Representations of a Binary Quadratic Form.

John L. Hunsucker

Louisiana State University and Agricultural & Mechanical College

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

Recommended Citation


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.
HUNSUCKER, John L., 1941-
REPRESENTATIONS OF A BINARY QUADRATIC FORM.

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

University Microfilms, Inc., Ann Arbor, Michigan
REPRESENTATIONS OF A BINARY QUADRATIC FORM

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
John L. Hunsucker
B. S., Lamar State College of Technology, June, 1963
M. S., Louisiana State University, August, 1965
January, 1969
ACKNOWLEDGMENT

The author wishes to express his appreciation for the guidance and assistance of Professor Gordon Pall who supervised this dissertation and without whose advice and encouragement this dissertation could not have been completed.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>11</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER I</td>
<td>3</td>
</tr>
<tr>
<td>CHAPTER II</td>
<td>34</td>
</tr>
<tr>
<td>CHAPTER III</td>
<td>75</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>81</td>
</tr>
<tr>
<td>BIOGRAPHY</td>
<td>82</td>
</tr>
</tbody>
</table>
This paper deals with two questions: reducing the problem of counting the number of imprimitive representations of a binary quadratic form to that of counting the primitive ones and counting the number of representations with a fixed \( g.c.d. \) of a binary as the sum of four squares of linear forms.

In the following \( B \) designates a binary quadratic form with primitive matrix and \( r_4[dB:r] \) represents the number of representations with \( g.c.d. r \) of \( dB \) as the sum of four squares of linear forms.

In Chapter I the properties of generic characters are used to determine the forms \( B \) and divisors \( d \) for which \( r_4[dB:1] \neq 0 \). Then \( r_4[dB:1] \) is determined in terms of ordinal invariants. It is then shown that \( r_4[dB:1] \) is factorable in the sense that

\[
\frac{r_4[d_1B:1]}{r_4[B:1]} \cdot \frac{r_4[d_2B:1]}{r_4[B:1]} = \frac{r_4[d_1d_2B:1]}{r_4[B:1]} \quad \text{for} \quad (d_1, d_2) = 1 \quad \text{and} \quad r_4[B:1] \neq 0.
\]

In Chapter II it is shown that for a fixed \( d, B^{2x2}, n \geq 2, A^{nxn} \) and \( r \) that the number of representations \( T^{nx2} \) of \( g.c.d. r \) such that \( T'AT = dB \) can
be determined by totaling the products of the number of V's such \( \frac{V*d_B V^*}{r^2} \) lies in a fixed order where \( V_{2x2} \) is hermite of determinant \( r \) times the number of primitive representation of a \( \frac{V*d_B V^*}{r^2} \) in that order. The number of such V's such that \( V^*B V^* \) lies in a fixed order is then determined.

In Chapter III the results of Chapter I and Chapter II are used to show that \( r_4[d_B:r] \) is factorable in the sense that

\[
\frac{r_4[d_1B:r]}{r_4[B:r]} \cdot \frac{r_4[d_2B:r]}{r_4[B:r]} = \frac{r_4[d_1d_2B:r]}{r_4[B:r]}
\]

when \( (d_1,d_2)=1 \) and \( r_4[B:r] \neq 0 \). The results of Chapter II are then applied to show how to calculate \( r_4[p^wB:r] \) where \( p \) is a prime in terms of the results of Chapter I.
INTRODUCTION

In this paper we will be dealing with representations of a binary quadratic form by other forms. Let $A^{(n \times n)}$ and $B^{(k \times k)}$ be non-singular, symmetric real matrices, $1 \leq k \leq n$. We say that $A$ represents $B$ if there exists an integral matrix $T_1^{(n \times k)}$ such that $T_1'AT_1 = B$. Here, $T_1$ is called a representation of $B$ by $A$. Two representations are considered equal only if they are identical matrices. We will use $\delta_k(T_1)$ to denote the g.c.d. of the minor determinants of order $k$ in $T_1$. Of $\delta_k(T_1) = 1$, $T_1$ is called a primitive representation.

As regards further notation we will always mean a prime when we write $p$. By $(f|p)$ we will mean the value of the generic character for a form $f$ and an odd prime $p$. If $Q^{(2 \times 2)}$ is a symmetric matrix, by $(Q|p)$ we mean the value of the generic character $(f|p)$ where $f$ is the form associated with $Q$.

We use capital letters $A, \ldots, Z$ to denote matrices unless otherwise indicated. Also $I$ stands for the identity matrix, $A^*$ for the adjoint of $A$, $T'$ for the transpose of $T$, $|f|$ for the determinant of the form $f$; and $T$ unimodular means $T$ is square integral and $|T| = 1$. 

1
It is further assumed that the reader is familiar with the basic properties of binary quadratic forms and in particular with generic characters of forms.

Also we will be dealing only with forms with integer coefficients. All our matrices are integral or quasi-integral. That is, the elements on the diagonal are integers and the elements off the diagonal are integers or halves of integers.
CHAPTER I

Let us first consider an easy representation problem involving the number of representations of a binary quadratic form as the sum of two squares of linear forms.

Theorem 1.1. If \([a, b, c]\) is the sum of two squares of linear forms and \(b^2 - 4ac \neq 0\) then \(b\) must be even, 
\(d = b^2 - 4ac\) is the negative of a square and \(e = (a, b, c)\) is the sum of two squares. Furthermore if \(ac - b^2\) is a non-zero square then the number of representations of \([a, 2b, c]\) as the sum of two squares of linear forms is 
\(2r_2(e)\) where \(r_2(e)\) is the number of representations of 
\(e = (a, b, c)\) as the sum of 2 squares of integers.

Proof: Suppose \(ax^2 + b_1xy + cy^2 = (p_1x + q_1y)^2 + (p_2x + q_2y)^2\).
Then \(a = p_1^2 + p_2^2, c = q_1^2 + q_2^2\) and \(b_1 = 2p_1q_1 + 2p_2q_2\).
So \(b_1\) must be even. Therefore let \(b_1 = 2b\) and our equations become

1) \(a = p_1^2 + p_2^2, c = q_1^2 + q_2^2, b = p_1q_1 + p_2q_2.\)

Observe that \((2b)^2 - 4ac = 4[(p_1q_1 + p_2q_2)^2 - (p_1^2 + p_2^2)(q_1^2 + q_2^2)] = -4(p_1q_2 - p_2q_1)^2.\)
Therefore the discriminant must be the negative of a square, say \(-4t\)? With this notation, \(t^2 + b^2 = ac.\)
Now consider the Gaussian integer $b + it$. Every factorization of this integer as $b + it = (p_1 - p_2)(q_1 + q_2)$ with $p_1^2 + p_2^2 = a$ and $q_1^2 + q_2^2 = c$ yields $b = p_1q_1 + p_2q_2$ and therefore yields a unique quartet $p_1, p_2, q_1, q_2$ that satisfies I). By a theorem of Professor Pall's (see [5] for a generalization) we know that the number of factorizations of a Gaussian integer of norm $b^2 + t^2$ as the product of two Gaussian integers of norm $a$ and $c$ respectively is $r_2(e)$ where $e = (t, b, a, c)$, and that we get $r_2(e)$ different factorizations by considering $b - it$.

Note also that every quartet satisfying 1) corresponds uniquely to a factorization of exactly one of $b + it$ and $b - it$.

**Lemma:** If $(t, b, a, c) = e_1$, $(b, a, c) = e$, and $t^2 + b^2 = ac$ then $e = e_1$.

**Proof:** From the hypothesis $e_1 | e$. Since $e | a, e | c$ and $e | b$ we see that $e^2 | ac - b^2$ or $e^2 | t^2$. So $e | t$.

The next logical step in our discussion would be to consider the number of representations of a binary as the sum of three squares of linear forms. Professor Pall, however, has already taken care of this case in his article [4]. In this paper he derives an algorithm which we will use extensively in the discussion of the number of representations of a binary as the sum of four squares of
Algorithm and Discussion: Let $T_1$ be a primitive representation of $B_1$ by $A$. Where, as before, $B_1$ is $k \times k$, $A$ is $n \times n$ and $T_1$ is $n \times k$ with $1 \leq k < n$. From Professor Pall's article we know there exists a complement $T_2$ of $T_1$ such that $T = (T_1 T_2)$ is unimodular. Then

$$B = T' A T = \begin{bmatrix} T_1' A T_1 & T_1' A T_2 \\ T_2' A T_1 & T_2' A T_2 \end{bmatrix} = \begin{bmatrix} B_1 & K' \\ K & B_2 \end{bmatrix}$$

is equivalent to $A$. Also construct $S' = T^{-1}$, $S = (S_1 S_2)$ with $S_1(n \times k)$ and $S_2(n \times k)$. Then

$$D = B^* = S' C S = \begin{bmatrix} S_1' C S_1 & S_1' C S_2 \\ S_2' C S_1 & S_2' C S_2 \end{bmatrix} = \begin{bmatrix} D_1 & L' \\ L & D_2 \end{bmatrix}$$

where $C = A^*$. Now let $b_1 = |B_1|$ and $d_2 = |D_2|$. On completing squares, that is replacing $B$ by $P'B P$ and $D$ by $P' D Q$ where

$$P = \begin{bmatrix} I_1 & -B_1^{-1} K' \\ 0 & I_2 \end{bmatrix}$$

and

$$Q = \begin{bmatrix} I_1 & 0 \\ -P_2^{-1} L & I_2 \end{bmatrix}$$

$P Q' = Q' P = I$, we arrive at

$$P'B P = \begin{bmatrix} B_1 & 0' \\ 0 & b_1^{-1} G \end{bmatrix}; Q' D Q = \begin{bmatrix} d_2^{-1} E & 0 \\ 0 & D_2 \end{bmatrix}$$

where $G = b_1 B_2 - KB_1^* K'$ and $E = d_2 D_1 - L'D_2^* L$.

These considerations lead us to Professor Pall's Theorem 1.
which follows.

With any primitive representation $T_1$ of $B_1$ by $A$ is associated an aggregate of pairs of matrices $U'GU$ and $U'K + H'B_1$, the aggregate being derivable from any one pair $G + K$ by use of an arbitrary unimodular $U$ and integral $H$. The same matrices $G$ and $K$ are associated with $WT_1$ where $W$ is any unimodular automorph of $A$.

Conversely, for a given $B_1$, $G$, and $K$ such that $KB_1K' \equiv -G \pmod{b_1}$, we can set $G + KB_1^*K' = b_1B_2$.

$$B = \begin{bmatrix} B_1 & K' \\ K & B_2 \end{bmatrix}.$$ If $A$ is equivalent to $B$ and $T$ is a unimodular automorph of $A$ into $B$ then $T_1$ consisting of the first $k$ columns of $T$ is a primitive representation of $B_1$ by $A$.

