresponding expressions in (1.7.7) by
taking \( s_0 = -2t_1 + t_3, s_1 = t_0 - 2t_2, s_2 = t_2, s_3 = t_1 \).
Applying this transformation, which has determinant 1, to
the rest of (1.7.11), we obtain the expressions for
\( x_1, x_2, x_3, x_4, x_5 \) and \( x_6 \) given by (1.7.1). These expressions
make the following an identity, for \( x_1, x_4 \) and \( x_5 \) odd,\n\( x_2, x_3 \) and \( x_6 \) even:
\[(1.7.15)\]
\[ x_1^2 + x_2^2 = -x_3^2 + 5x_4^2 = x_5^2 + 5x_6^2 \]

Let \( p \) be a prime represented by \( x_1^2 + x_2^2 \) and by
\( x_5^2 + 5x_6^2 \); such representations are essentially unique.
Further, let \( p \) be such that the representation \( p = x_5^2 + 5x_6^2 \)
has $x_5$ odd and $x_6$ even. The expressions in (1.7.5) and (1.7.7) yield all solutions of (1.7.4), so they yield all solutions, except for changes in the signs of $x_3$ and $x_4$, of $p = x_1^2 + x_2^2 = -x_3^2 + 5x_4^2$. The expressions in (1.7.1) make (1.7.15) an identity, so they make (1.6.1) an identity, whenever $p$ is as above. By the uniqueness of representation of $p$ by $x_1^2 + x_2^2$ and $x_5^2 + 5x_6^2$, it follows that any solution of (1.6.1) is the unique solution. Hence we only need to know that we have (1) every parametric solution of (1.7.4), plus (2) expressions for $x_5$ and $x_6$ in terms of these parameters which make (1.7.15) an identity, in order to find a complete parametric solution of (1.6.1) when

$x_1, x_4, x_5$ are odd, and $x_2, x_3, x_6$ are even. As shown above, we know these facts: the point to notice is that we do not need the norm-form $s_0^2 + s_1^2 + 5s_2^2 + 5s_3^2$ to be in a genus of one class. We can pass over this obstacle, since we are only interested in representing primes.

Now we examine the expressions for $x_1$ and $x_2$ in both (1.7.5) and (1.7.14); the latter expressions are made to correspond to the former by taking $u_0 = t_0$, $u_1 = t_2$, $u_2 = -t_1$, and $u_3 = t_3$ (a transformation of determinant 1). Applying these transformations to the rest of (1.7.14) yields the expressions for $x_1, x_2, x_3, x_4, x_5$ and $x_6$ given by (1.7.2); these expressions make (1.7.15) an identity, in the case that $x_1, x_4$ and $x_6$ are odd, and $x_2, x_3$ and $x_5$ are even.
By a repetition of the argument in the paragraph preceding the last, we deduce that the expressions in (1.7.2) yield all solutions, except for changes in the sign of $x_3$ and $x_4$, of (1.6.1), in the case where $x_1$, $x_4$, and $x_6$ are odd, $x_2$, $x_3$, and $x_5$ are even, and $p$ is a prime represented by both $x_1^2 + x_2^2$ and $x_5^2 + 5x_6^2$.

This finishes the procedure for obtaining all integral parametric solutions of (1.6.1), in the cases cited above, and completes the proof of Theorem 1.7.

Q.E.D.

In the statement and proof of the following representation theorem, the letters $x_1$ through $x_6$ refer to the expressions in (1.6.1).

THEOREM 1.10. Let $(p|5) = 1$, $p \equiv 1 \pmod{4}$, and $f_1 = [1,0,-5p]$. Then:

(a) If $p = x_5^2 + 5x_6^2$, with $x_5$ even, then $f_1$ never represents $-1$; it represents $5$ or $-5$, according as $(p|5)_4 = 1$ or $-1$.

(b) If $p = a^2 + 25b^2$, with $a$ even, then $f_1$ never represents $-5$; it represents $5$ or $-1$, according as $(p|5)_4 = 1$ or $-1$.

(c) If $(p|5)_4 = -1$, then $f_1$ never represents $5$; it represents $-1$ or $-5$ according as $p = x_5^2 + 5x_6^2$ with $x_5$ odd,
or \( p = x_5^2 + 5x_6^2 \) with \( x_5 \) even.

(d) If \( (p|5)_4 = 1 \), then \( f_1 \) represents 5 if \( p = x_5^2 + 5x_6^2 \) with \( x_5 \) even; otherwise, any of the possibilities that \( f_1 \) represents \(-1, 5, \) or \(-5\) can occur.

**NOTE.** It is clear that \( (p|5)_4 = 1 \) or \(-1\) implies that 
\( p \equiv 1 \) or \( 9 \) (mod 20), respectively; the reason that the Legendre symbols are used is this: In later theorems in which 5 is replaced by a larger prime, it is much more elegant to say that, for instance, \( (p|29)_4 = 1 \), than to say that \( p \equiv 1,7,16,20,23,24 \) or \( 25 \) (mod 29). In short, it generalizes more easily.

Proof of Theorem 1.10 is based on the following lemmas:

**LEMMA 1.11.** (a) If \( x_5 \) is even, then \((x_1 + x_5|5) = 0\) or 1, and \((x_2 + x_5|5) = 0\) or \(-1\). (b) If \( x_5 \) is odd, then 
\((x_1 + x_5|5) = 0\) or \(-1\), and \((x_2 + x_5|5) = 0\) or 1.

**PROOF.** (a) If \( x_5 \) is even, we refer to the expressions in (1.7.2). Then 
\[ x_1 + x_5 = t_0^2 + t_1^2 - t_2^2 - t_3^2 + 4(t_0 t_3 + t_1 t_2) + 2(t_0 t_1 - t_2 t_3) + 4(t_0 t_2 + t_1 t_3) \]
\[ + (t_0 + t_1)^2 + 4(t_0 + t_1)(t_2 + t_3) - (t_2 + t_3)^2 \]
\[ = (t_0 + t_1)^2 + 4(t_0 + t_1)(t_2 + t_3) + 4(t_2 + t_3)^2 \pmod{5} \]
\[ = (t_0 + t_1 + 2(t_2 + t_3))^2 \pmod{5}. \]
Hence \((x_1 + x_5|5) = 0\) or 1.
Also, \( x_2 + x_5 = 2(-t_0 t_3 + t_1 t_2 + 2(t_0^2 + t_2^2 - t_1^2 - t_3^2) + 2(t_0 t_1 - t_2 t_3) \\
+ 4(t_0 t_2 + t_1 t_3) = 2((t_0 + t_2)^2 - (t_1 - t_3)^2 + (t_0 + t_2)(t_1 - t_3)) \\
\equiv 2((t_0 + t_2) - 2(t_1 - t_3))^2 \pmod{5} \). Hence \( (x_2 + x_5 | 5) = 0 \) or \( (2 | 5) = 0 \) or \(-1\).

(b) If \( x_5 \) is odd, we refer to the expressions in (1.7.1). Then \( x_1 + x_5 = t_0^2 + t_1^2 - t_2^2 - t_3^2 \\
+ 4(-t_0 t_2 + t_1 t_3) + t_0^2 + t_3^2 - t_1^2 - t_2^2 - 4(t_0 t_2 + t_1 t_3) \\
= 2(t_0^2 - t_2^2 - 4t_0 t_2) = 2(t_0 - 2t_2)^2 \pmod{5} \).

Hence \( (x_1 + x_5 | 5) = 0 \) or \( (2 | 5) = 0 \) or \(-1\). Also,
\( x_2 + x_5 = t_0^2 + t_3^2 - t_1^2 - t_2^2 + 4(-t_0 t_2 + t_1 t_3) + 2(-t_0 t_3 + t_1 t_2) \\
+ 4(t_0 t_1 + t_2 t_3) = (t_0 - t_3)^2 - (t_1 - t_2)^2 + 4(t_0 - t_3)(t_1 - t_2) \\
= ((t_0 - t_3) + 2(t_1 - t_2))^2 \pmod{5} \). Hence \( (x_2 + x_5 | 5) = 0 \) or \(1\).

Q.E.D.

**Lemma 1.12.** (a) Let \((p | 5)_4 = 1\). Then \( x_5 \) is even if and only if \( 5 \) divides \( x_1 \). (b) Let \((p | 5)_4 = -1\). Then \( x_5 \) is even if and only if \( 5 \) divides \( x_2 \).

**Proof.** We first make the following observations: if \((p | 5) = 1\), then \( p \) is represented by a form in the principal genus of determinant \( 5 \), i.e. by \( x_5^2 + 5x_6^2 \); also, if \((p | 5) = 1\), and \( p = x_1^2 + x_2^2 \) with \( x_1 \) odd, \( x_2 \) even, then either \( x_1 \) or \( x_2 \) is divisible by \( 5 \). For, if \( p = x_1^2 + x_2^2 \equiv 1 \) or \( 9 \pmod{20} \), then \( p = 1 \) implies either
$x_1^2 = 5$, $x_2^2 = 16$, or $x_1^2 = 1$, $x_2^2 = 0 \pmod{20}$, and $p = 9$ implies either $x_1^2 = 5$, $x_2^2 = 4$, or $x_1^2 = 9$, $x_2^2 = 0 \pmod{20}$.

(a) Let $(p|5)_4 = 1$. If $x_5$ is even, then $(x_2 + x_5|5) = 0$ or $-1$. If $x_1 \neq 0 \pmod{5}$, then $x_2 \equiv 0 \pmod{5}$, so that $(x_5|5) = 0$ or $-1$. Since $(x_5|5) = 1$, $(x_5|5) = -1$. Hence $p = x_5^2 \pmod{5}$ and $(x_5^2|5)_4 = -1$ imply $(p|5)_4 = -1$, a contradiction. Hence $x_1 \equiv 0 \pmod{5}$. Conversely, if $x_1 \equiv 0 \pmod{5}$, then $(x_1 + x_5|5) = (x_5|5)$. If $x_5$ were odd, then (as $(x_5|5) = 1$) we would have $(p|5)_4 = -1$, which would contradict $(p|5)_4 = 1$, as before. Hence $x_5$ is even.

(b) Suppose $(p|5)_4 = -1$, and $x_5$ is even. If $x_2 \neq 0 \pmod{5}$, then $x_1 \equiv 0 \pmod{5}$; hence $(x_5|5) = (x_1 + x_5|5) = 1$ (since $(x_5|5) = 1$). This implies that $(p|5)_4 = 1$, a contradiction, so that $x_2 \equiv 0 \pmod{5}$. Conversely, if $x_2 \equiv 0 \pmod{5}$, then $(x_2 + x_5|5) = (x_5|5)$. If $x_5$ were odd, then $(x_5|5) = 1$ implies $(x_5|5) = 1$, so that, as above, $(p|5)_4 = 1$, a contradiction. Hence $x_5$ is even.

Q.E.D.

**Lemma 1.13.** If either (a) $(p|5)_4 = 1$ and $x_5 \equiv 0 \pmod{5}$, or (b) $(p|5)_4 = -1$ and $x_2 \equiv 0 \pmod{5}$, then $(x_1 + 2x_2|5) = -1$, for either choice of sign.

**Proof.** Suppose $(p|5)_4 = 1$ and $x_1 \equiv 0 \pmod{5}$. Then

\[ p = x_1^2 + x_2^2 \equiv 5 + x_2^2 \equiv 1 \pmod{20} \]

implies $x_2^2 \equiv 16 \pmod{20}$, $x_2 \equiv \pm 4 \pmod{10}$. Hence $(x_1 + 2x_2|5) = (5 + 8|5) = (\pm 3|5) = -1$. 


On the other hand, if $(p|5)_4 = -1$ and $x_2 \equiv 0 \pmod{5}$, then 
$p = x_1^2 + x_2^2 = x_1^2 = 9 \pmod{20}$ implies $x_1 \equiv \pm 3 \pmod{10}$.
Hence $(x_1 \pm 2x_2|5) = (\pm 3|5) = -1$.

Q.E.D.

**Lemma 1.14.** If $(p|5)_4 = -1$, then $(x_3|5) = 1$. Hence if $(p|5)_4 = -1$, then $f_1$ does not represent 5.

**Proof.** If $(p|5)_4 = -1$, and $p = -x_3^2 + 5x_4^2 = -x_3^2 \pmod{5}$, then $-1 = (p|5)_4 = (-x_3^2|5)_4 = (4x_3^2|5)_4 = (2x_3|5)$
$= (2|5)(x_3|5) = -(x_3|5)$. Hence $(x_3|5) = 1$. This does not satisfy the conditions (b) in Theorem 1.6 for $f_1$ to represent 5, and the conclusion follows.

Q.E.D.

**Proof of Theorem 1.10.**

(a) Let $p = x_5^2 + 5x_6^2$, with $x_5$ even. If $(p|5)_4 = 1$, then $x_1 \equiv 0 \pmod{5}$, and if $(p|5)_4 = -1$, then $x_2 \equiv 0 \pmod{5}$ (by Lemma 1.12). By Lemma 1.13, $(x_1 \pm 2x_2|5) = -1$; this violates conditions (a) in Theorem 1.6 for $f_1$ to represent -1. By Lemma 1.14, if $(p|5)_4 = -1$, $f_1$ never represents 5; hence, $f_1$ represents -5. Since $x_5$ is even, this violates conditions (c) in Theorem 1.6 for $f_1$ to represent -5 if $(p|5)_4 = 1$. Hence, $f_1$ represents 5 if $(p|5)_4 = 1$, and -5 if $(p|5)_4 = -1$.

(b) If $p = a^2 + 25b^2$, with $a$ even, then $p = x_1^2 + x_2^2$,
with \( x_1 \equiv 0 \pmod{5} \). If \((p|5)_4 = 1\), then \( x_5 \) is even (by Lemma 1.12), so \( f_1 \) does not represent \(-5\). (part (a)). If \((p|5)_4 = -1\), then \( x_5 \) is odd (Lemma 1.12), so \( f_1 \) does not represent \(-5\) (Theorem 1.6 (c) is violated). If \( p|5 \), then by Lemma 1.23, \((x_1 + 2x_2|5) = -1\), so that \( f_1 \) does not represent \(-1\). Hence \((p|5)_4 = 1\) implies \( f_1 \) represents \(5\); if \((p|5)_4 = -1\), then \( f_1 \) represents \(-1\), since \( f_1 \) never represents \(5\) (Lemma 1.14). This proves (b).

(c) If \((p|5)_4 = -1\), then \( f_1 \) never represents \(5\) (by Lemma 1.14). If \( x_2 \equiv 0 \pmod{5} \) (equivalently, if \( x_5 \) is even), then \( f_1 \) represents \(-5\) (part a) above). If \( x_1 \equiv 0 \pmod{5} \) (equivalently, if \( x_5 \) is odd) then \( f_1 \) represents \(-1\) (part (b) above).

(d) If \((p|5)_4 = 1\) and \( x_5 \) is even, then \( f_1 \) represents \(5\) (by (a) above); if \( x_5 \) is odd, the following are examples of \( f_1 \) representing each of \(-1, 5, -5\) (determined by computing the chain of reduced forms in the class of \( f_1 \)): if \( p = 101 \), \( f_1 \) represents \(5\); if \( p = 181 \), \( f_1 \) represents \(-5\); if \( p = 461 \), \( f_1 \) represents \(-1\) (note that \( 101 = 9^2 + 5 \cdot 2^2 \), \( 181 = 1^2 + 5 \cdot 6^2 \), and \( 461 = 21^2 + 5 \cdot 2^2 \)).

Q.E.D.
In this chapter, we generalize several theorems from Chapter I. We generalize Theorem 1.6, proving several theorems dealing with necessary conditions that the form \( f_1 = [1,0,-pq] \) represent \(-1\), \( q \), or \(-q\) (in the discussion, \( p \) and \( q \) denote primes of the form \( 4n + 1 \) for which \((p|q) = 1\)). We generalize Theorem 1.7, replacing 5 by an arbitrary prime \( q \), and express the solutions of the resulting systems of Diophantine equations by means of independent integral parameters. Finally, we prove a representation theorem which resembles Theorem 1.10, in the case \( q = 13 \).

**Theorem 2.1.** Let \( q = a^2 + b^2 \), with \( a \) odd, \( b \) even. If \( f_1 \) represents \(-1\), then there exist integers \( x_1 \) odd, \( x_2 \) even such that \( p = x_1^2 + x_2^2 \) and such that either

(a) \( (ax_1 + bx_2 | q) = 1 \) and \( (bx_1 - ax_2 | q) = (2|q) \), or

(b) \( (ax_1 - bx_2 | q) = 1 \) and \( (bx_1 + ax_2 | q) = (2|q) \).

**Proof.** If there exist integers \( u,v \) (we may assume \( v > 0 \)) such that \( u^2 - pqv^2 = -1 \), then the form \( g = [pqv,2u,v] \) has determinant 1. Since \( v > 0 \), \( g \sim [1,0,1] \). We then have the following Cantor diagram

\[
[1,0,1] \xrightarrow{T} [pqv,2u,v] = g
\]

\[
h = [z_1,2z_2,z] \xleftarrow{T'} [1,0,-qp] = f_1
\]
By Proposition 1.5, \( z_1 + z = 0 \); hence \( z = -z_1 \), and there is
a form \( h = [z_1, 2z_2, -z_1] \) in the class of \( f_1 \). Comparing
determinants, we have \( qp = z_1^2 + z_2^2 \); \( h \) is primitive, so \( z_1 \)
is odd and \( z_2 \) is even. Now \( p \) is a prime \( \equiv 1 \pmod{4} \), so
there exist integers \( x_1 \) odd, \( x_2 \) even such that \( p = x_1^2 + x_2^2 \),
the \( x_i \) being unique up to choice of sign. Hence
\[
qp = (a^2 + b^2)(x_1^2 + x_2^2) = z_1^2 + z_2^2
\]
in that order; \( h \) is in
the genus of \( f_1 \), and primitively represents \( z_1 \) and \( 2z_2 \), so
\( (z_1|q) = (2z_2|q) = 1 \). Hence, either \( (ax_1 + bx_2|q) = 1 \), or
\( (ax_1 - bx_2|q) = 1 \), or \( (bx_1 + ax_2|q) = 1 \).
From this follows the desired conclusion.

Q.E.D.

**Theorem 2.2.** Suppose there exist \( u, v \) \((v > 0)\) such that
\( u^2 - qpv^2 = q \); then the form \( g = [qpv, 2u, v] \) has determinant
\( -q \) and g.c.d. 2. Suppose \( g \sim [2, 2, -\frac{1}{2}(q-1)] \). If either
(a) \( (2|q) = 1 \), or (b) \( (2|q) = -1 \) and the least positive
solution \( s_1 \) of \( r^2 - qs^2 = 4 \) is odd, then there exist integers
\( x_3 \) even, \( x_4 \) odd such that \( p = -x_3^2 + qx_4^2 \) and \( (x_3|q) = 2 \).

**Proof.** To see that the form \( g = [qpv, 2u, v] \) has g.c.d. 2,
observe that \( 1 = q = u^2 - pqa^2 = u^2 - v^2 \pmod{4} \); hence \( u \)
must be odd and \( v \) must be even. If \( g \) is equivalent to
\[ [2, 2, -\frac{1}{2}(q-1)] \], then we form the following Cantor diagram:

\[
[2, 2, -\frac{1}{2}(q-1)] \xrightarrow{T} [qpv, 2u, v] \]

\[
h = [x, 2y, c] \xleftarrow{T'} [1, 0, -qp] \]
By Proposition 1.5, \( 2x + 2y - \frac{1}{2}(q-1)c = 0 \), so that
\[
x = \frac{1}{4}(q-1)c - y \quad \text{(recall that } q \equiv 1 \pmod{4} \text{ implies that} \ \frac{1}{4}(q-1) \text{ is an integer). Hence there is a form}
\]
\[h = \left[ \frac{1}{4}(q-1)c - y, 2y, c \right] \sim f_1;\] comparing determinants, we find that \( qp = y^2 + cy - \frac{1}{4}(q-1)c^2 \). There are two cases to consider:

(a) \( (2|q) = 1 \). Then \( q \equiv 1 \pmod{8} \), so that \( \frac{1}{4}(q-1) \) is even, and hence \( y \) is odd (if not, \( pq \) would be even); we also deduce that \( c \) is even. Writing \( c = 2x_3 \), we obtain
\[
qp = y^2 + 2x_3y - (q-1)x_3^2 = (y + x_3)^2 - qx_3^2.
\]
Hence \( y + x_3 = qx_4 \), and we obtain \( p = -x_3^2 + qx_4^2 \equiv -x_3^2 + x_4^2 \pmod{4} \); this implies that \( x_3^2 + p = x_3^2 + 1 = x_4 \pmod{4} \), so \( x_3 \) is even and \( x_4 \) is odd. Finally, since \( h \) is in the genus of \( f_1 \), we obtain
\[
1 = (c|q) = (2x_3|q); \text{ hence } (x_3|q) = (2|q).
\]

(b) \( (2|q) = -1 \), and the least positive solution \( s_1 \) of \( r^2 - qs_1^2 = 4 \) is odd. For some \( r_1 \), we have \( x_1^2 - qs_1^2 = 4 \); there are two subcases to consider:

(1) \( c \) is even. Then we write \( c = 2x_3 \), and proceed as in Case (a).

(2) \( c \) is odd. Now every automorph of the form
\[\left[ 1, 1, (1-q/4) \right] \] looks like
\[
U = \begin{bmatrix}
\frac{(r+s)/2}{2} & \frac{(q-1)s/4}{4} \\
\frac{s}{s} & \frac{(r+s)/2}{2}
\end{bmatrix}
\]
(see [5, p. 25]), where \( r^2 - qs^2 = 4 \); furthermore, exactly one of \((r_1 + s_1)/2, (r_1 - s_1)/2 \) is odd. We may assume, without loss, that \((r_1 + s_1)/2 \) is odd.

If in the equation \( qp = y^2 + cy - (q-1)c^2/4 \), \( y \) is odd, then we may replace \( y \) by \((r_1 - s_1)y/2 + (q-1)s_1c/4 = y_1 \) and \( c \) by \( s_1y + (r_1 + s_1)c/2 = c_1 \). This yields the equation \( qp = y_1^2 + c_1y_1 - (q-1)c_1^2/4 \), in which \( c_1 \) is even; we then proceed as in subcase (1). If \( y \) is even, then we may replace \( y \) by \((r_1 + s_1)y/2 + (q-1)s_1c/4 = y_1 \) and \( c \) by \( s_1y + (r_1 - s_1)c/2 = c_1 \); this yields the equation \( qp = y_1^2 + c_1y_1 - (q-1)c_1^2/4 \) with \( c_1 \) even, and we may proceed as in subcase (1). In either subcase, we deduce that \( p = -x_3^2 + qx_4^2 \), where \( x_3 \) is even, \( x_4 \) is odd, and \((x_3|q) = (2|q)\).

Q.E.D.

REMARK. The hypotheses for the preceding theorem are not as strong as they appear. For instance, the primes \( \equiv 1 (\text{mod } 4) \) less than 100 satisfying these hypotheses include 5, 13, 17, 29, 41, 53, 61, 73, 89, and 97; only 37 is excluded.

COROLLARY 2.2.1. If \( p \) and \( q \) satisfy the hypotheses of Theorem 2.2, then \((p|q)_4 = 1\). Hence if there is only one class of forms of determinant \( q \) and \( \text{g.d.d.2} \), and if either (a) \((2|q) = 1\), or (b) \((2|q) = -1\) and the least positive solution \( s_1 \) of \( r^2 - qs^2 = 4 \) is odd, then \((p|q)_4 = -1\).
implies that \( f_1 \) does not represent \( q \).

**PROOF.** If \( p \) and \( q \) satisfy the hypotheses of Theorem 2.2, then there exist \( x_3, x_4 \) such that \( p = -x_3^2 + qx_4^2 \), and 

\[(x_3|q) = (2|q). \]

Hence \( p \equiv -x_3^2 \pmod{q} \) implies that 

\[(p|q)_4 = (-x_3^2|q)_4 = (-1|q)_4(x_3^2|q)_4 = (-1|q)_4(x_3|q)_4 = (-1|q)_4(2|q). \]

Now, for \( q \equiv 1 \pmod{4} \), \((1|q)_4 = 1 \) or \(-1 \) according as \( q \equiv 1 \) or \( 5 \pmod{8} \). Hence, if \( q \equiv 1 \pmod{4} \), then 

\[(-1|q)_4 = (2|q), \]

so that \((p|q)_4 = 1\).