This algorithm leads us to a method of determining exactly what forms are representable as the sum of four squares of linear forms. This question is equivalent to asking for a form $f$ with matrix $B_1^{(2 \times 2)}$, how many matrices $T_1^{(4 \times 2)}$ exist such that $B_1 = T_1^IT_1$, where $I$ is the $4 \times 4$ identity matrix.

In terms of the above notation if $g$ is a form with matrix $G$, $|G| = b_1$, and there exists a matrix $K^{(2 \times 2)}$ such that $KB_1^*K \equiv -G \pmod{b_1}$ we have $B = \begin{bmatrix} B_1 & K' \\ K & B_2 \end{bmatrix}$. Also
\[
\begin{bmatrix}
I_{2x2} & 0 \\
S' & I_{2x2}
\end{bmatrix}
B
\begin{bmatrix}
I_{2x2} & S \\
0 & I_{2x2}
\end{bmatrix}
= 
\begin{bmatrix}
B_1 & 0 \\
0 & G_{b_1}
\end{bmatrix}.
\]

The determinant of
\[
\begin{bmatrix}
B_1 & 0 \\
0 & G_{b_1}
\end{bmatrix}
= 1
\]
so

B is equivalent to \( I_{4x4} \). Therefore if for a given \( B_1 \) there exist matrices \( G \) and \( K \) such that \( |G| = b_1 \) and

\( KB_1^*K' \equiv -G \mod b_1 \)

then \( f \), the form associated with \( B_1 \), can be represented primitively.

Also it should be noted that if \( KB_1^*K' \equiv -G \mod b_1^S \)

is solvable for every \( p|b_1 \) where \( p^S||b_1 \) then

\( KB_1^*K' \equiv -G \mod b_1 \) is solvable.

Let \( K \) and \( G \) satisfy \( G = -KB_1^*K' \mod b_1 \) where

\( b_1 = |B| = |B_1^*| = |G| \). Solving adjoint-wise through the algorithm we find \( E = B_1^* \) and \( G* = D_2 \). Also \( d_2 = b_1 \) and \( B_1^* = -L'G L \mod b_1 \). This yields two relations between \( B_1^* \) and \( G \).

1) \( G = -K' \mod b_1 \)

2) \( B_1^* = -L'G L \mod b_1 \)

Let \( G = d_1Q \) and \( B_1^* = d_2R \) where \( Q \) and \( R \) are primitive matrices and \( d_1 \) and \( d_2 \) are positive. Then from 1), \( d_2|d_1 \) and from 2), \( d_1|d_2 \). Therefore \( d_1 = d_2 \). So set
d = d_1 = d_2. Note that |Q| = |R| = \frac{b_1}{d^2}. Our two relations now become

3) Q = -KRK' \mod \frac{b_1}{d^2}

4) R = -L'QL \mod \frac{b_1}{d}.

Let \( p^s \parallel b_1/d \) for \( p \) odd. Assume \( T \) and \( S \) are integral matrices with \( |T| = |S| = 1 \) such that \( T'QT \) and \( S'RS \) are congruent mod \( p^s \) to diagonal forms. So we can suppose \( T'QT = \begin{bmatrix} x & 0 \\ 0 & yp^t \end{bmatrix} \) and \( S'RS = \begin{bmatrix} w & 0 \\ 0 & zp^t \end{bmatrix} \mod p^s \)

where \((x,p) = (y,p) = (z,p) = (w,p) = 1\). Then 3) becomes

\[
\begin{bmatrix} x & 0 \\ 0 & yp^t \end{bmatrix} = -K \begin{bmatrix} w & 0 \\ 0 & zp^t \end{bmatrix} K' \mod p^s \text{ where } 0 \leq t \leq s.
\]

Note that if \( Q \), for example, is primitive but the form associated with \( Q \) is not, it will be convenient to write \( T'QT = \begin{bmatrix} 2x & 0 \\ 0 & 2zp^t \end{bmatrix} \), where \((x,2) = (y,2) = 1\). The same holds for \( R \). This will be important later in determining generic characters.

Now consider

\[
\begin{bmatrix} x & 0 \\ 0 & yp^t \end{bmatrix} = -\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} w & 0 \\ 0 & zp^t \end{bmatrix} \begin{bmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{bmatrix} \mod p^s.
\]

This yields

5) \( k_{11}^2 w + k_{12}^2 zp^t = -x \mod p^s \)
6) \( k_{21}w + k_{22} z^p = -yp^t \mod p^s \)

7) \( k_{11}k_{21}w + k_{12}k_{22}z^p = 0 \mod p^s \).

**Theorem 1:** If the forms associated with \( Q \) and \( R \) are primitive and either \( t = 0 \) or \( (Q|p) = (-1|p) \) then the system 5), 6), and 7) is solvable for \( p > 2 \).

**Proof:** Case I: \( t \neq 0 \). \(-x = k_{21}^2w \mod p\) is solvable since \((-x|p) = (w|p)\). Now suppose \(-x = k_{11}^2w \mod p^r\).

Then let \( k_{r+1} = k_r + hp^r \). So \((k_{r+1})^2w = w(k_r^2 + 2k_rhp^r + h^2p^{2r}) = k_rw + 2hk_r^2p^rw \mod p^{r+1}\). Thus

\[
\frac{-k_r + x}{p^r} = 2k_rh \mod p \text{ which has a solution since }
\]

\((k_r, p) = (2, p) = 1\). Take \( k_{12} = k_{21} = 0 \mod p^s\). Then 7) is solvable and 6) reduces to \( k_{22}^2 z^p = -yp^t \mod p^s\). If \( s = t \) this is obviously solvable. If \( t < s \) consider \( k_{22}^2 x = -y \mod p^{s-t}\). This will have a solution if

\((-y|p) = (z|p)\). On considering determinants we see that \( xy^p = wz^p \mod p^s\), or \( xy = wz \mod p^{s-t}\). Since \((-x|p) = (w|p)\), then \((-y|p) = (z|p)\) and Case I is finished.

Case II: \( t = 0 \). Take \( k_{12} = k_{21} = 0 \mod p^s\) first. This case is then the same as Case I, since we can assume, when \( p \nmid \) determinant of \( f_1 \) that \( (w|p) = (-x|p)\).
Lemma: If \( f = [a, 2b, c] \) is i.p., that is \( (a, 2b, c) = 2 \) but \( 2 \nmid b \) then \( |f| = ac - b^2 \equiv 3 \mod 4 \).

Proof: \( ac - b^2 \equiv -b^2 \equiv -1 \equiv 3 \mod 4 \) since \( 2|a, 2|c \) and \( (2, b) = 1 \).

Theorem 2: If \( G \) and \( B_1 \) have the same determinant \( b_1 \equiv 1 \mod 4 \), there exists a solution \( K \) of \( G \equiv -KB_1^*K' \mod b_1 \), \( G \) has the generic character \( (G|p) \) and \( B_1 \) has the generic character \( (G|p) \) then \( (G|p) = (-1|p)(B_1|p) \).

Proof: As before \( G \equiv -KB_1^*K' \mod b_1 \) reduces to
\( Q \equiv -KRK' \mod b_1/d \) where \( Q \) and \( R \) are primitive matrices and are matrices of primitive forms by the above lemma. By definition \( (G|p) = (Q|p) \) and \( (R|p) = (B_1|p) \). Therefore if the form associated with \( Q \) represents \( w \mod p \) then the form associated with \( R \) represents an integer congruent to \( 2 - k_{11}w \mod p \).

Theorem 3: If \( f \) is a positive definite form with determinant \( b_1 \equiv 1 \mod 4 \), then \( f \) is representable primitively as the sum of four squares of linear forms.

Proof: By previous work we need only show the existence of a primitive matrix \( Q \) with associated form \( q \) such that
\( (Q|p) = (-1|p)(R|p) \) if \( p|b_1 \), and \( |Q| = |R| \). Obviously \( |R| \equiv 1 \mod 4 \). Designate this determinant by \( c \). We impose
also on \( Q \) the restriction that \((-1|q) = (-1|f_1)\) and appeal to the product theorem (a statement of which appears later) to show that \( q \) exists.

\[
(-1|q) \prod_{p|c} (q|p) = (-1|f_1) \prod_{p|c} (-1|f_1)(f_1|p) = (-1|c)(1|f_1) \prod_{p|c} (f_1|p)
\]

= 1 since \( c \equiv 1 \mod 4 \) and \((-1|f_1) \prod_{p|c} (f_1|p) = 1 \) by the existence of \( f_1 \). So such a \( q \) exists.

It should be noted that if the prime \( p \) does not divide \( c \) then the congruences 6), 7) and 8) are solvable without placing any further restrictions on the generic characters.

We will now consider the system 5), 6) and 7) in the case where the primitive matrix \( R \) is associated with an imprimitive form. Then we have

\[
\begin{bmatrix}
x \\
0
\end{bmatrix}
\begin{bmatrix}
0 & 1 \\
p & 0
\end{bmatrix}
\begin{bmatrix}
k_{11} & k_{12} \\
k_{21} & k_{22}
\end{bmatrix}
\begin{bmatrix}
w \\
2zp^t
\end{bmatrix}
\begin{bmatrix}
k_{11} & k_{21} \\
k_{12} & k_{22}
\end{bmatrix}
\mod p^s,
\]

which yields

8) \( 2k_{11}w + 2k_{12}zp^t = -x \mod p^s \)

9) \( 2k_{21}w + 2k_{22}zp^t = -y^t \mod p^s \)

10) \( 2k_{11}k_{21}w + 2k_{12}k_{22}zp^t = 0 \mod p^s \).

We will now prove

**Theorem 4**: If the form associated with \( R \) is imprimitive and the form associated with \( Q \) is primitive then if either
t = 0 or \((Q|p) = (-2|p)(R_1|p); \) the system 8), 9), and 10) has solutions, where by \((R_1|p)\) we mean the generic character of the primitive form associated with \(R\). Likewise if \(R\) is associated with a primitive form and \(Q\) is not then if either \(t = 0\) or \((-2|p)(Q_1|p) = (R|p)\) the equation
\[
\begin{bmatrix}
2x & 0 \\
0 & 2yp^t
\end{bmatrix} = -K
\begin{bmatrix}
w & 0 \\
0 & zp^t
\end{bmatrix}
\]
has solutions where by \((Q_1|p)\) we mean the generic character of the primitive form associated with \(Q\).