The second statement is simply a contrapositive of the first statement.

Q.E.D.

**THEOREM 2.3.** Suppose \( u^2 - qpv^2 = -q \), where \( v > 0 \). Let 

\[ g = [qp,v,2u,v], \]

\[ g_1 = [1,0,q], \]

and 

\[ g_2 = [2,2,(q+1)/2]. \]

Then:

(a) If \( g \sim g_1 \), then there exist \( x_5 \) odd, \( x_6 \) even such that 

\[ p = x_5^2 + qx_6^2, \]

\[ (x_5|q) = 1, \]

and 

\[ (p|q)_4 = 1. \]

(b) If \( g \sim g_2 \), then there exist \( x_5 \) even, \( x_6 \) odd such that 

\[ p = x_5^2 + qx_6^2, \]

\[ (x_5|q) = (2|q), \]

and 

\[ (p|q)_4 = (2|q). \]

**PROOF.** (a) If \( g \sim g_1 \), then we form the following Cantor diagram:

\[
\begin{array}{c}
[1,0,q] \xrightarrow{T} [qp,v,2u,v] \\
[a,2b,x_5] \xrightarrow{T'} [1,0,-qp]
\end{array}
\]
By Proposition 1.5, \( a + qx_5 = 0 \), so \( a = -qx_5 \), and there is a form \( h = [-qx_5, 2b, x_5] \) in the class of \( f_1 \). Comparing determinants, we find that \( qp = b^2 + qx_5^2 \); since \( h \) is primitive, \( x_5 \) is odd, so \( b \) is even. Since \( q \mid b \), we write \( b = qx_6 \), and \( p = x_5^2 + qx_6^2 \), where \( x_5 \) is odd and \( x_6 \) is even. Since \( h \) is in the genus of \( f_1 \), \( (x_5 \mid q) = 1 \). Hence \( (x_5^2 \mid q)^4 = 1 \), and we deduce, from the congruence \( p \equiv x_5^2 \pmod{q} \), that \( (p \mid q)^4 = 1 \).

(b) If \( g \sim g_2 \), we form the following Cantor diagram:

\[
\begin{align*}
[2, 2, (q+1)/2] & \xrightarrow{T} [qp, 2u, v] \\
[a, 2b, c] & \xleftarrow{T'} [1, 0, -qp]
\end{align*}
\]

By Proposition 1.5, \( 2a + 2b + (q+1)c/2 = 0 \). Since \( q \equiv 1 \pmod{4} \), \( (q+1)/2 \) is odd; hence \( c \) is even. Writing \( c = 2x_5 \), we obtain \( a = -b - (q+1)x_5/2 \), and there is a form \( h = [-b - (q+1)x_5/2, 2b, 2x_5] \) in the class of \( f_1 \). Comparing determinants, we have \( qp = b^2 + 2bx_5 + (q+1)x_5^2 \) (hence \( b \) is odd, so \( x_5 \) is even --- recall \( h \) is primitive). Hence \( p = (b + x_5)^2 + qx_5^2 \); writing \( b + x_5 = qx_6 \), we have \( p = x_5^2 + qx_6^2 \), where \( x_5 \) is even (and hence \( x_6 \) is odd). Since \( h \) is in the genus of \( f_1 \), we must have \( 1 = (c \mid q) = (2x_5 \mid q) \), so that \( (x_5 \mid q) = (2 \mid q) \). Finally, \( p \equiv x_5^2 \pmod{q} \) implies that \( (p \mid q)^4 = (x_5^2 \mid q)^4 = (x_5 \mid q) = (2 \mid q) \).

Q.E.D.
We now prove a generalization of Theorem 1.7.

**THEOREM 2.4.** Let \( q \) be a prime of the form \( 4n + 1 \). Then all solutions of the system of equations

\[
(2.4.1) \quad p = x_1^2 + x_2^2 = -x_3^2 + qx_4^2 = x_5^2 + qx_6^2
\]

can be expressed in the form of representations of the \( x_i \) by independent integer-valued parameters, in the case where \( x_1 \) and \( x_4 \) are odd, \( x_2 \) and \( x_3 \) are even, \( x_5 \) and \( x_6 \) have opposite parity, and \( p \) is a prime representable by the forms \( x_1^2 + x_2^2 \) and \( x_5^2 + qx_6^2 \).

**PROOF.** First we study the equation

\[
(2.4.2) \quad x_1^2 + x_2^2 = -x_3^2 + qx_4^2
\]

in the case that \( x_1 \) and \( x_4 \) are odd, and \( x_2 \) and \( x_3 \) are even. To do this, we study the solutions of \( qx_4^2 = x_1^2 + x_2^2 + x_3^2 \), and observe that \( Q = x_1i_1 + x_2i_2 + x_3i_3 \) is a quaternion in the Lipschitz ring (see Theorem 1.7) of norm \( qx_4^2 \). As before, since the norm form \( t_0^2 + t_1^2 + t_2^2 + t_3^2 \) is in a genus of one class, we may apply Lemma 1.8, and write \( Q = \sigma^* \tau \sigma \), where \( N(\sigma) = x_4 \), \( N(\tau) = q \), and \( \tau \) is pure; as a further consequence of Lemma 1.8, \( \sigma \) and \( \tau \) are unique up to unit factors. If we write \( \sigma = t_0 + t_1i_1 + t_2i_2 + t_3i_3 \) and \( \tau = a_1i_1 + b_2i_2 + c_3i_3 \), then

\[
Q = x_1i_1 + x_2i_2 + x_3i_3 = (t_0 - t_1i_1 - t_2i_2 - t_3i_3)(a_1i_1 + b_2i_2 + c_3i_3) (t_0 + t_1i_1 + t_2i_2 + t_3i_3);
\]

expanding and collecting coefficients of \( i_1, i_2, \) and \( i_3 \) yields
\[ x_1 = a(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2b(t_0 t_3 + t_1 t_2) + 2c(-t_0 t_2 + t_1 t_3) \]
\[ x_2 = 2a(-t_0 t_3 + t_1 t_2) + b(t_0^2 + t_2^2 - t_1^2 - t_3^2) + 2c(t_0 t_1 + t_2 t_3) \]

(2.4.3)

\[ x_3 = 2a(t_0 t_2 + t_1 t_3) + 2b(-t_0 t_1 + t_2 t_3) + c(t_0^2 + t_3^2 - t_1^2 - t_2^2) \]
\[ x_4 = N(\sigma) = t_0^2 + t_1^2 + t_2^2 + t_3^2 \]

Since \( q \) is a prime \( \equiv 1 \) (mod 4), we may write \( q = A^2 + B^2 \), where \( A \) is odd, \( B \) is even, and both are positive. We observe that \( x_1 \equiv a \), \( x_2 \equiv b \), and \( x_3 \equiv c \) (mod 2); hence \( a \) is odd, and \( b \) and \( c \) are even. Repeating the argument at this stage of the proof of Theorem 1.7, we observe that there are exactly two choices for \( \tau \) which yield essentially different parametric solutions of (2.4.2); these are \( \tau_1 = A_1 t_1 + B_2 \) and \( \tau_2 = A_1 t_1 + B_2 \). If we let \( \tau = \tau_1 \), we obtain:

\[ x_1 = A(t_0^2 + t_1^2 + t_2^2 + t_3^2) + 2B(t_0 t_3 + t_1 t_2) \]
\[ x_2 = 2A(-t_0 t_3 + t_1 t_2) + B(t_0^2 + t_2^2 - t_1^2 - t_3^2) \]

(2.4.4)

\[ x_3 = 2A(t_0 t_2 + t_1 t_3) + 2B(-t_0 t_1 + t_2 t_3) \]
\[ x_4 = t_0^2 + t_1^2 + t_2^2 + t_3^2 \] (where one or three of the \( t_i \) are odd)

If we let \( \tau = \tau_2 \), we obtain:
\[ x_1 = A(t_0^2 + t_1^2 - t_2^2 - t_2^2) + 2B(-t_0 t_2 + t_1 t_3) \]
\[ x_2 = 2A(-t_0 t_3 + t_1 t_2) + 2B(t_0 t_1 + t_2 t_3) \]

\[(2.4.5)\]
\[ x_3 = 2A(t_0 t_2 + t_1 t_3) + B(t_0^2 + t_3^2 - t_1^2 - t_2^2) \]
\[ x_4 = t_0^2 + t_1^2 + t_2^2 + t_3^2 \] (when one or three of the \( t_1 \) are odd).

By virtue of the unique factorization properties of this quaternion ring guaranteed by Lemma 1.8, the expressions in \((2.4.4)\) and \((2.4.5)\) yield all solutions (as before, except for changes of the signs of \( x_3 \) and \( x_4 \)) of \((2.4.2)\) in independent parameters, in the case that \( x_1 \) and \( x_4 \) are odd, and \( x_2 \) and \( x_3 \) are even.

To study the solutions of
\[(2.4.6)\]
\[ x_1^2 + x_2^2 = x_5^2 + q x_6^2 \]
in integral parameters in the case that \( x_1 \) and \( x_6 \) are odd, and \( x_2 \) and \( x_5 \) are even, we consider the equation \( q x_6^2 = -x_1^2 - x_2^2 + x_5^2 \), and observe that the right-hand side is the norm of \( Q = x_1 i_1 + x_2 i_2 + x_5 i_3 \) in the ring of quaternions with the following multiplication defined: \( i_1^2 = i_2^2 = -i_3^2 = 1; \)
\( i_1 i_2 = -i_2 i_1 = -i_3; i_2 i_3 = -i_3 i_2 = i_1; i_3 i_1 = -i_1 i_3 = i_2. \)
Again, as in the proof of Theorem 1.7, we will show that it does not matter whether the norm-form \( u_0^2 + u_3^2 - u_1^2 - u_2^2 \) is in a genus of one class. For our purposes, it will suffice
to consider solutions of (2.4.6) obtained by employing previous techniques, i.e. by writing $Q = \sigma^*r\sigma$, where $N(\sigma) = x_6$ and $N(\tau) = -q$. Now $Q$ is pure, so $\tau$ is also:

writing \( \tau = a_1i_1 + b_1i_2 + c_1i_3 \), we have

\[
Q = (u_0u_1 - u_2u_3)(a_1b_1c_1)(u_0u_1 + u_2u_3) = x_1i_1 + x_2i_2 + x_3i_3.
\]

Expanding and collecting coefficients of \( i_1, i_2 \), and \( i_3 \), we obtain:

\[
x_1 = a(u_0^2 - u_2^2 - u_1^2 + u_3^2) + 2b(u_0u_3 - u_1u_2) + 2c(-u_0u_2 + u_1u_3)
\]

\[
x_2 = 2a(-u_0u_3u_1 - u_1u_2) + b(u_0^2u_1^2 - u_2^2) + 2c(u_0u_1 + u_2u_3)
\]

(2.4.7)

\[
x_5 = 2a(-u_0u_2 - u_1u_3) + 2b(u_0u_1 - u_2u_3) + c(u_0^2 + u_1^2 + u_2^2 + u_3^2)
\]

\[
x_6 = N(\sigma) = u_0^2 + u_3^2 - u_1^2 - u_2^2 \text{ (where one or three of the } u_i \text{ are odd).}
\]

We observe that, in order for \( x_1 \) to be odd, \( x_6 \) must be odd, so that the restrictions on the \( u_i \) are necessary.

Since \( x_1 = a \), \( x_2 = b \), and \( x_5 = c \text{(mod 2)} \), we know that \( a \) must be odd, \( b \) and \( c \) must be even. For our purposes, the choices \( a = A \), \( b = B \), \( c = 0 \) (\( A \) and \( B \) as above) will suffice; as will be made clear, we need make no other choice. Using \( \tau = Ai_1 + Bi_2 \), we obtain:

\[
x_1 = A(u_0^2 + u_2^2 - u_1^2 - u_3^2) + 2B(u_0u_3 - u_1u_2)
\]

\[
x_2 = 2A(-u_0u_3 - u_1u_2) + B(u_0^2 + u_1^2 - u_2^2 - u_3^2)
\]
\[(2.4.8)\]

\[x_5 = 2A(-u_0u_2 - u_1u_3) + 2B(u_0u_1 - u_2u_3)\]

\[x_6 = u_0^2 + u_3^2 - u_1^2 - u_2^2\] (where one or three of the \(u_i\) are odd).

The expressions in \((2.4.8)\) comprise a parametric solution to \((2.4.6)\), in the case where \(x_1\) and \(x_6\) are odd, \(x_2\) and \(x_5\) are even. As before, we make no claims of uniqueness or completeness.

To obtain solutions for \((2.4.1)\), we first examine the expressions for \(x_1\) and \(x_2\) in both \((2.4.4)\) and \((2.4.8)\). The latter expressions can be made to coincide with the former expressions by taking \(u_0 = t_0, u_1 = t_2, u_2 = -t_1, u_3 = t_3\). Applying this unimodular transformation to the rest of \((2.4.8)\), we obtain the following:

\[x_1 = A(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2B(t_0t_3 + t_1t_2)\]

\[x_2 = 2A(-t_0t_3 + t_1t_2) + B(t_0^2 + t_2^2 - t_1^2 - t_3^2)\]

\[x_3 = 2A(t_0t_2 + t_1t_3) + 2B(-t_0t_1 + t_2t_3)\]

\[(2.4.9)\]

\[x_4 = t_0^2 + t_1^2 + t_2^2 + t_3^2\]

\[x_5 = 2A(t_0t_1 - t_2t_3) + 2B(t_0t_2 + t_1t_3)\]

\[x_6 = t_0^2 + t_3^2 - t_1^2 - t_2^2\] (where one or three of the \(t_i\) are odd).
These expressions make the following an identity, in the case that $x_1, x_4,$ and $x_6$ are odd, and $x_2, x_3$ and $x_5$ are even.

\[(2.4.10) \quad x_1^2 + x_2^2 = -x_3^2 + qx_4^2 = x_5^2 + qx_6^2\]

Let $p$ be a prime representable by $x_1^2 + x_2^2$ and by $x_5^2 + qx_6^2$ for which $x_1$ and $x_6$ are odd, and $x_2$ and $x_5$ are even. Except for sign changes, such expressions are unique. Since the expressions for $x_1, x_2, x_3$ and $x_4$ in (2.4.9) yield all solutions of (2.4.2) with the given parity restrictions, and since the expressions for $x_1$ through $x_6$ in (2.4.9) yield an identity for (2.4.10), it follows that if $p$ is a prime as above, all solutions of (2.4.1) in the case $x_1, x_4, x_6$ odd, $x_2, x_3, x_5$ even are given by the expressions (2.4.9). We may do this because of two facts: the norm-form $x_4$ is in a genus of one class, and the representations of a prime by a sum of two squares and by a square plus a prime multiple of a square are essentially unique. (This is a repetition of the argument in Theorem 1.7.)

At this point, we would like to proceed in the following manner. As in Theorem 1.7, study the solutions of

\[(2.4.11) \quad -x_3^2 + qx_4^2 = x_5^2 + qx_6^2\]

in the case that $x_3$ and $x_6$ are even, and $x_4$ and $x_5$ are odd. Then compare the expressions for $x_3$ and $x_4$ in both such a
set of expressions and (2.4.5), match them by applying a
unimodular transformation to one of these sets of expressions,

obtain expressions which make (2.4.10) an identity, and
proceed as above. Unfortunately, obtaining expressions for
the solutions of (2.4.11) would not be beneficial, for we
could not find the aforementioned unimodular transformation,
in general, even though it is possible to do this for any
specific q. However, we are able to guess at the "right"
expressions for x_5 and x_6, by examining several special
cases; the following make (2.4.10) an identity, in the case
where x_1, x_4 and x_5 are odd, and x_2, x_3 and x_6 are even:

\[
\begin{align*}
x_1 &= A(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2B(-t_0 t_2 + t_1 t_3) \\
x_2 &= 2A(-t_0 t_3 + t_1 t_2) + 2B(t_0 t_1 + t_2 t_3) \\
x_3 &= 2A(t_0^2 + t_1^2 + t_3^2) + B(t_0^2 + t_3^2 - t_1^2 - t_2^2) \\
x_4 &= t_0^2 + t_1^2 + t_2^2 + t_3^2 \\
x_5 &= A(t_0^2 + t_3^2 - t_1^2 - t_2^2) + 2B(-t_0 t_2 - t_1 t_3) \\
x_6 &= 2(-t_0 t_1 + t_2 t_3) \quad \text{(where one or three of} \\
& \quad \text{the t_i are odd).}
\end{align*}
\]

(2.4.12)

Suppose p is a prime representable by \(x_1^2 + x_2^2\) and
\(x_5^2 + q x_6^2\), where \(x_1\) and \(x_5\) are odd, and \(x_2\) and \(x_6\) are even.
Then, as the expressions for \(x_1, x_2\) and \(x_4, x_5\) in (2.4.12) yield
essentially all solutions of (2.4.2), we deduce (as above)
that the expressions in (2.4.12) yield all solutions of
(2.4.1), in the case that $x_1, x_4$ and $x_5$ are odd, and $x_2, x_3$ and $x_6$ are even, except possibly for changing the signs of $x_3$ and $x_4$.

This completes the proof of Theorem 2.4.

Q.E.D.

As corollaries we establish some important relationships among $x_1, x_2$ and $x_5$ ($x_1, x_2$ and $x_5$ are as above).

COROLLARY 2.5. Suppose $p$ is a prime represented by $x_1^2 + x_2^2$ and $x_5^2 + qx_6^2$, where $q = A^2 + B^2$ is as in Theorem 2.4.

(a) If $x_5$ is odd, then $(x_1 + x_5 | q) = 0$ or $(2A | q)$.
(b) If $x_5$ is even, then $(x_1 + x_5 | q) = 0$ or $(A | q)$.

PROOF. Observe first that $A^2 = -B^2 \pmod{q}$.

Assume $p$ is as above.

(a) Suppose $x_5$ is odd. Then, according to the representations of $x_1$ and $x_5$ in (2.4.12), we have

$$A(x_1 + x_5) = A^2(t_0^2 + t_1^2 - t_2^2 + t_3^2 + t_0^2 + t_1^2 - t_2^2) + 2AB(-t_0 t_2 + t_1 t_3 - t_0 t_2 - t_1 t_3)$$

$$= 2(A^2(t_0^2 - t_2^2) - 2ABt_0 t_2) = 2(A^2t_0^2 - 2ABt_0 t_2 + B^2t_2^2) \pmod{q}$$

$$= 2(At_0 - Bt_2)^2 \pmod{q}.$$ Hence $(x_1 + x_5 | q) = (A^2(x_1 + x_5) | q)$

$$= (2A(At_0 - Bt_2)^2 | q) = \text{either 0 or } (2A | q)$.

(b) Suppose $x_5$ is even. Then, according to the representations of $x_1$ and $x_5$ in (2.4.9), we have
\[ A(x_1 + x_5) = A^2(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2AB(t_0 t_3 = t_1 t_2) \]
\[ + 2A^2(t_0 t_1 - t_2 t_3) + 2AB(t_0 t_2 + t_1 t_3) \]
\[ = A^2(t_0 + t_1)^2 - A^2(t_2 + t_3)^2 + 2AB(t_0 + t_1)(t_2 + t_3) \]
\[ = A^2(t_0 + t_1)^2 + 2AB(t_0 + t_1)(t_2 + t_3) + B^2(t_2 + t_3)^2 (\text{mod } q) \]
\[ = (A(t_0 + t_1) + B(t_2 + t_3)^2 (\text{mod } q). \] Hence

\[ (x_1 + x_5 | q) = (A^2(x_1 + x_5) | q) = (A(A(t_0 + t_1) + B(t_2 + t_3))^2 | q) = \text{either 0 or } (A | q). \]

Q.E.D.

**COROLLARY 2.6.** Suppose \( p \) is a prime represented by \( x_1^2 + x_2^2 \) and by \( x_5^2 + qx_6^2 \), where \( q = A^2 + B^2 \) is as in Theorem 2.4.

(a) If \( x_5 \) is odd, then \((x_2 + x_5 | q) = 0 \) or \((A | q)\).

(b) If \( x_5 \) is even, then \((x_2 + x_5 | q) = 0 \) or \((B | q)\).

**PROOF.** (a) Suppose \( x_5 \) is odd; recall that \( A^2 = -B^2 (\text{mod } q) \).

According to the representation of \( x_2 \) and \( x_5 \) in (2.4.12), we

\[ A(x_2 + x_5) = 2A^2(-t_0 t_3 + t_1 t_2) + 2AB(t_0 t_1 + t_2 t_3) + A^2(t_0^2 + t_1^2 - t_2^2 - t_3^2) \]
\[ + 2AB(t_0 t_2 - t_1 t_3) \]
\[ = A^2(t_0 - t_3)^2 - A^2(t_1 - t_2)^2 + 2AB(t_0 - t_3)(t_1 - t_2) \]
\[ = (A(t_0 - t_3) + B(t_1 - t_2))^2 (\text{mod } q). \] Hence

\[ (x_2 + x_5 | q) = (A^2(x_2 + x_5) | q) + (A(A(t_0 - t_3) + B(t_1 - t_2))^2 | q) = 0 \text{ or } (A | q). \]
(b) Suppose \( x_5 \) is even; according to the representations of \( x_2 \) and \( x_5 \) in (2.4.9), we have

\[
B(x_2+x_5) = 2AB(-t_0t_3+t_1t_2) + B^2(t_0^2+t_2^2-t_1^2-t_3^2)
\]
\[
+ 2AB(t_0t_1-t_2t_3) + 2B^2(t_0t_2+t_1t_3)
\]
\[
= B^2(t_0+t_2)^2 - B^2(t_1-t_3)^2 + 2AB(t_0+t_2)(t_1-t_3)
\]
\[
= (B(t_0+t_2) + A(t_1-t_3))^2 \pmod{q}.
\]
Hence

\[
(x_2+x_5|q) = (B^2(x_2+x_5)|q) = (B(B(t_0+t_2)+A(t_1-t_3))^2|q) = 0 \text{ or } (B|q).
\]

Q.E.D.

L E M M A 2 . 6 . 1 . I f \( q \) is a prime \( \equiv 1 \pmod{4} \), and \( q = A^2 + B^2 \), with \( A \) odd, \( B \) even, then \((A|q) = 1 \) and \((B|q) = (2|q)\).

P R O O F . \( A \) is odd, so \( q \equiv B^2 \pmod{A} \) implies \((q|A) = 1\). Since \( q \equiv 1 \pmod{4} \), we have \((A|q) = 1\). Writing \( B = 2^\alpha \cdot c \), where \((2,c) = 1\), we have that \( q \equiv A^2 \pmod{c} \) implies \((c|q) = (q|c) = 1\). Hence \((B|q) = (2^\alpha|q)(c|q) = (2|q)^\alpha\). Now \( q \equiv A^2 + 2^{2\alpha}c^2 \equiv 1 + 4^\alpha \pmod{8} \). If \( \alpha \) is odd, then \( q \equiv 5 \pmod{8} \) implies \((2|q) = -1 = (2|q)^\alpha = (B|q)\), and if \( \alpha \) is even, then \( q \equiv 1 \pmod{8} \) implies \( l = (2|q) = (2|q)^\alpha = (B|q)\). Hence \((B|q) = (2|q)\).

Q.E.D.

As a corollary, we have

C O R O L L A R Y 2 . 7 . L e t \( p \) and \( q \) be as in Corollaries 2.5 and
2.6.

(a) If \( x_5 \) is odd, then \((x_1 + x_5 | q) = 0 \) or \((2 | q)\) and \\
\((x_2 + x_5 | q) = 0 \) or 1.

(b) If \( x_5 \) is even, then \((x_1 + x_5 | q) = 0 \) or 1 and \\
\((x_2 + x_5 | q) = 0 \) or \((2 | q)\).