**Proof:** The proof of both parts of this theorem follow from the proof of Theorem 1. Replace \(2w\) by \(w'\) and \(2z\) by \(z'\) in 8), 9), and 10). Then 8), 9), and 10) become 5), 6), and 7) with \(w\) and \(z\) replaced by \(w'\) and \(z'\) respectively. The generic condition in the first part of this theorem then becomes \((x|p) = (-2|p)(w|p) = (-2|p) = (-w'|p)\) which is what is needed for the proof of Theorem 1.

The second part of this theorem follows from the proof of Theorem 1 by replacing \(x\) and \(y\) by \(2x\) and \(2y\) respectively in 5), 6), and 7).

It will be necessary here to recall the product theorem and the existence theorem for a genus of binary quadratic forms.

**Product Theorem:** Let \(d\) be the discriminant of a primitive
binary quadratic form \( g \). Let \( a \) be a number prime to \( 2d \) which is represented by \( g \). Then

\[
(2|a)^w \cdot (-1|a)^{\frac{e+1}{2}} \cdot \Pi (g|p) = 1 \quad \text{where} \quad d = -2^w e, \ e \text{ odd and} \ p \text{ is an odd prime.}
\]

Existence Theorem: Let \( d \) be a given non-zero integer, \( d \equiv 0 \) or \( 1 \mod 4 \); let \( i = 0 \) if \( d < 0 \), \( i = 1 \) if \( d > 0 \). Assign to the symbols \((f|p)\), for each odd prime dividing \( d \), \((-1|f)\) if \( d \equiv 0 \) or \(-4 \mod 16\), \((2|f)\) if \( d \equiv 0 \) or \(8 \mod 32\), and \((-2|f)\) if \( d \equiv -8 \mod 32\) any values of \(+1\) or \(-1\) consistent with the product relation. Then there exists a primitive form \( f \) with discriminant \( d \) and index \( i \), and the values thus assigned to its generic characters.

Theorem 5: Let \( b_1 \equiv 3 \mod 8 \). If \( f \) is a form whose determinant is \( b_1 \) and \( f = df_1 \) where \( f_1 \) is primitive and has a primitive integral matrix then there exists a form \( g \) with matrix \( G \) such that \( |G| = b_1 \), \( g = dQ \), \( Q \) primitive, \( q \) the form associated with \( Q \) is equal to \( 2q_1 \) with \( q_1 \) primitive and \((q_1|p) = (-2|p)(f_1|p)\) for \( p \) dividing \( |f| \) where \( p > 2 \). Also if the determinant of \( f = b_1 \) and the primitive matrix associated with \( f \) is in turn associated with an imprimitive form, say \( 2f_1 \) then there exists a form \( g \) with matrix \( G \) such that \( |G| = b_1 \), \( G \) has the same divisor as the matrix of \( f \), the primitive
matrix $Q$ associated with $g$ has a primitive form $g_1$ associated with it and $(-2|p)(g_1|p) = (f_1|p)$ for $p$ dividing $|f_1|$, $p$ odd. Thus if a form has its determinant $\equiv 3 \pmod{8}$, it is primitively representable as the sum of four squares of linear forms.

\textbf{Proof:} The discriminant of $f = -4b_1$, the discriminant of $q = -\frac{4b_1}{d^2}$; the discriminant of $q_1 = -\frac{b_1}{d^2}$. Since

$$d^2 \equiv 1 \pmod{8}, \Delta = \text{discriminant of } q_1 \equiv -3 \pmod{8}.$$

So $f_1$ and $q_1$ have only generic characters of the form $(f_1|p)$ and $(q_1|p)$. We will now appeal to the product theorem to show $q_1$ exists.

$$\prod_{p | \Delta} (q_1|p) = \prod_{p | \Delta} (-2|p)(f_1|p) = (-2|\Delta) \prod_{p | \Delta} (f_1|p) = 1.$$ 

So $q_1$ does exist. Now we must show that $2q_1$ has a primitive matrix. Let $q_1 = [a, b, c]$ where $b^2 - 4ac \equiv -3 \pmod{8}$. So $b$ must be odd. Therefore since $(a, b, c) = 1$, $(2a, b, 2c) = 1$ also and $2q_1$ has a primitive matrix.

Obviously this approach will also work for the other half of the theorem. An appeal to Theorem 4 finishes the proof.

\textbf{Theorem 6:} Let $B^*_1 = dR$, $R$ primitive, $|R| = c \equiv 1 \pmod{4}$ and $2^n || d$. If $n = 1$ the form associated with $B^*_1$ is
primitively representable. If \( n \geq 2 \) it is not primitively representable.

**Proof:** Let \( f_1 \) be the form associated with \( R \). Since \( c \equiv 1 \mod 4 \), \( f_1 \) is primitive. Our original congruence is now \( Q \equiv -KRK' \mod dc \). Since \(|Q| = |R| = c \equiv 1 \mod 4 \), \( Q \equiv -KRK' \mod 2 \) is always solvable without imposing any restrictions on the generic characters of \( Q \). Since \( c \equiv 1 \mod 4 \), \( Q \equiv -KRK' \mod c \) is also solvable and the first part of the theorem is proved.

For \( n \geq 2 \) consider \( Q \equiv -KRK' \mod 2^n \). Then since \( n \geq 2 \), \( Q \equiv -KRK' \mod 4 \). Also suppose \( Q \) represents the odd integer \( m \mod 4 \). Then there exists a transformation \( S \) such that \( m \equiv S'QS \equiv -S'KRK'S \mod 4 \). Then \( m' = S'KRK'S \) is obviously a number prime to 2 and represented by \( R \) and \( m \equiv -m' \mod 4 \). Since \( c \equiv 1 \mod 4 \), \( f_1 \) and \( q \) have the respective generic characters \((-1|f_1)\) and \((-1|q)\).

We also know from the product formula that
\[
(-1|q) \prod_{p|c} (q|p) = 1 \text{ if } q \text{ exists. However } (-1|q) = -(1|f_1) .
\]

So
\[
(-1|q) \prod_{p|c} (q|p) = -(1|f_1) \prod_{p|c} (-1|p) = -(1|f_1)(-1|c) \prod_{p|c} (f_1|p) = -1 .
\]

So we have no such \( q \).

At this point it will be convenient to recall some well known facts about binary quadratic forms.
Lemma: Let $f = 2^a[a,2b,c]$ where $(a,2b,c) = 1$ or $(a,2b,c) = 2$, $b$ odd. If $ac - b^2 \equiv 1 \pmod{4}$, or $ac - b^2 \equiv 3 \pmod{4}$ and $(a,2b,c) = 1$, or $ac - b^2 \equiv 7 \pmod{8}$ and $(a,2b,c) = 1$, or $ac - b^2 \equiv 0 \pmod{2}$ then $f$ is equivalent to a form of the type $[2^{-m},0,2^{2n}]$ modulo an arbitrarily large power of 2. If $ac - b^2 \equiv 3 \pmod{8}$ and $(a,2b,c) = 2$, $b$ odd then $f$ is equivalent to a form of the type $2^a[2,2,2]$. If $ac - b^2 \equiv 7 \pmod{8}$ and $(a,2b,c) = 2$, $b$ odd then $f$ is equivalent to a form of the type $2^a[0,2,0]$.

Theorem 7: Let $B_1^* = dR$ where $R$ is primitive and $2^p || d$, $|R| = c \equiv 3 \pmod{8}$. Then there are no primitive representations for $n > 0$.

Proof: Again consider $Q = -KRK'$ mod $dc$. In order to solve this mod $c$ we know that one of $Q$ and $R$ is p.p. and the other i.p. Suppose $Q$ is p.p. Then $Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ mod 2. Our congruence then becomes $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{bmatrix} = \begin{bmatrix} 2k_{12}k_{11} & \cdots \\ k_{12}k_{21} + k_{11}k_{22} & \cdots \end{bmatrix}$ mod 2.

This implies $1 = 2k_{12}k_{11}$ mod 2, an obvious contradiction.

Now suppose $Q$ is i.p. Our congruence is then

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{bmatrix}$.
\[
\begin{bmatrix}
    k_1^2 + k_{12}^2 & k_{11}k_{21} + k_{12}k_{22} \\
    k_{11}k_{21} + k_{12}k_{22} & k_{21}^2 + k_{22}^2
\end{bmatrix} \mod 2.
\]

This implies \( k_{11}^2 + k_{12}^2 \equiv k_{21}^2 + k_{22}^2 \equiv 0 \mod 2 \) and \( k_{11}k_{21} + k_{12}k_{22} \equiv 1 \mod 2 \). Then \( k_{11}^2 + k_{12}^2 = 0 \) implies \( k_{11} \equiv k_{12} \mod 2 \). Likewise we see that \( k_{21} \equiv k_{22} \mod 2 \).

So our last congruence becomes \( 2k_{12}k_{21} \equiv 1 \mod 2 \), a contradiction.

It will be convenient to recall here the fact that if \( f \) is a form with determinant \( \equiv 7 \mod 8 \) then \( f \) has only generic characters of the form \((f_1|p)\).

Theorem 8: Let \(|B_1^*| = b_1 = d^2c, c \equiv 7 \mod 8\). Then there are no primitive representations.

Proof: Using the previous notation let \( B_1^* = dR \) and \( f_1 \) be the form associated with \( R \). Either \( f_1 \) is p.p. or i.p.. In the first case \( f_1 \) has discriminant \( \equiv 4 \mod 32 \) and in the second the p.p. form associated with \( f_1 \) has odd discriminant. Suppose there does exist a matrix \( Q \) satisfying the congruence \( Q \equiv -KRK' \mod dc \) and \(|Q| = c\). Then \( q \) the form associated with \( Q \) is either p.p. or i.p. and like \( f_1 \) has only \((q|p)\) where \( p|c \) as a generic character.

Let us now assume \( f_1 \) is p.p. and \( q \) is p.p.. The
matrix congruence then yields $-x \cdot k_{12}^2 w = k_{12}^2 z p^t \mod p^s$ for $p \mid c$, $p$ odd. This implies $(-q \mid p) = (f_1 \mid p)$ for $p \mid c$, $p$ odd. Then however
\[ \prod_{p \mid c} (q \mid p) = \prod_{p \mid c} (-1 \mid p)(f_1 \mid p) = (-1 \mid c) \prod_{p \mid c} (f_1 \mid p) = -1. \]
So no such $q$ can exist.