PROOF. Follows from 2.5, 2.6 and 2.6.1.

Q.E.D.

We now consider the case \( q = 13 \). The necessary conditions that \( f_1 = [1, 0, -13p] \) represent \(-2\) and \(13\) are expressed in Theorems 2.1 and 2.2, respectively. The latter is true because the least positive solution of \( x^2 - 13y^2 = 4 \) is \( x = 249, y = 33 \). Since there are two positive classes of determinant 13, represented by \( g_1 = [1, 0, 13] \) and \( g_2 = [2, 2, 7] \), all of the necessary conditions that \( f_1 \) represent \(-13\) are expressed in Theorem 2.3. In the solutions (2.4.9) and (2.4.12) of (2.4.1), \( A = 3 \) and \( B = 2 \); in the following, we will write \( g_1 \) to mean the form \( x_5^2 + 13x_6^2 \).

THEOREM 2.8. Suppose \( p \equiv 1(\text{mod } 4), \ (p|13) = 1, \) and \( f_1 \) and \( g_1 \) are as above. Then:

(a) If \( g_1 \) represents \( p \) with \( x_5 \) even, then \( f_1 \) never represents \(-1\); it represents 13 or \(-13\), according as \((p|13) = 1 \) or \(-1\).

(b) If \( g_1 \) represents \( p \) with \( x_5 \) odd, then \( f_1 \)
represents \(-1\) if \((p|13)_4 = -1\); otherwise, any of the three possibilities may occur.

(c) If \((p|13)_4 = -1\), then \(f_1\) never represents 13; it represents \(-1\) or \(-13\), according as \(g_1\) represents \(p\) with \(x_5\) odd or with \(x_5\) even. Moreover, if \((p|13) = -1\), then \(g_1\) always represents \(p\), so that, assuming \((p|13)_4 = 1\), the above conditions for representing \(-1\) or \(-13\) are necessary and sufficient.

(d) If \((p|13)_4 = 1\), then \(f_1\) represents 13 if \(g_1\) represents \(p\) with \(x_5\) even; otherwise, any of the three possibilities may occur.

The proof is based on the following lemmas.

**LEMMA 2.8.1.** Each condition in column A implies the respective conditions in columns B and C.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>(p \mod 13)</td>
<td>(\pm x_1 \mod 13)</td>
<td>(\pm x_5 \mod 13)</td>
</tr>
<tr>
<td>1</td>
<td>0, 1, 7, or 11</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0, 5, 9, or 11</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>0, 3, 5, or 7</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0, 1, 9, or 11</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>0, 1, 3, or 7</td>
<td>6</td>
</tr>
<tr>
<td>12</td>
<td>0, 3, 5, or 9</td>
<td>5</td>
</tr>
</tbody>
</table>

**PROOF.** Straightforward verification.
LEMMA 2.8.2. Suppose \((p|13) = 1\).

(a) If \(p \equiv 1 \pmod{13}\), then \(x_5\) is even iff \(\pm x_1 \equiv 0\) or \(11 \pmod{13}\).

(b) If \(p \equiv 3 \pmod{13}\), then \(x_5\) is even iff \(\pm x_1 \equiv 0\) or \(5 \pmod{13}\).

(c) If \(p \equiv 9 \pmod{13}\), then \(x_5\) is even iff \(\pm x_1 \equiv 0\) or \(7 \pmod{13}\).

(d) If \(p \equiv 4 \pmod{13}\), then \(x_5\) is even iff \(\pm x_1 \equiv 1\) or \(11 \pmod{13}\).

(e) If \(p \equiv 10 \pmod{13}\), then \(x_5\) is even iff \(\pm x_1 \equiv 3\) or \(7 \pmod{13}\).

(f) If \(p \equiv 12 \pmod{13}\), then \(x_5\) is even iff \(\pm x_1 \equiv 5\) or \(9 \pmod{13}\).

PROOF. We will prove (a); proofs of the rest are similar.

(a) If \(p \equiv 1 \pmod{13}\), it is straightforward to check that if \(x_1\) satisfies the condition in column A, then all other conditions in the same row are satisfied.

<table>
<thead>
<tr>
<th>(\pm x_1 \pmod{13})</th>
<th>(+ x_2 \pmod{13})</th>
<th>(x_1 + x_5 \pmod{13})</th>
<th>(x_2 + x_5 \pmod{13})</th>
<th>((x_1 + x_5) \pmod{13})</th>
<th>((x_2 + x_5) \pmod{13})</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0 or 2</td>
<td>1</td>
<td>0 or -1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0 or 2</td>
<td>1</td>
<td>0 or -1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>6 or 8</td>
<td>10 or 12</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>10 or 12</td>
<td>6 or 8</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>
If \( x_5 \) is even, then by Corollary 2.7, \((x_1 + x_5 | 13) = 0\) or 1 and \((x_2 + x_5 | 13) = 0\) or \(-1\). The only way that both of these conditions may be satisfied simultaneously is if \( \pm x_1 = 0 \) or \(11 \mod 13\). Conversely, if \( x_5 \) is odd, then by Corollary 2.7, \((x_1 + x_5 | 13) = 0\) or \(-1\) and \((x_2 + x_5 | 13) = 0\) or 1; the only way that both of these conditions may be satisfied simultaneously is if \( \pm x_1 = 1 \) or \(7 \mod 13\). Since \( \pm x_1 = 0,1,7 \) or \(11 \mod 13\) if \( p = 1 \mod 13 \) (by the previous lemma), this proves (a). Parts (b) through (f) are proved by exhibiting similar tables.

Q.E.D.

LEMMA 2.8.3. Suppose \( g_1 \) represents \( p \) with \( x_5 \) even. Then \((3x_1 \pm 2x_2 | 13) = -1\), for both choices of sign.

PROOF. Suppose \( g_1 \) represents \( p \) with \( x_5 \) even. If \( p = 1 \mod 13 \), then, by Lemma 2.8.2, \( \pm x_1 = 0 \) or \(11 \mod 13\); \( x_1 = 0 \) implies \( \pm x_2 = 1 \), and \(3x_1 \pm 2x_2 = \pm 2 \mod 13\); \( \pm x_1 = 11 \) implies \( \pm x_2 = 7 \), and \(3x_1 \pm 2x_2 = \pm 6 \) or \(8 \mod 13\).

In either case, \((3x_1 + 2x_2 | 13) = -1\) for both choices of sign. The proofs for the cases \( p = 3,4,9,10,12 \mod 13 \) are analogous and are omitted.

Q.E.D.

LEMMA 2.8.4. If \((p | 13) = 1\), then \( g_1 \) represents \( p \).

PROOF. If \((p | 13) = 1\), then \( p \) is represented by some form
in the principal genus of determinant $13$, which contains only the class containing $g_1$. 

Q.E.D.

**Proof of Theorem 2.8.**

(a) Suppose $g_1$ represents $p$, with $x_5$ even. By Lemma 2.8.3, $(3x_1 + 2x_2 | 13) = -1$, for both choices of sign; this is contrary to the necessary conditions in Theorem 2.1, so that $f_1$ does not represent $-1$. If $(p|13)_4 = 1$, then $x_5$ even implies that none of the conditions in Theorem 2.3 are met (neither $(p|13)_4 = 1$ and $x_5$ odd, nor $(p|13)_4 = (2|13) = -1$ and $x_5$ even); hence $f_1$ does not represent $-13$. Hence $f_1$ represents $13$. Finally, if $(p|13)_4 = -1$, then by Corollary 2.2.1, $f_1$ does not represent $13$; hence $f_1$ represents $-13$.

(b) Suppose $g_1$ represents $p$ with $x_5$ odd. If $(p|13)_4 = -1$, then by Corollary 2.2.1, $f_1$ does not represent $13$. The conditions in Theorem 2.3 are not met, so that $f_1$ does not represent $-13$. Hence $f_1$ represents $-1$. If $(p|13)_4 = 1$, then the following are examples in which $f_1$ may represent $-1, 13$, or $-13$: if $p = 53 = 1^2 + 13\cdot 2^2$ $f_1$ represents $-13$; if $p = 61 = 3^2 + 13\cdot 2^2$, $f_1$ represents $13$; if $p = 937 = 27^2 + 13\cdot 4^2$, $f_1$ represents $-1$.

(c) Suppose $(p|13)_4 = -1$. By Corollary 2.2.1, $f_1$ never represents $13$. If $g_1$ represents $p$ with $x_5$ odd,
$f_1$ represents $-1$ by (b). If $g_1$ represents $p$ with $x_5$ even, $f_1$ represents $-13$ by (a). The second statement follows from the first statement and from Lemma 2.8.4 (i.e. that $(p|13) = 1$ implies $g_1$ represents $p$).

(d) Suppose $(p|13)_4 = 1$. If $g_1$ represents $p$ with $x_5$ even, then $f_1$ represents $13$, by (a). If $g_1$ represents $p$ with $x_5$ odd, the examples given in (b) prove the last statement.

Q.E.D.
CHAPTER III

In this chapter we prove some partial results concerning the primes $q = 29, 53$ and $61$.

**THEOREM 3.1.** Suppose $p \equiv 1 \pmod{4}$, $(p|29) = 1$, and $f_1 = [1,0,-29p]$. Then $f_1$ represents $-29$ implies either

(a) there exist integers $x_5$ and $x_6$ such that $p = x_5^2 + 29x_6^2$ and either (1) $x_5$ is odd and $(p|29)_4 = 1$, or (2) $x_5$ is even and $(p|29)_4 = -1$; or (b) there exist integers $y_5$ and $y_6$ such that $p = 5y_5^2 + 2y_5y_6 + 6y_6^2$ and either (1) $y_6$ is odd and $(p|29)_4 = 1$, or (2) $y_6$ is even and $(p|29)_4 = -1$.

**PROOF.** If there exist integers $u,v$ (as usual, we may assume $v > 0$) such that $u^2 - 29pv^2 = -29$, then the form $g = [29pv, 2u, v]$ has determinant $29$, and so is in one of the six positive-definite classes of that determinant.

If $g \sim g_1 = [1,0,29]$, or if $g \sim g_2 = [2,2,15]$, then the consequences have been determined by Theorem 2.3; they are precisely statements (a-1) and (a-2), as above.

If $g \sim g_3 = [3,2,10]$, or if $g \sim g_4 = [3,-2,10]$, we form the following Cantor diagram:

$$[3, \pm 2, 10] \xrightarrow{T} [29pv, 2u, v]$$

$$h = [a,2b,c] \xleftarrow{T'} [1,0,-29p] = f_1$$

57
By Proposition 1.5, \( 3a + 2b + 10c = 0 \); writing \( a = 2x \), we find that there is a form \( h = [2x, +2(5c+3x),c] \) in the class of \( f_1 \). Comparing determinants, we find that

\[ 29p = 25c^2 + 28cx+9x^2; \]

comparing modulo 29, we obtain the congruences

\[ 0 \equiv 25c^2 - 30cx + 9x^2 = (5c - 3x)^2 \pmod{29}, \]

\[ 5c \equiv 3x \pmod{29}, \]

and \( x \equiv -8c \pmod{29} \). If we write \( x = -8c + 29y \), the above equation becomes

\[ 29p = 25c^2 + 28(-8c+29y) + 9(-8c+29y)^2 \]

\[ = 377c^2 - 29\cdot116cy + 9\cdot29^2y^2; \]

hence

\[ p = 13c^2 - 116cy + 261y^2. \]

Applying the unimodular transformation \( c = 4y_5 - 5y_6, y = y_5 - y_6 \) leads to the equation

\[ p = 5y_5^2 + 2y_5y_6 + 6y_6^2; \]

since \( p \) is odd, so is \( y_5 \), and since \( h \) is primitive, \( c \) is odd, so \( y_6 \) is also odd. Moreover, \( h \) is in the genus of \( f_1 \), so \( \ell = (c|29) = (4y_5 - 5y_6|29) = (-6|29)(4y_5 - 5y_6|29) = (-24y_5 + 30y_6|29) = (5y_5 + y_6|29). \)

Finally, we have that \( 5p = (5y_5 + y_6)^2 + 29y_6^2 \), so that \( 5p \equiv (5y_5 + y_6)^6 \pmod{29} \), and so \( (p|29)_4 = (5|29)_4 = (5|29)_4 \)

\[ = (5|29)_4((5y_5 + y_6)^2|29)_4 = (5|29)_4(5y_5 + y_6|29) = (5|29)_4 \]

\[ = (11|29) = (29|11) = (7|11) = -1. \]

This proves that statement \((b-2)\) may be a necessary condition for \( f_1 \) to represent -29.