Let us now suppose that $f_1$ is p.p. and $q$ is i.p. Our matrix congruence then yields $-2 x \cdot k_{12}^2 w = k_{12}^2 z p^t \mod p^s$ for $p \mid c$. Therefore $(-2q \mid p) = (f_1 \mid p)$ for $p \mid c$. Then
\[ \prod_{p \mid c} (q \mid p) = \prod_{p \mid c} (-2 \mid p)(f_1 \mid p) = (-2 \mid c) \prod_{p \mid c} (f_1 \mid p) = -1. \]
So no such $q$ exists.

If we suppose that $q$ is p.p. and that $f_1$ is i.p. or that both $q$ and $f_1$ are i.p. then by applying the methods used in the other cases we see that $q$ does not exist.

**Theorem 9:** Let $b_1 = d^2c$, $c = 2^w c'$ where $(c', 2) = 1$ and $w \geq 2$. Then there are no primitive representations.

**Proof:** If we suppose that $Q$ exists the congruence immediately yields $(-1 \mid q) = -(-1 \mid f_1)$ and $(q \mid p) = (-1 \mid p)(f_1 \mid 1)$ for $p \mid c$.

Let us now consider the case where $w$ is even. The left hand side of the product relation becomes
\[ (-1 \mid q)^{c' + 1} \prod_{p \mid c} (q \mid p) = [(-1 \mid f_1)]^{c' + 1} (-1 \mid c') \prod_{p \mid c'} (f_1 \mid p) = (-1)^{c'} = -1. \] So no such $q$ exists when $w$ is even.
In the case where \( w \) is odd, \( w \geq 3 \). From the congruence we see that if \( q \) represents \( m \mod 8 \), \( m \) odd then \( f_1 \) represents an integer \( m' \mod 8 \) such that \( m \equiv -m' \mod 8 \). From this we see

\[
(2|q) = (2|m) = (-1) \frac{m^2-1}{8} = (-1) \frac{m'^2-1}{8} = (2|f_1)
\]

So

\[
\prod_{p|c'} (q|p) \cdot (2|q) \cdot (-1|q) \frac{c'+1}{2} = \prod_{p|c'} f_1|p \cdot (2|f_1) \cdot (-1) \frac{c'+1}{2} \cdot (-1|f_1) \frac{c'+1}{2} = -1.
\]

So no such \( q \) exists.

**Theorem 10:** Let \( b_1 = d^2c \), \( c = 2c' \), \((c',2) = (d,2) = 1\). Then \( B_1 \) has primitive representations.

**Proof:** Since \( 2||c \) we can take \( R = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \mod 2 \). Likewise we can assume if \( |Q| = |R| \) that \( Q \equiv R \mod 2 \). So \( Q \equiv -KRK' \mod 2 \) is solvable without any restrictions on the generic characters of \( Q \). For our congruence to be solvable module \( c' \) we require only that \((q|p) = (-1|p)(f_1|p)\). On examining the product relation we see that \( Q \) has generic characters with respect to 2 appearing to the first power. These can be adjusted to satisfy the product relation and guarantee the existence of \( Q \) such that \( Q \equiv -KRK' \mod dc \) for some \( K \).
Theorem 11: Let \( b_1 = d^2c, c = 2c', (c', 2) = 1 \) and \( 2\|d \). Then \( B_1 \) can be primitively represented.

Proof: Let us first consider \( c' \equiv 1 \mod 4 \). Then \((-2|4)\) is the only kind of generic character with respect to 2 that either \( Q \) or \( R \) can possess where \(|Q| = c\). Let us restrict \( Q \) further by requiring that \((-2|q) = (-2|f_1)\).

Then it is well known that \( q \) and \( f_1 \) represent the same odd numbers \( \mod 4 \). So let us assume \( Q \equiv R \equiv \begin{bmatrix} m_1 & 0 \\ 0 & 2m_2 \end{bmatrix} \mod 4 \)

where \( m_1m_2 \equiv 1 \mod 4 \). The congruence \( Q = -K_{RP} \mod 4 \)
yields \(-m = k_{11}m_1 + 2k_{12}m_1 \mod 4, 0 = k_{11}k_{21}m_1 + 2k_{12}k_{22}m_1 \mod 4 \)
and \( 2m_1 = k_{21}m_1 + 2k_{22}m_1 \mod 4 \). If we choose
\( k_{11} = k_{12} = k_{22} \equiv 1 \mod 4 \) and \( k_{21} \equiv 2 \mod 4 \) then this system of congruences is satisfied. If we further require
\((-1|p)(q|p) = (f_1|p)\) then the matrix congruence
\( Q = -K_{RP} \mod p^s \) has solutions where \( p^s || c' \).

The left hand side of the product relation becomes
\((-2|q)_p(q|p) = (-2|f_1)_p(f_1|p) =
(-2|f_1)(-1|c')_p(f_1|p) = 1. \) So a form \( q \) with the necessary values of its generic characters exists.

Let \( Q \equiv \begin{bmatrix} m_1 & 0 \\ 0 & 2m_2 \end{bmatrix} \) and \( R \equiv \begin{bmatrix} t_1 & 0 \\ 0 & 2t_2 \end{bmatrix} \mod 4 \)

where \( m_1m_2 \equiv t_1t_2 \equiv c' \equiv 3 \mod 4 \). Our congruences then become
\(-m_1 \equiv k_{11}^2t_1 + 2k_{12}^2t_2 \mod 4, 0 \equiv k_{11}k_{21}t_1 + 2k_{12}k_{22}t_2 \mod 4,\)
2m_2 \equiv k_1^2 + 2k_2^2 \mod 4. \text{ It } m_1 \not\equiv t_1 \mod 4 \text{ then } k_{12} \equiv k_1 \equiv 0 \text{ and } k_{11} \equiv k_2 \equiv 1 \mod 4 \text{ is a solution. If } m_1 \equiv t_1 \mod 4 \text{ then } k_{11} \equiv k_{12} \equiv k_2 \equiv 1 \text{ and } k_1 \equiv 2 \mod 4 \text{ is a solution. If we also require } (-1|p)(q|p) = (f_1|p) \text{ then the matrix congruence is solvable mod } p^8 \text{ where } p^8 \mid c'.

On examining the product relation we see that (2|q) occurs to the first power. Since we have made no requirements on Q regarding this character, it can be adjusted to make the lefthand side equal to 1 and thus guarantee the existence of q.

**Theorem 12:** Let \( b_1 = d^2c, \ 2\|c, \ c = 2c', \ 2^t\|d \text{ and } t > 1. \) Then there are no primitive representations.

**Proof:** Consider \( Q = -K\mathbb{R} \mod 8. \) If \( q \) represents \( m \mod 8 \) then \( f_1 \) represents \( -m \mod 8. \) Also it is easily shown that \( (2|m) = (2|-m) \) and that \( (-1|m) = (-(-1|-m)). \) We also know that \( (q|p) = (-1|p)(f_1|p) \) for \( p|c' \) or else we have no solution to the matrix congruence. On examining the lefthand side of the product relation we see that

\[
(2|m)(-1|m) \frac{c'+1}{2} \prod_{p|c'}(q|p = (2|-m)[-(-1|-m)] \frac{c'+1}{2} .
\]

\[
\frac{c'+1}{2} \prod_{p|c'}(-1|p\cdot(f_1|p) = (2|-m).(-1|-m) \frac{c'+1}{2} . \prod_{p|c'}(-1|f_1).(-1)^c' = 1\cdot(-1)^c' = -1. \text{ So } q \text{ does not exist.}
\]

We will now determine the number of primitive
representations of a form. Let \( r_4[B_1:m] \) be the number of primitive representations \( T_1 \) such that \( \delta_2(T_1) = m \). Then from Professor Pall's article [4] we see that
\[
r_4[B_1:1] = w \prod_{j=1}^{n} \rho(G^j_j) \]
where \( u_j \) is the number of unimodular automorphs of \( G^j \), \( \rho(G^j) \) denotes the number of solutions \( K \) of \( KB_1^*K' = -G^j \mod b_1 \) which are incongruent modulo \( B_1 \), \( w \) is the number of unimodular automorphs of \( L^{4x4} \) and \( G^1, \ldots, G^n \) is a collection of matrices one from each class of the allowable solution genera. Our problem is now to determine \( \rho(G^j) \).

First let us determine the number of solutions \( K \) of \( G = -KB_1^*K' \mod b_1 \) for a fixed \( G \) with \( K \) determined modulo \( b_1 \). Using the same notation as before we will consider \( Q = -KRK' \mod dc \). It should be recalled that \( p^s \mid dc, p^t \mid c, 0 \leq t \leq s, s \neq 0 \) and \( p^{2s-t} \mid b_1 \). The letter \( p \) will designate an odd prime.

We will need the following lemmas.

**Lemma:** \( x^2 + m \equiv p \) for \( p^{-\frac{m}{2}} \pmod{p} \)
\[
\begin{align*}
1 & \quad \text{for } p^{-\frac{2}{2}} \equiv (-m \pmod{p}) \\
0 & \quad \text{for } 1 + (-m \pmod{p})
\end{align*}
\]
values of \( x \pmod{p} \) when \( (m,p) = 1 \).

**Proof:** Consider \( m = y^2 - x^2 \equiv (y-x)(y+x) \pmod{p} \). Let \( u = y-x, v = y+x \). Then there exist \( p-1 \) ordered pair \( u,v \) such that \( m = uv \pmod{p} \). Therefore, since \( u = y-x, \)
v = y + x is solvable for x and y, there exist p - 1 ordered pairs x,y such that m + x^2 = y^2 mod p. However there are 1 + (-m|p) values of x such that y^2 is 0 in this set. So there are p - 1 - [1 + (-m|p)] = p - 2 - (-m|p) sets of ordered pairs x,y such that m + x^2 = y^2 mod p and y ≠ 0. Also for each x there are two y's, ± y. So there are \( \frac{p-2-(-m|p)}{2} \) values of x such that \( (x^2 + m|p) = 1 \).

Since there are obviously 1 + (-m|p) values of x for which \( (x^2 + m|p) = 0 \) we have \( p - \left[ \frac{p-2-(-m|p)}{2} + 1 + (-m|p) \right] = p - (-m|p) \) values of x for which \( (x^2 + m|p) = -1 \).

**Lemma:** \((ax^2 + m|p) = -1\) for \( \frac{p-(-am|p)}{2} - \frac{1-(a|p)}{2} \) where \( (a,p) = (m,p) = 1 \).

**Proof:** We first observe that

\[ (a \lambda^2 + m|p) = (a|p)(\lambda^2 + am|p) = -(a|p) \text{ for } \frac{p-(-am|p)}{2} \text{ values} \]

and \((a|p)\) for \( \frac{p-2-(-am|p)}{2} \) values of x mod p. Comparing this last statement with the statement of our lemma we see the two statements are the same in the two cases \((a|p) = 1\) and \((a|p) = -1\).