If \( g \sim g_5 = [5,2,6] \), or if \( g \sim g_6 = [5,-2,6] \), we form the following Cantor diagram:
\[ [5, \pm 2, 6] \overset{T}{\longrightarrow} [29p, 2u, v] \]

\[ h = [a, 2b, c] \overset{T'}{\longrightarrow} [1, 0, -29p] = f_1 \]

By Proposition 1.5, \( 5a + 2b + 6c = 0 \); hence \( a \) is even. Writing \( a = 2x \), we obtain a form \( h = [2x, \pm 2(5x + 3c), c] \) in the class of \( f_1 \). Comparing determinants, we find that
\[ 29p = 25x^2 + 28xc + 9c^2; \] comparing modulo 29, we obtain the congruences
\[ 0 \equiv 25x^2 - 30xc + 9c^2 \equiv (5x - 3c)^2 \pmod{29}, \]
\[ 5x \equiv 3c \pmod{29}, \] and \( x \equiv -11c \pmod{29} \). Writing \( x = -11c + 29y \)
leads to the equation
\[ 29p = 29^2 \cdot 25y^2 - 522 \cdot 29yc + 29 \cdot 94c^2, \]
or that \( p = 725y^2 - 522yc + 94c^2 \). Applying the unimodular transformation \( y = -y_5 + 4y_6 \), \( c = -3y_5 + 11y_6 \) yields the equation
\[ p = 5y_5^2 + 2y_5y_6 + 6y_6^2. \] Since \( p \) is a prime, \( y_5 \) is odd; since \( h \) is primitive, \( c \) is odd, so \( y_6 \) is even. Moreover, \( h \) is in the genus of \( f_1 \), so \( l = (c|29) = (-3y_5 + 11y_6|29) = -(8|29)(-3y_5 + 11y_6|29) = -(24y_5 + 88y_6|29) = -(5y_5 + y_6|29). \) Hence \( (5y_5 + y_6|29) = -1; \) since
\[ 5p \equiv (5y_5 + y_6)^2 \pmod{29}, \] we have \( (p|29)_4 = -(5|29)_4 = 1. \) This proves that condition (b-1) can be a necessary one if \( f_1 \) represents -29.

Since we have exhausted all the possibilities, we have shown that one of (a-1), (a-2), (b-1) and (b-2) must occur whenever \( f_1 \) represents -29.

Q.E.D.
We now prove the following representation theorem.

**THEOREM 3.2.** Suppose $p \equiv 1 \pmod{4}$, $(p|29) = 1$, and there exist integers $x_5$ and $x_6$ such that $p = x_5^2 + 29x_6^2$. Suppose $f_1 = [1, 0, -29]$. Then:

(a) If $x_5$ is even, then $f_1$ never represents $-1$; it represents either $29$ or $-29$, according as $(p|29)_4 = 1$ or $-1$.

(b) If $x_5$ is odd, then $f_1$ represents $-1$ if $(p|29)_4 = -1$; otherwise, any of the three possibilities ($f_1$ represents $-1, 29, -29$) may occur.

(c) If $(p|29)_4 = -1$, then $f_1$ never represents $29$; it represents $-1$ or $-29$, according as $x_5$ is odd or even.

(d) If $(p|29)_4 = 1$, then $f_1$ represents $29$ if $x_5$ is even; otherwise, any of the three possibilities may occur.

We observe that this theorem does not describe the behavior of all primes of the form $4n+1$ which are quadratic residues of $29$, but only of those which, in addition, are represented by the form $[1,0,29]$. Primes such as 5, 13 and others represented by $[5,2,6]$ are not treated in this theorem; in order to do so, it is necessary to study the relationships among the forms $[1,0,1]$, $[1,0,-29]$ and $[5,2,6]$. Moreover, if the prime $q \equiv 1 \pmod{4}$ is such that the principal genus of determinant $q$ contains many classes, then the number of possible forms by which a prime $p$, $(p|q) = 1$, may be represented increases. (An example of such a prime is
q = 89; there are six classes in the principal genus of determinant 89). For such primes the difficulty in obtaining complete representation theorems increases; we will explore these difficulties in detail when we study the prime q = 17. At that time we will explain the basic difference primes of the form 8n + 1 and those of the form 8n + 5.

Proof of Theorem 3.2 is based on the following lemmas (in the following, \(x_1\) through \(x_6\) are as in equation (2.4.1).

**LEMMA 3.2.1.** Each condition in column A implies the corresponding condition in column B and one of the corresponding conditions in column C.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>(p \mod 29)</td>
<td>( \pm x_5 \mod 29 )</td>
<td>all pairs ((\pm x_1, \pm x_2))or((\pm x_2, \pm x_1))mod 29</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>((0,1), (5,11), (6,9), (8,13))</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>((0,2), (3,13), (7,10), (11,12))</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>((0,11), (1,2), (3,5), (8,12))</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>((0,8), (1,11), (6,12), (10,14))</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>((0,6), (1,8), (4,7), (9,10))</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>((0,3), (2,11), (4,14), (5,10))</td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td>((0,10), (2,3), (6,8), (7,14))</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>((0,4), (3,6), (5,7), (9,14))</td>
</tr>
<tr>
<td>20</td>
<td>7</td>
<td>((0,7), (2,4), (5,13), (6,10))</td>
</tr>
<tr>
<td>22</td>
<td>14</td>
<td>((0,14), (3,10), (4,8), (9,12))</td>
</tr>
<tr>
<td>23</td>
<td>9</td>
<td>((0,9), (1,14), (4,6), (12,13))</td>
</tr>
<tr>
<td>24</td>
<td>13</td>
<td>((0,13), (1,9), (2,7), (5,12))</td>
</tr>
<tr>
<td>25</td>
<td>5</td>
<td>((0,5), (1,13), (3,4), (7,11))</td>
</tr>
<tr>
<td>28</td>
<td>12</td>
<td>((0,12), (2,13), (8,14), (9,11))</td>
</tr>
</tbody>
</table>

**PROOF.** Straightforward verification.
LEMMA 3.2.2. If \((p|29)=1\), \(p \equiv 1(\text{mod } 4)\), and \(p\) is represented by \(x_1^2 + x_2^2\) and by \(x_5^2 + 29x_6^2\), then

\[\text{(a) } x_5 \text{ even implies } (x_1 + x_5|29) = 0 \text{ or } 1 \text{ and } (x_2 + x_5|29) = 0 \text{ or } -1\]

\[\text{(b) } x_5 \text{ odd implies } (x_1 + x_5|29) = 0 \text{ or } -1 \text{ and } (x_2 + x_5|29) = 0 \text{ or } 1.\]

PROOF. This is just Corollary 2.7 in the case \(q = 29\).

LEMMA 3.2.3. If \(p\) is as in Lemma 3.2.2, and \(x_5\) is even, then \(f_1\) does not represent \(-1\).

PROOF. We will prove this in the case \(p \equiv 1(\text{mod } 29)\); proofs in the other thirteen cases involve only changes in the numerical values of \(p\), \(x_1\), \(x_2\) and \(x_5\). The forms of the proofs in the other thirteen cases are the same as what follows. Let \(p \equiv 1(\text{mod } 29)\) and \(p \equiv 1(\text{mod } 4)\); we then have the following table. All values are given modulo 29, except the Legendre symbols; by Lemma 3.2.1, \(\pm x_5 \equiv 1(\text{mod } 29)\).

| \(\pm x_1 \pm x_2 \pm (5x_1+2x_2)(5x_1+2x_2|29)\pm (x_1+x_5)(x_1+x_5|29)\pm (x_2+x_5)(x_2+x_5|29)\) | 0 | 1 | 2 | -1 | 1 | 1 | 0,2 | 0,-1 |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 5 | 1 | 0,2 | 0,-1 | 1 | 1 |
| 1 | 0 | 5 | 0 | 1 | 0,2 | 0,-1 | 1 | 1 |
| 5 | 11 | 11 | 3 | 11 | 4,6 | 1 | 10,12 | -1 |
| 6 | 9 | 10,12 | -1 | 5,7 | 1 | 8,10 | -1 |
| 8 | 13 | 8,14 | -1 | 7,9 | 1 | 12,14 | -1 |
| 9 | 6 | 1,4 | 1 | 8,10 | -1 | 5,7 | 1 |
| 11 | 5 | 7,13 | 1 | 10,12 | -1 | 4,6 | 1 |
| 13 | 8 | 6,9 | 1 | 12,14 | -1 | 7,9 | 1 |
Suppose $x_5$ is even. Then, by the results of Lemma 3.2.2, we deduce that $\pm x_1 \equiv 0, 5, 6$ or $8 \pmod{29}$. For such $x_1$, we see that $(5x_1 \pm 2x_2 \pmod{29}) = -1$, for either choice of signs. This contradicts the necessary conditions in Theorem 2.1, that $f_1$ represent $-1$; hence $x_5$ even and $p \equiv 1 \pmod{29}$ implies $f_1$ does not represent $-1$. The cases $p = 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25$ and $28 \pmod{29}$ are handled in the same manner.

Q.E.D.

PROOF OF THE THEOREM. Suppose $p$ and $x_5$ are as in the hypothesis.

(a) If $x_5$ is even, then by Lemma 3.2.3, $f_1$ never represents $-1$. If $(p|29)_4 = 1$, then none of the conditions in Theorem 3.1 are met, so $f_1$ does not represent $-29$; hence $f_1$ represents $29$. If $(p|29)_4 = -1$, then by Corollary 2.2.1, $f_1$ does not represent $29$; hence $f_1$ represents $-29$.

(b) Suppose $x_5$ is odd and $(p|29)_4 = -1$. None of the conditions of Theorem 3.1 are met, so $f_1$ does not represent $-29$; $f_2$ never represents $29$ for such $p$, by (a), so $f_1$ must represent $-1$. If $(p|29)_4 = 1$, the techniques developed here will not ascertain which of the three numbers $-1, 29, -29$ is represented by $f_1$; in fact, there are primes where any of $-1, 29, -29$ is represented. The smallest are $197$ for $-1$, $1069$ for $29$, and $1213$ for $-29$. 
(c) Suppose \( (p|29)_4 = -1 \). If \( x_5 \) is even, then by part (a), \( f_1 \) represents \(-29\), and if \( x_5 \) is odd, then by part (b), \( f_1 \) represents \(-1\).

(d) Suppose \( (p|29)_4 = 1 \). If \( x_5 \) is even, then \( f_1 \) represents \(29\), by part (a); otherwise, it is not possible, using these techniques, to ascertain which of \(-1, 29, -29\) is represented by \( f_1 \). Examples of each are given in (c).

Q.E.D.

Analogs of Theorem 3.1 hold for the primes \( q = 53 \) and 61. This is because there are exactly six positive classes of forms of each of the determinants 53 and 61. Hence the principal genera of determinants 53 and 61 each contain three classes: the principal class (represented by \([1,0,53]\) and \([1,0,61]\), respectively) and a pair of improperly equivalent classes (represented by \([6,\pm 2,9]\) and \([5,\pm 4,13]\), respectively). The non-principal genera of these determinants have the same structure: that of determinant 53 contains \([2,2,27]\), \([3,2,18]\), and \([3,-2,28]\); that of determinant 61 contains \([2,2,31]\), \([7,6,10]\), and \([7,-6,10]\). Analogs of Theorem 3.2 may be proved, because the primes \( q = 53 \) and 61 are of the form \( 8n+5 \), which means that, in Corollary 2.7, changing the parity of \( x_5 \) changes the signs of \((x_1 + x_5|q)\) and \((x_2 + x_5|q)\). (Primes such as 17, 73 and 97 of the form \( 8n+1 \) does not have this property: more on
this in the next chapter).

**THEOREM 3.3.** Suppose \( p \equiv 1 \pmod{4} \), \((p|53) = 1\), and \( f_1 = [1,0,-53p] \). If \( f_1 \) represents \(-53\), then either

(a) there exist \( x_5, x_6 \) such that \( p = x_5^2 + 53x_6^2 \) and either (1) \( x_5 \) is odd and \((p|53)_4 = 1\), or (2) \( x_5 \) is even and \((p|53)_4 = -1\); or

(b) there exist \( y_5, y_6 \) such that \( p = 6y_5^2 + 2y_5y_6 + 9y_6^2 \) and either (1) \( y_5 \) is odd and \((p|53)_4 = 1\) or (2) \( y_5 \) is even and \((p|53)_4 = -1\).

**SKETCH OF THE PROOF.** If there exist \( u,v (v > 0) \), as usual) such that \( u^2 - 53pv^2 = -53 \), then the form \( g = [53pv, 2u, v] \) has determinant 53, and as such, is equivalent to one of the aforementioned forms. Using the Cantor diagrams in the manner of Theorem 3.1, we deduce the following: if \( g \sim [1,0,53] \), then condition (a-1) results; if \( g \sim [2,2,27] \), then condition (a-2) results; if \( g \sim [6,2,9] \), or if \( g \sim [6,-2,9] \), then condition (b-1) results; of \( g \sim [3,2,18] \), or if \( g \sim [3,-2,18] \), then condition (b-2) results.

Using the same techniques, we prove

**THEOREM 3.4.** Suppose \( p \equiv 1 \pmod{4} \), \((p|61) = 1\), and \( f_1 = [1,0,-61p] \). If \( f_1 \) represents \(-61\), then either

(a) there exists \( x_5, x_6 \) such that \( p = x_5^2 + 61x_6^2 \) and either (1) \( x_5 \) is odd and \((p|61)_4 = 1\), or (2) \( x_5 \) is even
and \((p|61)_4 = -1\); or

(b) there exist \(y_5, y_6\) such that \(p = 5y_5^2 + 4y_5y_6 + 13y_6^2\) and either (1) \(y_5\) is even and \((p|61)_4 = 1\), or (2) \(y_5\) is odd and \((p|61)_4 = -1\).

**Sketch of the Proof.** If there exist \(u, v\) \((v > 0)\) such that \(u^2 - 61pv^2 = -61\), then the form \(g = [61pv, 2u, v]\) has determinant 61. Using Cantor diagrams, the following can be deduced: if \(g \sim [1, 0, 61]\), then (a-1) results; if \(g \sim [2, 2, 31]\), then (a-2) results; if \(g \sim [5, 4, 13]\), or if \(g \sim [5, -4, 13]\), then (b-1) results, if \(g \sim [7, 6, 10]\) or if \(g \sim [7, -6, 10]\), then (b-2) results.

Using Theorems 3.3 and 3.4, we may prove the following representation theorem:

**Theorem 3.5.** Let \(q = 53\) or \(61\). Let \(p \equiv 1 \pmod{4}\), \((p|q) = 1\), and suppose there exist \(x_5\) and \(x_6\) such that \(p = x_5^2 + qx_6^2\). Suppose \(f_1 = [1, 0, -pq]\). Then:

(a) If \(x_5\) is even, then \(f_1\) never represents \(-1\); it represents either \(q\) or \(-q\), according as \((p|q)_4 = 1\) or \(-1\).

(b) If \(x_5\) is odd, then \(f_1\) represents \(-1\) if \((p|q)_4 = -1\); however, if \((p|q)_4 = 1\), then any of the possibilities \((f_1\) represents \(-1, q, -q\) may occur.

(c) If \((p|q)_4 = -1\), then \(f_1\) never represents \(q\);
it represents $-1$ or $-q$, according as $x_5$ is odd or even.

(d) If $(p|q)_4 = 1$, then $f_1$ represents $q$ if $x_5$ is even if not, any of the possibilities may occur.

SKETCH OF THE PROOF.

(a) First, state and prove a lemma (for each of 53 and 61) which gives the appropriate restrictions on $p$, $x_1, x_2, x_5$, analogous to Lemma 3.2.1.

(b) Second, restate Lemma 3.2.2, replacing 29 by 53, then by 61.

(c) Third, state and prove a lemma to the effect that if $x_5$ is even, then $f_2$ does not represent $-1$. This is done analogously to Lemma 3.2.3, by checking cases, inspecting tables, and using previous results concerning $x_1, x_2, x_5$.

(d) Fourth, use the three lemmas to prove the theorem, in precisely the same manner as is done for Theorem 3.2.

One further remark is in order: it appears that partial results analogous to Theorem 3.2 are true for all primes $q = 5 (\text{mod} \ 8)$, because of the fact that changing the parity of $x_5$ in the representation of a prime $p$, $(p|q) = 1$, as $x_5^2 + qx_6^2$, changes the signs of $(x_1 + x_5|q)$ and $(x_2 + x_5|q)$. We will state such a general theorem without proof.
THEOREM 3.6. Let \( p \equiv 1 \pmod{4} \), \( q \equiv 5 \pmod{8} \), \( (p|q) = 1 \), \( f_1 = [1,0,-pq] \), and suppose there exist integers \( x_5, x_6 \) such that \( p = x_5^2 + qx_6^2 \). Then:

(a) If \( x_5 \) is even, then \( f_1 \) never represents \(-1\); it represents \( q \) or \(-q\), according as \( (p|q)_4 = 1 \) or \(-1\).

(b) If \( x_5 \) is odd, then \( f_1 \) represents \(-1\) if \( (p|q)_4 = -1 \); otherwise, any of the possibilities \( (f_1 \) represents \(-1, q, \) or \(-q) \) may occur.

(c) If \( (p|q)_4 = -1 \), then \( f_1 \) never represents \( q \); it represents \(-1 \) or \(-q\), according as \( x_5 \) is odd or even.

(d) If \( (p|q)_4 = 1 \), then \( f_1 \) represents \( q \) if \( x_5 \) is even; otherwise, any of the possibilities may occur.
CHAPTER IV

In this chapter, we study the case \( q = 17 \), and investigate a fundamental difficulty which occurs in this study.

By elementary investigation, we deduce that there are four positive-definite classes of discriminant \(-4,17\), i.e. of determinant 17; the classes containing \([1,0,17] = g_1\) and \([2,2,9] = g_2\) are in the principal genus (recall that \((2|17) = 1\)), and the classes containing \([3,2,6] = g_3\) and \([3,-2,6] = g_4\) are in the non-principal genus. We now study this question: for \( p \equiv 1 \pmod{4}, (p|17) = 1 \), which of \(-1,17,-17\) is represented by \( f_1 = [1,0,-17p] \)? As before, we deduce certain necessary conditions that each of \(-1,17,-17\) be represented by \( f_1 \), which may be summarized in the following theorem:

THEOREM 4.1. Let \( p \equiv 1 \pmod{4}, (p|17) = 1 \), and \( f_1 = [1,0,-17p] \).

(a) If \( f_1 \) represents \(-1\), then there exist integers \( x_1 \) odd, \( x_2 \) even such that \( p = x_1^2 + x_2^2 \) and either

(1) \( (x_1 + 4x_2|17) = 1 = (4x_1 - x_2|17) \), or \( (x_1 - 4x_2|17) = 1 = (4x_1 + x_2|17) \).

(b) If \( f_1 \) represents 17, then there exist integers \( x_3 \)
even, \( x_4 \) odd such that \( p = -x_3^2 + 17x_4^2 \) and \((x_3 | 17) = 1\).

(c) If \( f_1 \) represents \(-17\), then either (1) there exist integers \( x_5, x_6 \) such that \( p = x_5^2 + 17x_6^2 \) and \((p | 17)_4 = 1\), or (2) there exist integers \( y_5, y_6 \) such that \( p = 2y_5^2 + 2y_5y_6 + 9y_6^2 \) and \((p | 17)_4 = -1\).

PROOF. Statement (a) is just Theorem 2.1, in the case \( q = 17 \). Then, in that theorem, \( a = 1 \), \( b = 4 \), and \((2 | q) = (2 | 17) = 1\). Statement (b) is just Theorem 2.2, in the case \( q = 17 \), along with the observation that \((2 | q) = (2 | 17) = 1\). Statement (c-1) is just Theorem 2.3*, in the case \( q = 17 \); again, along with the observation that \((2 | q) = (2 | 17) = 1\). We now prove statement (c-2), using the Cantor diagrams.

Suppose there exist \( u, v \) \((v > 0)\) such that \( u^2 - 17pv^2 = -17 \), then the form \( g = [17pv, 2u, v] \) has determinant \( 17 \). If \( g \sim g_1 \) or \( g \sim g_2 \), then condition (c-1) results: the remaining possibilities are \( g \sim g_3 \) and \( g \sim g_4 \). If either of these occur, we form the following Cantor diagram:

\[
\begin{align*}
[3 + 2, 6] & \xrightarrow{T} [17pv, 2u, v] \\
h = [a, 2b, c] & \xleftarrow{T'} [1, 0, -17p]
\end{align*}
\]

By Proposition 1.5, \( 3a + 2b + 6c = 0 \), so \( a = 2x \); hence \( b = \pm 3(x + c) \), and there is a form \( h = [2x, \pm 2(3(x + c)), c] \) in the class of \( f_1 \). Comparing determinants we find that
$17p = 9(x + c)^2 - 2xc = 9x^2 + 16xc + 9c^2$. Modulo 17, we have the following congruences: $0 \equiv 9x^2 - 18xc + 9c^2 \equiv 3(x-c)^2 \pmod{17}$, $(x-c)^2 \equiv 0 \pmod{17}$, $x \equiv c \pmod{17}$. If we write $c = x + 17y$, we have $17p = 9x^2 + 16x(x + 17y) + 9(x + 17y)^2$

$= 2 \cdot 17x^2 + 2 \cdot 17^2xy + 9 \cdot 17^2y^2$. Hence, $p = 2x^2 + 2 \cdot 17xy + 9 \cdot 17y^2$; applying the translation $x = y_5 - 8y_6$, $y = y_6$ leads to the equation $p = 2y_5^2 + 2y_5y_6 + 9y_6^2$. Since $h$ is in the genus of $f_1$, $l = (a \mid 17) = (2x \mid 17) = (2y_5 - 16y_6 \mid 17) = (2y_5 + y_6 \mid 17)$. Hence $2p = (2y_5 + y_6)^2 + 17y_6^2$, so $(p \mid 17)_4 = (2 \mid 17)_4((2y_5 + y_6)^2 \mid 17)_4$

$= (6 \mid 17)(2y_5 + y_6 \mid 17) = (6 \mid 17) = -1$. This yields assertion (c-2); since all the possibilities are exhausted, we conclude that, if $f_1$ represents $-17$, then either (c-1) or (c-2) occurs.

Q.E.D.

After examining 30 or 40 cases, it seems likely that the following theorem is true:

THEOREM 4.2. Let $p \equiv 1 \pmod{4}$, $(p \mid 17) = 1$, and $f_1, g_1, g_2$ be as above. Then:

(a) If $g_2$ represents $p$, then $f_1$ never represents $-1$; it represents $17$ or $-17$, according as $(p \mid 17)_4 = 1$ or $-1$.

(b) If $g_1$ represents $p$, then $f_1$ represents $-1$ if $(p \mid 17)_4 = -1$; if $(p \mid 17)_4 = 1$, then any of the three possibilities $(f_1$ represents $-1, 17, -17)$ can occur.

(c) If $(p \mid 17)_4 = -1$, then $f_1$ never represents $17$; it
represents -1 or -17, according as p is represented by \( g_1 \) or by \( g_2 \).

(d) If \( (p|17)_4 = 1 \), then \( f_1 \) represents 17 if \( g_2 \) represents \( p \); however, if \( g_1 \) represents \( p \), then any of the possibilities can occur.

We will prove part of this theorem and demonstrate why the entire theorem cannot at this time be proven.