**Lemma:** Let \( f[-x,p] \) be the number of solutions \( k_{11}, k_{12} \)
of \( k_{11}^2 w + k_{12}^2 z p^t \equiv -x \mod p^s \). If \( t \nmid 0 \) then 
\[ f[-x,p^s] = 2p^s \text{ or } 0. \] 
If \( t = 0, s \nmid 0 \) then 
\[ f[-x,p^s] = p^{s-1}[p^{-(wz|p)}] \text{ or } 0 \] 
where \((x,p) = (w,p) = (z,p) = 1\).

**Proof:** Assume first that \( f[-x,p^s] \nmid 0 \). Consider the case 
where \( t \nmid 0 \). Then \((w|p) = (-x|p)\). Rewriting our congruence 
as \( k_{11}^2 w = -x - k_{12}^2 z p^t \mod p^s \) we see that for \( k_{12} \) a fixed 
residue there are two \( k_{11}'s \) which satisfy the congruence. 
So there are \( 2p^s \) solutions.

In the case where \( t = 0 \) transform the congruence into 
k\(^2 = -x - ah^2 \mod p^s \) where \( k = wk_{11}, a = wz \) and \( h = k_{12} \). 
There are \( p^{-(ax|p)} - \left(\frac{1+(a|p)}{2}\right) \) values of \( h \mod p \) which 
make \( (-x - ah^2|p) = 1 \). So there are 
\[ 2p^{s-1}[p^{-(ax|p)} - \left(\frac{1+(a|p)}{2}\right)] \] 
values of \( h,k \mod p^s \) with 
k \nmid 0 \mod p \ which satisfy the congruence.

If \( p|k \) we must have \( (-ax|p) = 1 \). Any such \( k \) yields 
2 \( h \)'s and there are \( p^{s-1} \) such \( k \)'s. So we have 
\[ 2p^{s-1}[\frac{1+(a|p)}{2}] \] pairs \( h,k \) where \( p|k \). On adding we get 
\[ p^{s-1}[p^{-(a|p)}] = p^{s-1}[p^{-(wz|p)}] \] solutions.

**Theorem 13:** Let \( t \nmid 0, t < s \). Then there are 
\[ 2p^{4s-3t} f[-x,p^s] \] solutions of 5), 6), and 7) where \( K \) is 
determined \mod p^{2s-t}.

**Proof:** Let \( k_{11},k_{12} \) be a solution of 5). Then \( k_{11} \nmid 0 \mod p \)
On considering 7) we see that $k_{21} \equiv -z p^t k_{12} k_{22} \mod p^s$.

So $k_{21}$ is determined by $k_{11}, k_{12}$ and $k_{22}$. By 6)

$$z^2 p^{2t} k_{12}^2 \frac{k_{22}^2 + z p^t k_{22}^2}{k_{11}^2} \equiv -y p^t \mod p^s \text{ or}$$

$$k_{22} \left[ \frac{z^2 p^t}{k_{11}^2} + z \right] \equiv -y \mod p^{s-t}.$$ So we must have $(k_{22}, p) = 1$.

Let $C = \frac{k_{12}^2 z^2 p^t}{k_{11}^2} + z$. Then $(C, p) = 1$ and our congruence becomes $C k_{22} \equiv -y \mod p^{s-t}$. Since $(C | p) = (z | p) = (-y | p)$ we have two solutions $k_{22} \mod p^{s-t}$. So we have $2 p^t$ solutions $k_{22} \mod p^s$ for each pair $k_{11}, k_{12}$. Therefore we have $2 p^t f[-x, p^s]$ solutions with $K$ determined mod $p^s$ but $K$ should be determined mod $p^{2s-t}$. Consider $k + q p^s$ where $q = 1, \ldots, p^{s-t}$. There are $p^{s-t}$ such numbers incongruent mod $p^{2s-t}$ but congruent mod $p^s$. Therefore since $K$ has four elements, for any solution mod $p^s$ we have $p^{4s-4t}$ solutions mod $p^{2s-t}$. So we have $2 p^t p^{4s-4t} f[-x, p^s] = 2 p^{4s-3t} f[-x, p^s]$ solutions mod $p^{2s-t}$.

**Theorem 14:** For $t = s \neq 0$ there are $p^{sf}[-x, p^s]$ solutions $K$ of 5), 6) and 7) with $K$ determined mod $p^{2s-t}$.

**Proof:** Let $k_{11}, k_{12}$ be a solution of 5). Then $(k_{11}, p) = 1$. On examining 7) we see that $k_{11} k_{21} \equiv 0 \mod p^s$. So $k_{21} \equiv 0 \mod p^s$. Then 6) reduces to $0 \equiv 0 \mod p^s$. So $k_{22}$
has no restrictions and there are \( p^s f[-x, p^s] \) solutions \( K \mod p^s \). Since \( 2s - t = s \) there are \( p^s f[-x, p^s] \) solutions \( \mod p^{2s-t} \).

**Theorem 15:** For \( t = 0, s \neq 0 \) there are \( 2p^{4s} f[-x, p^s] \) solutions of 5), 6) and 7) with \( K \) determined \( \mod p^{2s-t} \).

**Proof:** Let \( k_{11}, k_{12} \) be a solution of 5). One of these must be prime to \( p \), say \( k_{11} \). On examining 7) we see that

\[
k_{21} = -k_{12} k_{22} z \mod p^s.
\]

Then from 6)

\[
k_{22}^2 = \frac{k_{12}^2 z + k_{11}^2 w}{k_{11} w} \quad [k_{12}^2 z + k_{11}^2 w] \cdot k_{22}^2 (-xz) = y \mod p^s.
\]

Since the coefficient of \( k_{22} \) is prime to \( p \) we have two solutions \( k_{22} \mod p^s \). An equivalent procedure shows that we have two solutions if \( p \mid k_{11} \) and \( p \nmid k_{12} \). Therefore we have

\( 2f[-x, p^s] \) solutions \( K \mod p^s \), but again we need the number \( \mod p^{2s} \). Using the same procedure as before we see that we have \( 2p^{4s} f[-x, p^s] \) solutions \( K \) with \( K \) determined \( \mod p^{2s-t} \).

**Theorem 16:** For \( d \equiv 2 \mod 4 \) and \( c \equiv 1 \mod 4 \) there are \( 2^5 \) solutions \( K \) of \( G \equiv -KB_1 K' \mod 4 \) with \( K \) determined \( \mod 4 \).

**Proof:** Since \( c \) is odd we can consider \( Q = [\begin{array}{l} 1 \\ 0 \end{array}] \mod 2 \). Since \( 2 \nmid d c \) we will consider \( Q = K \mod 2 \). This yields the congruences

\[
k_{11}^2 + k_{12}^2 \equiv 1, \quad k_{21}^2 + k_{22}^2 \equiv 1 \quad \text{and} \quad k_{21}^2 k_{11} + k_{12}^2 k_{22} \equiv 0 \mod 2.
\]

Let \( k_{11}, k_{12} \) be one of the two solutions
to the first congruence. One of $k_{11}$ and $k_{12}$ is prime to 2 and the other is not. If $k_{11}$ is prime to 2 then $k_{21}$ is determined from the last congruence where $i = 1$ or 2. The last $k$ is then determined from the third congruence. So we have 2 solutions $K$ mod 2 and $2^5$ solutions $K$ with $K$ determined mod 4.

Theorem 17: For $c = 2c'$, $(d, 2) = (c', 2) = 1$, there are 4 solutions $K$ of $G = -KB_1K'$ mod 2 with $K$ determined mod 2.

Proof: Since $2\| c$, $Q$ and $R$ can be taken congruent to $[1 0] \mod 2$. Our congruences then become $k_{11}^2 = 1, k_{11}k_{21} = 0$ and $k_{21}^2 = 0 \mod 2$. So $k_{11}$ and $k_{21}$ are determined and we have two choices for each of $k_{12}$ and $k_{22}$. So there are 4 solutions $K$.

Theorem 18: For $c = d = 2 \mod 4$ there are $2^7$ solutions $K$ of $G = -KB_1K'$ mod 8 with $K$ determined mod 8.

Proof: On examining $c$ we see that we can take $Q = [0 m_1 0] \mod 4$ and $R = [0 q_1 0 \mod 4$. Our congruence $Q \cdot K \cdot R \cdot K' \mod 4$ then can be expressed as $-m_1 \equiv k_{11}^2 q_1 + 2k_{12}^2 q_2 \mod 4$, $2m_2 \equiv k_{21}^2 q_1 + 2k_{22}^2 q_2 \mod 4$ and $0 = k_{11}k_{21}q_1 + 2k_{12}k_{22}q_2 \mod 4$. Let $k_{11}, k_{12}$ be a solution of the first of these. Then $(k_{11}, 2) = 1$. On considering the last we see that $k_{21} = \frac{2k_{12}k_{22}q_2}{k_{11}q_1} \mod 4$. So $2 | k_{21}$ and the middle congruence reduces to $2m_2 \equiv 2k_{22}^2 q_2$. This implies that $k_{22}$ is odd. So
we have 2 solutions of the system for each solution of the first congruence. Therefore since the first congruence has 4 solutions mod 4 we have 8 solutions \( K \) with \( K \) determined mod 4 and \( 2^7 \) solutions \( K \) with \( K \) determined mod 8.

On examining the last few theorems we see that the number of solutions \( K \) of \( G \equiv -KB_1^*K' \mod b_1 \) depends only on ordinal invariants of \( G \) and \( B_1^* \) and therefore only on ordinal invariants of \( B_1 \). Let \( S(b_1) \) denote the number of solutions \( K \) of \( G \equiv -KB_1^*K' \mod b_1 \) where \( B_1 \) is a representable matrix, \( G \) is a fixed matrix associated with \( B_1 \) by our algorithm and \( K \) is determined mod \( b_1 \). Let \( s(p) \), \( p \) odd, denote the number of solutions mod \( p^{2s-t} \) where \( K \) is determined mod \( p^{2s-t} \). Let \( \epsilon(2) \) denote the number of solutions mod \( 2^r \) where \( 2^r \mid b_1 \). As usual \( p^{2s-t} \mid b_1 \), \( p^{s-t} \mid d \), \( p^t \mid c \), \( p^s \mid dc \) and \( b_1 = d^2c \). The results of the preceding theorems can then be compiled in the following theorem.

**Theorem 19:** We have \( S(b_1) = \epsilon(2) \prod_{p \mid b_1} s(p) \) where

\[
\begin{align*}
s(p) &= 2^2 p^{5s-3t} & \text{for } t \neq 0, t < s \\
&= 2p^{2s} & \text{for } t = s \neq 0 \\
&= 2p^{5s-1}[p - (-c|p)] & \text{for } t = 0, s \neq 0
\end{align*}
\]
and $\varepsilon(2) = 1$ for $b_1 \equiv 1 \mod 4$ or $b_1 \equiv 3 \mod 8$

$2^5$ for $c \equiv 1 \mod 4$, $d \equiv 2 \mod 4$

$2^2$ for $c \equiv 2 \mod 4$, $d$ odd

$2^7$ for $c \equiv 2 \mod 4$, $d \equiv 2 \mod 4$.

Let $K$ and $G$ satisfy $G \equiv -KB_1^*K' \mod b_1$. Since $B_1B_1^* = b_1I$, if $K$ satisfies the congruence so does $K + H'B_1$ with $H(2 \times 2)$ any integral matrix. These matrices are said to form a right sided residue class modulo $B_1$ and two of them in the same right sided residue class are said to be congruent mod $B_1$ or right congruent mod $B_1$. Therefore in order to determine the number of solutions to the congruence with $K$ determined mod $B_1$ we need to know how many $K + H'B_1$'s we have with $H$ determined mod $b_1$.

**Theorem 20:** Let $B_1$ be a matrix which is primitively representable. There are $p^{2k}$ solutions $M$ of $MB_1 \equiv 0 \mod p^k$ when $p^k || b_1$. Furthermore if $S(B_1)$ is the number of solutions of $G \equiv -KB_1^*K' \mod b_1$ with $K$ determined mod $B_1$ then

$$S(B_1) = \frac{S(b_1)}{b_1^2}.$$

**Proof:** Let $b_1$ be an exceptable determinant. Let $p$ be any prime such that $p | b_1$. Then $B_1$ can be taken congruent to

$$\begin{bmatrix} x_1 & 0 \\ 0 & y_1 \end{bmatrix} \mod p^k$$

when $p^k || b_1$ and $1 + j = k$. On
considering \[
\begin{bmatrix}
m_1 & m_2 \\
m_3 & m_4
\end{bmatrix}
\begin{bmatrix}
xP^1 \\
yP^j
\end{bmatrix} = 0 \text{ mod } p^k
\] we get the congruences \( m_1 xP^1 \equiv m_3 xP^1 \equiv m_2 yP^j \equiv m_4 yP^j \equiv 0 \text{ mod } p^k \).

Therefore we want \( p^j | m_1 \), \( p^j | m_3 \), \( p^i | m_2 \) and \( p^i | m_4 \). So we have \( p^i \) acceptable values of \( m_1 \), \( p^i \) acceptable values of \( m_3 \), \( p^j \) acceptable values of \( m_2 \) and \( p^j \) acceptable values of \( m_4 \). So there are \( p^{2k} \) solutions \( M \).

The last part of the theorem becomes obvious when we observe that any solution \( K \) has \( b_1^2 \) matrices \( K + H'B_1 \) associated with it.

Let us now recall the formula \( r_4[b_1:1] = \frac{p}{\prod_{j=1}^{n} \rho \left( \frac{G_j^d}{u_j} \right)} \).

We see from the preceding theorems that \( \rho(G_j^d) = S(B_1) \) for \( j = 1, \ldots, n \). Also we know that \( w = 192 \) and that since all the \( G_j^d \) belong to the same order, \( u_1 = u_2 = \ldots = u_n \). Therefore \( r_4[B_1:1] = 192 \cdot S(B_1) \cdot \frac{n}{u} \) where \( u = u_1 = \ldots = u_n \).

**Theorem 21:** Let \( R \) be a primitive matrix of a form which has primitive representations. Let \( |R| = c = p_1^{t_1} \ldots p_s^{t_s} \).

Let \( d \) be an integer such that \( dR \) has primitive representations and \( d = p_1^{n_1} \ldots p_s^{n_s} \ldots p_k^{n_k} \). Then

1) \( S(dR) = 2^y \cdot d \cdot \prod_{p | q} \left[ 1 - \frac{(-c | p)}{p} \right] \) where \( y \) is the number of odd primes in \( d \) plus the number of odd primes in \( c \) (some primes may be counted twice) and \( q \) is the product of the
odd primes \( p \) such that \( p \mid d \) but \( p \nmid c \).

2) \( r_4[(R:1)] = 192 \cdot \frac{p}{u} \cdot d \cdot 2^y \cdot \prod_{p \mid q} \left[ 1 - \frac{(-c|p)}{p} \right] \)

3) \( r_4[(R:1)] = r_4[(R:1)] \cdot d \cdot 2^x \cdot \prod_{p \mid q} \left[ 1 - \frac{(-c|p)}{p} \right] \)

when \( x \) is the number of odd primes in \( d \).

Proof: Let us first determine \( S(dR) \).

Case 1: \( d \) odd and \( c \) odd. From Theorems 19 and 20 we see that \( S(dR) = \frac{S(d^2c)}{d^2c^2} \)

\[
P_1 \cdot \frac{2^{t_1} \cdot \prod_{p \mid q} 2^{t_1+5n_1} \cdot \prod_{s+1} 2^{n_1} \left[ 1 - \frac{(-c|p)}{p} \right]}{2^{t_1+5n_1} \cdot \prod_{s+1} 2^{n_1} \left[ 1 - \frac{(-c|p)}{p} \right]}
\]

is proved in this case.

Case 2: \( c \) odd and \( d \) even. Let \( p_k = 2 \) then \( n_k \) must be 1 or else \( dR \) has no primitive representations. Then we see from Theorems 19 and 20 that \( S(dR) = \frac{S(d^2c)}{d^2c^2} \)

\[
2^5 \cdot \frac{2^{t_1} \cdot \prod_{w+1} 2^{t_1+5n_1} \cdot \prod_{s+1} 2^{n_1} \left[ 1 - \frac{(-c|p)}{p} \right]}{2^{t_1+5n_1} \cdot \prod_{s+1} 2^{n_1} \left[ 1 - \frac{(-c|p)}{p} \right]}
\]

\[
2^{k+s-w-1} \cdot \left[ 2^k \cdot \prod_{w+1} s \cdot \prod_{s+1} 2^{t_1+5n_1} \cdot \prod_{s+1} s \cdot \prod_{s+1} 2^{n_1} \left[ 1 - \frac{(-c|p)}{p} \right] \right]
\]

Therefore 1) is proved in this
case.

Case 3: c even and d odd. Let $p_1 = 2$. Then $f_1$ must be 1 or else $R$ has no primitive representations. We then have $S(dR) = S'(d^2c) = 2^{2t_1} \cdot 2^{2t_1+5n_1} \cdot \prod_{i=1}^{k-1} 2^{5n_i} \{1 - (-c|p_1)\} \cdot d^{-4} \cdot c^{-2} = 2^{k+s-w-1} \cdot d \cdot \prod_{i=1}^{k-1} 2^{5n_i} \{1 - (-c|p_1)\}$

and 1) is proved in this case.

Case 4: c even and d even. Let $p_{w+1} = 2$. Then $n_{w+1} = t_{w+1} = 1$. From Theorems 19 and 20 we have $S(dR) = \frac{s(d^2R)}{d^2c^2} = 2^{7} \cdot \prod_{i=1}^{k} 2^{p_1} \cdot 2^{2t_1+5n_1} \cdot \prod_{i=1}^{k-1} 2^{5n_i} \{1 - (-c|p_1)\} \cdot d^{-4} \cdot c^{-2} = 2^{k+s-w-2} \cdot d \cdot \prod_{i=1}^{k-1} 2^{5n_i} \{1 - (-c|p_1)\}$ and 1) is proved in this last case.

Part 2) of the theorem is an obvious consequence of our previous work now that we have determined $S(dR)$.

In order to prove 3) we must first recall that the number of unimodular automorphs of $G$ and $dG$ are the same and that the number of classes in the genus of $G$ is the same as the number of classes in the genus of $dG$. Then from 2) of this theorem we see that $r_4[R:1] = 192 \cdot \frac{m_1}{u_1} \cdot 2^{y_1}$ and $r_4[dR:1] = 192 \cdot \frac{m_d}{u_d} \cdot d \cdot 2^{y_d} \cdot \prod_{i=1}^{p|q} \{1 - (-c|p)\}$ where $m_1, u_1$ and $m_d, u_d$ are associated with $R$ and $dR$ respectively.
as in our previous work, \( y_1 \) is the number of odd primes in \( c \) and \( y_d \) is the number of odd primes in \( d \) plus the number in \( c \). Since \( m_1 = m_d \) and \( u_1 = u_d \) we have

\[
\begin{align*}
\frac{r_4[dR:1]}{r_4[R:1]} &= 192 \cdot 2^{y_1} \cdot \frac{m_1}{u_1} \cdot d \cdot 2^{y_d-y_1} \cdot \prod_{p \mid q} \left( 1 - \frac{(-c \mid p)}{p} \right) = \\
&= r_4[R:1] \cdot d \cdot 2^x \cdot \prod_{p \mid q} \left( 1 - \frac{(-c \mid p)}{p} \right)
\end{align*}
\]

where \( x \) is the number of odd primes in \( d \).

Theorem 22: Let \( R \) be a primitive matrix of a form which has primitive representations. If \( (d_1, d_2) = 1 \) then

\[
\frac{r_4[d_1d_2R:1]}{r_4[R:1]} = \frac{r_4[d_1R:1]}{r_4[R:1]} \cdot \frac{r_4[d_2R:1]}{r_4[R:1]}
\]

Proof: This theorem follows immediately from Theorem 21 when we observe that the \( x \) and \( q \) of 3) in Theorem 21 involves only the divisor \( d \).
CHAPTER II

Let $B$ be a $2\times 2$ matrix and $A$ be an $n\times n$ matrix. Let $T_1^{nx2}$ be a representation of $B$ by $A$, i.e. $B = T_1^{'AT_1}$. As before we will designate the g.c.d. of the second order determinants of $T_1$ by $\delta_2(T_1)$. In most cases it is easier to deduce the number of primitive representations (those in which $\delta_2(T_1) = 1$) than the number of all representations. So what is desired is a connection between the two. Hermite matrices lead us to such a connection.

Let us now recall some well known properties of Hermite matrices (c.f. [4]).