Since we need to know some properties of the form \( g_2 \) as related to a sum of two squares, we now attempt to obtain a complete parametric representation of the solutions of

\[(4.2.1) \quad p = x_1^2 + x_2^2 = 2y_5^2 + 2y_5y_6 + 9y_6^2\]

in the case that \( p \) is a prime represented by these two forms, \( x_1 \) is odd, and \( x_2 \) is even. To do this, we examine the auxiliary equation

\[(4.2.2) \quad 2x_1^2 + 2x_2^2 = (2y_5 + y_6)^2 + 17y_6^2.\]

Since \( p \) is odd, \( y_6 \) must be odd, and so \( z_5 = 2y_6 + y_6 \) is also odd. We consider the equation

\[-17y_6^2 = z_5^2 - 2x_1^2 - 2x_2^2,\]

and remark that the right side is the norm of the quaternion \( Q = z_5i_1 + x_1i_2 + x_2i_3 \) in the ring of quaternions with the following multiplication: \( i_1^2 = -1, \)

\( i_2^2 = i_3^2 = 2, \quad i_1i_2 = -i_2i_3 = t_3, \quad i_2i_3 = -i_3i_2 = 2i_1, \) and \( i_3i_1 = -i_2 \). The norm form of this system of quaternions is

\( F = u_0^2 + u_1^2 - 2u_2^2 - 2u_3^2. \) We now quote a theorem from [3] which implies that \( F \) is in a genus of one class, and as such,
Lemma 1.8 on the factorization of quaternions can be applied.

**Lemma 4.2.3.** If $F$ is an indefinite quadratic form of three or more variables, and if the reduced determinant $D$ of $F$ (See [2]) has the property that $16 | p$, and there is no prime $p$ such that $p^3 | D$, then $F$ is in a genus of one class.

In this case, with $F = u_0^2 + u_1^2 - 2u_2^2 - 2u_3^2$, it happens that $D = -2$, so $F$ is in a genus of one class. Since $-qy_6^2$ is odd, we may apply Lemma 1.8, and write $Q = \alpha \sigma$, where $N(\alpha) = -17y_6$, $N(\sigma) = y_6$; since $Q$ is pure, $Q^* = -Q$, so $\sigma^* \alpha^* = -\alpha \sigma$, $\sigma^*$ is a left divisor of $\alpha$. Hence we may write $Q = \sigma^* \tau \sigma$, where $N(\sigma) = N(u_0 + u_1 i_1 + u_2 i_2 + u_3 i_3) = y_6$, and $N(\tau) = -17$. Now, by Lemma 1.9, that $Q$ is pure implies $\tau$ is pure. If we put $\tau = a i_1 + b i_2 + c i_3$, then $Q = \sigma^* \tau \sigma = (u_0 - u_1 i_1 - u_2 i_2 - u_3 i_3)(a i_1 + b i_2 + c i_3)(u_0 + u_1 i_1 + u_2 i_2 + u_3 i_3)$

$$= i_1 (a(u_0^2 + u_1^2 + 2u_2^2 + 2u_3^2) + 4b(u_0 u_3 - u_1 u_2) + 4c(-u_0 u_2 - u_1 u_3))$$

$$+ i_2 (2a(u_0 u_3 + u_1 u_2) + b(u_0^2 + 2u_2^2 - u_1^2 - 2u_2^2) + 2c(-u_0 u_1 - 2u_2 u_3))$$

$$+ i_3 (2a(-u_0 u_2 + u_1 u_3) + 2b(u_0 u_1 - 2u_2 u_3) + c(u_0^2 + 2u_2^2 - u_1^2 - 2u_2^2)).$$

Now $z_5, x_1$ and $x_2$ are the coefficients of $i_1, i_2$, and $i_3$ respectively; hence, in determining $\tau$, we must have $a \equiv z_5$, $b \equiv x_1$, $c \equiv x_2$ (mod 2), so that $a$ and $b$ must be odd, and $c$ must be even. In addition, since $y_5 = (z_5 - y_6)/2$, and since $y_6 = N(\sigma) = u_0^2 + u_1^2 - 2u_2^2 - 2u_3^2$, we deduce that $y_5 = (a+1)(u_0^2 + u_1^2)/2$ (mod 2). In order for $y_6$, $z_5$, and $x_1$ to
be odd, \( u_0 = u_1 + 1 \) (mod 2). Hence \( u_0^2 + u_1^2 \equiv 1 \) (mod 2), and 
\( y_5 = \frac{1}{2}(a+1) \) (mod 2). If \( a \equiv 1 \) (mod 4), then \( y_5 \) is odd, and 
if \( a \equiv 3 \) (mod 4), then \( y_5 \) is even.

A general parametric solution of (4.2.1), in the case 
that \( p \) is a prime representable by both forms, \( x_1 \) is odd, 
\( x_2 \) is even, and (necessarily) \( y_6 \) is odd, is given by

\[
\begin{align*}
z_5 &= a(u_0^2+u_1^2+2u_2^2+2u_3^2)+4b(u_0u_3-u_1u_2)+4c(-u_0u_2-u_1u_3) \\
x_1 &= 2a(u_0u_3+u_1u_2)+b(u_0^2+2u_2^2-u_1^2-2u_3^2)+2c(-u_0u_1-2u_2u_3) \\
x_2 &= 2a(-u_0u_2+u_1u_3)+2b(u_0u_1-2u_2u_3)+c(u_0^2+2u_2^2-u_1^2-2u_3^2) \\
y_6 &= N(a) = u_0^2 + u_1^2 - 2u_2^2 - 2u_3^2 \\
y_5 &= (z_5-y_6)/2 = \frac{1}{2}(a-1)(u_0^2+u_1^2)+(a+1)(u_2^2+u_3^2)+2b(u_0u_3-u_1u_2) \\
&+ 2c(-u_0u_2 - u_1u_3) \quad \text{(with } u_0 \equiv u_1 + 1 \text{ (mod 2))}
\end{align*}
\]

where \( a \) is odd, \( b \) is odd, \( c \) is even, and \(-17 = a^2 - 2b^2 - 2c^2\).

At this point we would like to exhibit simple 
relationships among \( x_1, x_2, y_5 \) and \( y_6 \) (mod 17), analogous to 
those obtained in Corollary 2.5; such relationships would be 
used, in an analogous manner, to show that \( f_1 \) never 
represents -1 if \( g_2 \) represents \( p \). What we seek are 
relationships involving the quantities \( u_0, u_1, u_2, u_3, a, b, \) and 
\( c \), which would hold no matter what quaternion \( \tau \) is chosen, 
where \( N(\tau) = -17 = a^2 - 2b^2 - 2c^2 \). Such relationships would 
be obtained if we could assume that, by choosing one, or 
finitely many, values of \( \tau \), we would be assured of obtaining
all parametric solutions of (4.2.1). For example, suppose it could be shown that in order for all such solutions to be obtained by considering the expressions in (4.2.4), it would suffice to consider those expressions using \( \tau_1 = 1 + 3i_2 \) and \( \tau_2 = -1 + 3i_2 \). It would then be possible to prove, for instance, that if \( p \) is a prime represented by \( x_1^2 + x_2^2 \) and \( 2y_5^2 + 2y_5y_6 + 9y_6^2 \) then \( (2y_5 + y_6 + 6x_1|17) = 0 \) or 1. The basic difficulty is that so far, we have not been able to show that all solutions of (4.2.1) are obtainable by using finitely many values of \( \tau \) in the expressions (4.2.4). If this difficulty were surmounted or avoided, any theorems analogous to Theorem 4.2 could be proved.

We are able, however, to obtain a few partial results in the form of the following proposition:

**PROPOSITION 4.3.** Let \( p, f_1, g_1, \) and \( g_2 \) be as in the statement of Theorem 4.2.

(a) If \( (p|17)_4 = 1 \) and \( g_2 \) represents \( p \), or if \( (p|17)_4 = -1 \) and \( g_1 \) represents \( p \), then \( f_1 \) does not represent \(-17\).

(b) If \( (p|17)_4 = -1 \) and \( g_1 \) represents \( p \), then \( f_1 \) represents \(-1\).

(c) If \( (p|17)_4 = 1 \) and \( g_1 \) represents \( p \), then any of the three possibilities \( (f_1 \) represents \(-1, 17, -17) \) can occur.

**PROOF.** (a) This is immediate from part (c) of Theorem 4.1.
Examples of such primes are 13, 89, 101, 137, and the primes in part (b).

(b) By part (a), \( f_1 \) does not represent \(-17\), and by Corollary 2.2.1, \( f_1 \) does not represent 17. Hence \( f_1 \) represents -1. Examples of such primes are 53, 281, 349, 461, and 569.

(c) The following are examples of primes \( p \) represented by \( g \), which satisfy \( (p|17)_4 = 1 \), where any of \(-1, 17, \text{ and } -17\) is represented: for \(-1\), 157; for 17, 149; for \(-17\), 353.

Q.E.D.

Returning to the difficulty mentioned above, several methods of looking at the problem have been used, although none (so far) successfully. One approach is to study the solution of

\[
(4.3.1) \quad p = x_1^2 + x_2^2 = -x_3^2 + 17x_4^2 = 2y_5^2 + 2y_5y_6 + 9y_6^2
\]

in independent parameters; the hope is that one could obtain one parametric solution of

\[
(4.3.2) \quad -x_3^2 + 17x_4^2 = 2y_5^2 + 2y_5y_6 + 9y_6^2
\]

in parameters \( s_0, s_1, s_2, s_3 \), and then adjust the \( s_1 \) to match the expressions for \( x_3 \) and \( x_4 \) in the solutions (2.4.4) or (2.4.5) of \( 17x_4^2 = x_1^2 + x_2^2 + x_3^2 \). This would yield the desired parametric representations of a complete
solution to (4.3.1), by virtue of the previous completeness arguments (see proof of Theorem 1.7 or of Theorem 2.4). So far this method has not yielded the desired results.

An alternate approach is to adjust the parameters \( u_0, u_1, u_2, u_3 \) in the expressions for \( x_1 \) and \( x_2 \) in a particular solution (4.2.4) of equation (4.2.1) in the hope of matching the expressions for \( x_1 \) and \( x_2 \) in either (2.4.4) or (2.4.5), thereby obtaining a complete parametric solution of (4.3.1). In fact, for the choice \( a = 1, b = 3, c = 0 \) in (4.2.4), a transformation has been found which carries the expression for \( x_1 \) in (4.2.4) into the expression for \( x_1 \) in (2.4.4). However, the expressions for \( x_2 \) are not matched by the given transformation; this approach may yet yield the desired results.

A third approach is to examine the expressions in (4.2.4), and to prove directly that all solutions of (4.2.1) are obtained by using only finitely many choices of \( \tau = a_1 + b_2 + c_3 \). One possible way of doing this might be to prove that all solutions of

\[
(4.3.2) \quad -17 = a^2 - 2b^2 - 2c^2
\]

fall into finitely many distinct sets of solutions. This would involve considering the automorphs of the ternary form \( x^2 - 2y^2 - 2z^2 \). So far, this method has not proved fruitful. It is the conviction of the author that Theorem
4.2 is true (by considering a great many examples); as has been said many times before, "All I need is a little proof!"
BIBLIOGRAPHY


AUTOBIOGRAPHY

Ezra Allan Brown was born on January 22, 1944, in Reading, Pennsylvania. He graduated from Isidore Newman High School, New Orleans, Louisiana, in June, 1961. He entered William Marsh Rice University, Houston, Texas, in September, 1961, and was granted the degree of Bachelor of Arts from that institution in June, 1965. He entered the Graduate School of Louisiana State University in September, 1965, and received the degree of Master of Science in the field of Mathematics in August, 1967. Presently he is a candidate for the degree of Doctor of Philosophy in the field of Mathematics at Louisiana State University. Since June 1, 1967, he has had the good fortune to be married to the former Tommie Jo Jones of Arkadelphia, Arkansas.
EXAMINATION AND THESIS REPORT

Candidate: Ezra Allan Brown

Major Field: Mathematics

Title of Thesis: Representations of Discriminantal Divisors by Binary Quadratic Forms

Approved:

Gordon Pall
Major Professor and Chairman

Max Goodrich
Dean of the Graduate School

EXAMINING COMMITTEE:

R. J. Koch

L. E. Dickson

J. R. Durbeck

L. S. Mada

Date of Examination:

July 8, 1969