**Theorem A:** Let $T_1$ be an $n\times k$ integral matrix with $\delta_k(T_1) = u$, $1 \leq k \leq n$. Then $T_1$ can be expressed uniquely in the form $T_1 = R_1M$ when $R_1$ is integral and $n\times k$, $\delta_k(R_1) = 1$, $M$ is integral and $k\times k$, $|M| = u$ and $M$ has the form

\[
\begin{bmatrix}
  u_1 & u_{12} & \ldots & u_{1k} \\
  0 & u_2 & \ldots & u_{2k} \\
  \vdots & \vdots & \ddots & \vdots \\
  0 & \ldots & \ldots & 0 & u_k
\end{bmatrix}
\]

where $u_1 \cdot u_2 \cdot \ldots \cdot u_k = u$, $0 \leq u_{ji} < u_1$ ($i = 2, \ldots, k; j < i$).

$M$ is called a Hermite matrix by rows. If we replace $T_1$ by $R_1M$ in $T_1^{'}AT_1 = B$ we have $M'R_1^{'}ARM = B$ or
$R_1'AR_1 = M^{-1}'BM^{-1}$. On considering determinants we see that $u^2 | \text{determinant of } B$. So there are only a finite number of $M$'s which can be involved. Since $R_1'AR_1$ is integral then $M^{-1}'BM$ must also be integral. Therefore to find all the representations of $B$ by $A$ we need only count the number of primitive representations of $M^{-1}'BM^{-1}$ for each $M$ for which $M^{-1}'BM$ is integral and $|M|^2$ divides $|B|$.

This method of attacking the problem can be simplified even further to the case when $|M|$ is a power of a prime by the following well known lemma.

Lemma: i) Let $m_1, m_2$ be coprime integers. An integral matrix $Q$ of determinant $m_1 m_2$ has a unique Hermite matrix of determinant $m_2$ as right divisor.

ii) If $m_1, m_2, ..., m_s$ are coprime in pairs, a matrix $Q$ of determinant $m_1 \cdot ... \cdot m_s$ can be expressed in one and only one way in the form $VM_1M_2 \cdot ... \cdot M_s$ when $V$ is unimodular and $M_1, M_2, ..., M_s$ are Hermite matrices of determinants $m_1, m_2, ..., m_s$.

iii) If $M_1, ..., M_s$ are Hermite matrices of determinants $m_1, ..., m_s$ coprime in pairs then the matrix $Q$ of determinant $m_1 m_2 \cdot ... \cdot m_s$ having $M_i$ as its right divisor of determinant $m_i (i = 1, ..., s)$ is uniquely determined up to a left unimodular factor. Hence, if $Q$ is an Hermite matrix, it is unique.
The third part of this lemma is of particular significance to this discussion. Quite often all forms in a given genus have the same number of primitive representations. Therefore it would be to our advantage to know for how many M's such that $|M|^2$ divides $|B|$ and $M^{-1}'BM^{-1}$ is integral does $M^{-1}'BM^{-1}$ lie in a genus capable of primitive representation. We recall that two quadratic forms are in the same genus if they have the same index, determinant, and divisor, and are in the same class with respect to $p$ for every prime $p$ dividing the determinant and for $p = 2$. Also we should recall that this $p$-class is invariant under integral transformations of determinant prime to $p$. Let $M_p$ denote the Hermite right divisor of $M$ whose determinant is the largest power of $p$ dividing $|M|$. It follows that the $p$-class of $M^{-1}'BM^{-1}$ is the same as the $p$-class of $M_p^{-1}'BM_p^{-1}$. From part 3 of the lemma we see that the number of Hermite matrices $M$ of determinant $p_1 \cdots p_s$ such that $M^{-1}'BM^{-1}$ lies in a particular genus is the product of the number of Hermite matrices $M_{p_1}$ for which $M_{p_1}^{-1}BM_{p_1}$ lies in the $p_1$-class determined by that genus. Therefore it would be beneficial for us to know for a fixed $k$, how many Hermite matrices $M_p$ of determinant $p^k$ exist such that $M_p^{-1}'BM_p^{-1}$ is in a $p$-class of a particular genus, or said another way, we would like to know the number of Hermite matrices $M_p$ with
determinant $p^k$ which make $M_p^{-1} B M_p^{-1}$ have a particular power of $p$ as divisor and make the form associated with $M_p^{-1} B M_p^{-1}$ have a fixed value of the generic characters mod $p$ and mod 2.

In searching for a method of counting these $M_p$'s certain cases become immediately obvious as having to be considered separately. However careful re-evaluation of the methods of proof involved will show that certain sub-cases of the following theorems can be combined. From this author's point of view however, this may tend to obscure how the proofs were found. So each theorem is stated in laborious detail.

Since $M^{-1} B M^{-1} = M^* B M^* \frac{1}{|M|^2}$, we will concern ourselves with transformations which are Hermite by columns.

**Lemma:** Let $u = \begin{bmatrix} p^\alpha & z \\ 0 & p^\beta \end{bmatrix}$, $\alpha + \beta = k$, $0 \leq z < p^\alpha$.

Then if $f$ is equivalent to $g$, the number of forms with a given divisor and generic character obtained from $f$ by applying the transformations in $u$ is the same as the number of forms with this divisor and generic character obtained from $g$ by applying the transformations in $u$.

**pf:** Let $u = \{u_1, \ldots, u_c\}$, $F$ be the matrix of $f$, $G$ be the matrix of $g$ and $W$ an integral matrix such that
W'GW = F, |W| = 1. Consider the collections $F_i = U_i^j F U_i$ and $G_i = U_i^j G U_i$, $i = 1, \ldots, t$. We know that for each $U_i$ there exist unique $U_i$ and $V_i$ such that $U_i \in U_i$, $|V_i| = 1$ and $U_i V_i = W U_j$. So $F_j = U_j^j F U_j = U_j^j W' G W U_j = V_j^j U_j^j G U_j V_j = V_j^j G V_j V_j$. Therefore the $F_i$ are equivalent in some order to the $G_i$ and the theorem is proved.

From this lemma we see that $B$ can be canonicized mod p to a large power as in the lemma preceding Theorem 6 of Chapter I.

Let $f$ be a primitive form which can be diagonalized modulo an arbitrarily large power of 2. Let $U = \{[2^a z^i] | a + \beta = k, 0 \leq z < 2^a\}$ where $k$ is fixed. We can take $f$ to be $[a,0,c' 2^m]$ where $2^{m+2} \parallel$ discriminant of $f$, $(a,2) = (c',2) = 1$, and $(a,p) = 1$ where $p \mid$ determinant of $f$. On applying a transformation from $U$ to $f$ we get $a z^{2^a} x^2 + (az^{2^a+1})xy + (az^2 + c' 2^{2m})y^2$. Let the collection of all such form obtained from $f$ by transformations from $U$ be designated by $J_1$. In the following $z_1$ is always prime to 2 and if we write $2^x \parallel z$ and $x$ is 0 we mean $(2,z) = 1$.

Theorem 1: For $m \neq 0$ there are $2^{k-1}$ forms in $J_1$ with divisor prime to 2 which represent a mod 8 and a mod p, and $2^{k-1}$ more forms with divisor prime to 2 which represent a mod $2^m$ and a mod p.
Proof: For $a = 0$, we have $z = 0$ and the form represents $a \mod 8$ and $a \mod p$ and has no divisor with respect to 2. Now suppose $a \not= 0$. Since $m \not= 0$, the form has no divisor with respect to $Z$ if $(z, 2) = 1$. There are $2^{a-1}$ such $z$'s for each $a$ and the forms represent $a 2^{2a} \mod p$ and $a \mod 2^{2a+m}$. Therefore we have $\sum_{a=1}^{k-1} 2^{a-1} = 2^{k-1} - 1$ forms with no divisor with respect to 2 which represent a mod 8 and $2^{k-1}$ forms with no divisor which represent a mod $2^m$ when $a \not= 0$.

On summing we see that altogether we have $2^{k-1}$ forms which represent a mod 8 and $2^{k-1}$ forms which represent a mod $2^m$; all of which represent a $q^2 \mod p$, where $q$ is a power of 2.

On examining determinant $|U'FU|$ we see that the largest exponent a divisor can have is the minimum of $2k$ and $[\frac{m}{2}] + k + 1$. Also, as a matter of notation, if we say that a form represents $b \mod n$ we mean that the part of the form which is primitive with respect to 2, represents $b \mod n$.

Theorem 2: For $m/2 \geq k$ we have $2k$ as the maximum exponent of a divisor. Also in $\mathfrak{F}_1$ we have
<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. 2</th>
<th>Restrictions</th>
<th>Divisor</th>
<th>Represent w.r.t. p</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) $2^{k-1}$</td>
<td>$a \mod 8$</td>
<td>--------------</td>
<td>$2^0$</td>
<td>$a$</td>
</tr>
<tr>
<td>2) $2^{k-1}$</td>
<td>$a \mod 2^m$</td>
<td>--------------</td>
<td>$2^0$</td>
<td>$a$</td>
</tr>
<tr>
<td>3) $1$</td>
<td>$a \mod 8$</td>
<td>--------------</td>
<td>$2^{2k}$</td>
<td>$a$</td>
</tr>
<tr>
<td>4) $2^{k-1-1}$</td>
<td>$a \mod 8$</td>
<td>$0 &lt; i &lt; k$</td>
<td>$2^{2i}$</td>
<td>$a$</td>
</tr>
<tr>
<td>5) $2^{k-1-1}$</td>
<td>$a \mod 2^m$</td>
<td>$0 &lt; i &lt; k$</td>
<td>$2^{2i}$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

**Proof:** Parts 1) and 2) follow from Theorem 1. In order to have divisor $2^{2k}$, we must have $\alpha = k$ and $\beta = 0$. Then since $m \geq 2k$, we must have $2^k | z$ which implies that $z = 0$. So we have one form with this divisor and it represents a mod $p$ and a mod $8$.

In order to have divisor $2^{2i}$ for $0 < i < k$, we must have $\alpha \geq 1$. If $\alpha = i$ then $2^i$ must divide $z$ and therefore $z = 0$. This yields one form with this divisor and it represents a mod $p$ and a mod $8$. Let $\alpha = i + j$, $0 < j < k - 1$. Then from the last coefficient, $2^i | z$. From the middle coefficient we see that $2^{2i+j+1} | 2^{\alpha+1} z$. Therefore we must have $2^i || z$. Let $z = 2^i z_1$. From $z < 2^\alpha$ we see that $z_1 < 2^j$. There are $2^{j-1}$ such $z_1$'s. Therefore we have $(\sum_{l=1}^{k-i-1} 2^{j-1}) + 1 = 2^{k-i-1}$ forms with divisor $2^{2i}$ which represent a mod $8$ and mod $p$ and $2^{k-i-1}$ forms with divisor $2^{2i}$ which represent a mod $2^m$ and a mod $p$.

We will now show there are no divisors with odd
exponent. Suppose we have the divisor $2^{2n+1}$. Then we must have $2a > 2n + 1$ or $a > n + 1$. Since $m > 2k > 2a > 2n + 1$, we must have $2^{n+1}|z$. So the only chance for this divisor comes from the middle coefficient, but $2^{n+3}|2^a+^z$. So we have no odd exponent divisors. (We could also establish this fact by counting the number of forms with even exponent divisors and showing that this equals the number of forms in $\mathcal{F}_1$).

Theorem 3: For $m/2 < k$, $m$ even and $ac' \equiv 1 \mod 4$ we have in $\mathcal{F}_1$

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. 2</th>
<th>Restrictions</th>
<th>Divisor Represent w.r.t. p</th>
</tr>
</thead>
<tbody>
<tr>
<td>6) $2^{k-1}$</td>
<td>$a \mod 8$</td>
<td>$m \equiv 0$</td>
<td>$2^0$ $a$</td>
</tr>
<tr>
<td>7) $2^{k-1}$</td>
<td>$a \mod 2^m$</td>
<td>$m \equiv 0$</td>
<td>$2^0$ $a$</td>
</tr>
<tr>
<td>8) $2^{k-j}$</td>
<td>$a \mod 8$</td>
<td>$j &lt; 2^j - 1$</td>
<td>$2^2j$ $a$</td>
</tr>
<tr>
<td>9) $2^{k-m/2}$</td>
<td>$a \mod 8$</td>
<td></td>
<td>$2^{m-2}$ $a$</td>
</tr>
<tr>
<td>10) $2^{k-2}$</td>
<td>$a+4 \mod 8$</td>
<td></td>
<td>$2^{m-2}$ $a$</td>
</tr>
<tr>
<td>11) 1</td>
<td>N.G.C.</td>
<td>$k-2j - \frac{m}{2} = 1$</td>
<td>$2^{m+2j+1}$ $2a$</td>
</tr>
<tr>
<td>12) $2^{k-2j-\frac{m}{2}-2}$</td>
<td>$a+c' \mod 8$</td>
<td>$k-2j - \frac{m}{2} \geq 2$</td>
<td>$2^{m+2j+1}$ $2a$</td>
</tr>
<tr>
<td>13) $2^{k-2j-\frac{m}{2}-2}$</td>
<td>$a+9c' \mod 8$</td>
<td>$k-2j - \frac{m}{2} \geq 2$</td>
<td>$2^{m+2j+1}$ $2a$</td>
</tr>
<tr>
<td>14) 1</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j$</td>
<td>$2^{m+2j}$ $a$</td>
</tr>
<tr>
<td>15) 1</td>
<td>$(-1\mid \phi), a \mod 8$</td>
<td>$k = \frac{m}{2} + 2j+1$</td>
<td>$2^{m+2j}$ $a$</td>
</tr>
<tr>
<td>Number of forms</td>
<td>Represent w.r.t. 2</td>
<td>Restrictions</td>
<td>Divisor Represent w.r.t. p</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
<td>--------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>16) 1</td>
<td>(-1</td>
<td>ϕ),c' mod 8</td>
<td>k = \frac{m}{2} + 2j + 1</td>
</tr>
<tr>
<td>17) 2</td>
<td>a mod 8</td>
<td>k ≥ \frac{m}{2} + 2j + 2</td>
<td>2^{m+2j} a</td>
</tr>
<tr>
<td>18) 2</td>
<td>a + 4 mod 8</td>
<td>k ≥ \frac{m}{2} + 2j + 2</td>
<td>2^{m+2j} a</td>
</tr>
<tr>
<td>19) 2</td>
<td>c' mod 8</td>
<td>k ≥ \frac{m}{2} + 2j + 2</td>
<td>2^{m+2j} a</td>
</tr>
<tr>
<td>20) 2</td>
<td>c' + 4 mod 8</td>
<td>k ≥ \frac{m}{2} + 2j + 2</td>
<td>2^{m+2j} a</td>
</tr>
</tbody>
</table>

(In this table, if determinant conditions restrict the different kinds of generic characters with respect to 2 which are possible, it is noted in the representation with respect to 2 column by either listing the possible kinds of generic characters or writing N.G.C. which means no generic character).

**Proof:** To prove 8) we see that if the form has divisor \(2^{2j}\) then \(a ≥ j\). If \(a = j\) then \(2^j|z\) since \(m > 2j\). Therefore \(z = 0\) and we have one form which represents a mod 8 and mod p. Now let \(a = j + i, i = 1, ... , k - j\). Then \(2^j|z\) since \(m > 2j\) and the middle coefficient obviously is divisable by a large enough power of \(z\). So let \(z = 2^jz_1\). Then since \(2^jz_1 < 2^{j+1}\) we have \(z_1 < 2^1\). There are \(2^{i-1}\) such \(z_1\)'s and thus \(2^{i-1}z_1\)'s. So there are \(\sum_{i=1}^{k-j}2^{i-1} = 2^{k-j} - 1\) more forms with divisor \(2^{2j}\) which represent a mod 8 and mod p and 8) is proved.
In order to have divisor $2^{m-2}$ we see that $a \geq \frac{m}{2} - 1$.

If $a = \frac{m}{2} - 1$ then $z = 0$ yields one form which represents $a \mod 8$. For $a \geq \frac{m}{2} - 1$ we see as before that $2^\frac{m}{2}-1 \mid z$. The last coefficient then becomes $2^{m-2}(az_1^2 + 2^{2b+2}c')$ so if $b \geq 1$ the form represents $a \mod 8$. If $b = 0$ then $a = k$ and the form represents $az_1^2 + 4c' = a + 4 \mod 8$. Therefore we have

$$k \equiv (\frac{m}{2} - 1) \cdot 2^{i-1} = 2^{\frac{m}{2}} - 1$$

more forms which represent $a \mod 8$ and $2^{\frac{m}{2}}$ forms which represent $a + 4 \mod 8$. This proves (9) and (10).

Let us now consider the divisor $2^{m+2j+1}$. From the discriminant we know that $m + 2j + 1 \leq k + 1 + \frac{m}{2}$ or $2j \leq k - \frac{m}{2}$. Also we see from the first coefficient that $a \geq \frac{m}{2} + j + 1$ and from the last that $2^{\frac{m}{2} + j} \mid z$. Suppose $2^{\frac{m}{2} + j + 1} \mid z$ then $2^{m+2j+3} \mid 2^{a+1}z$. We then have either an even power or else too large a power dividing the last coefficient. So for this divisor $2^{\frac{m}{2}+j+1} \mid z$. Therefore let $z = 2^{\frac{m}{2}+j}z_1$. Then $az_1^2 + c'2^{2b+m} = a2^{m+2j}z_1^2 + c'2^{2b+m}$. Since $2^{m+2j+2} \mid az_1^{a+1}$, the last coefficient will determine the divisor. So we must have $b = j$ and $a = k - j$. These conditions are consistent with the range of $j$ and $2^{\frac{m}{2} + j} \mid z$. Then $az_1^2 + c'2^{2b+m} = 2^{m+2j}(az_1^2 + c')$. Also $az_1^2 + c' \equiv 2 \mod 4$. Since $2^{\frac{m}{2} + j}z_1 \leq 2^{k-j}$ we see that $z_1 \leq 2^{k-2j-\frac{m}{2}}$. Parts
11), 12) and 13) then follow immediately when we observe from the conditions on \( k, \alpha \) and \( j \) that \( k \geq \frac{m}{2} + 2j + 1 \).

We will now consider the number of forms with divisor \( 2^{m+2j} \). We immediately see that for these forms \( k \geq \frac{m}{2} + j \) and \( \alpha \geq \frac{m}{2} + j \). Let \( \alpha = \frac{m}{2} + j \). Then \( \beta = k - (\frac{m}{2} + j) \). The last coefficient implies that \( 2\beta + m \geq 2j + m \). So \( \beta \geq j \).

Therefore \( k - (\frac{m}{2} + j) \geq j \) or \( k - \frac{m}{2} \geq 2j \). So we get one form with \( z = 0 \) which represents a mod 8 and mod p. Now let \( \alpha = \frac{m}{2} + j + 1; i = 1, \ldots, k - (\frac{m}{2} + j) \). If \( \beta > j \) we then have \( k - (\frac{m}{2} + j + 1) > j \) or said another way \( k - (\frac{m}{2} + 2j + 1) \geq 1 \). So we must have \( k - (\frac{m}{2} + 2j + 2) \geq 0 \) in this case for \( \beta > j \).

Therefore let \( \alpha = \frac{m}{2} + j + 1; i = 1, \ldots, k - (\frac{m}{2} + 2j + 1) \). From the last coefficient we must have \( 2^m \parallel z \). Therefore \( 2^m \mid z < 2^{m} + j + 1 \) or \( z_1 < 2^1 \). We have \( 2^{1-1} \) forms for each \( i \). So we have \( \sum_{i=1}^{k-1} 2^{i-1} = 2^1 - 1 \) more forms of which \( 2^{1-1} - 1 \) represent \( \alpha \) and \( k - (\frac{m}{2} + 2j + 2) \) represent \( \alpha + 4 \) mod 8. Now for \( \beta = j \). Then \( \alpha = k - j = \frac{m}{2} + j + 1 \) or put another way \( k - (\frac{m}{2} + 2j) = 1 \). So \( k \geq \frac{m}{2} + 2j + 1 \). If \( k = \frac{m}{2} + 2j + 1 \) we get one form which represents \( c' \) mod 8. If \( k \geq \frac{m}{2} + 2j + 2 \) then \( \frac{m}{2} + 2j + 1 \) \( 2^2 \mid z \). Thus \( 2^2 \mid z \) or \( z_2 < 2^k - j \) or \( z_2 < 2^{k - (\frac{m}{2} + 2j + 1)} \).
Therefore we have $2^{k-(S+2j+2)}$ forms which represent $c' \mod 8$
and $2^{k-(S+2j+2)}$ which represent $4+c' \mod 8$. This finishes the proof.

**Theorem 4:** For $\frac{m}{2} < k$ and $m$ odd, the maximum exponent of a divisor is $\frac{m-1}{2} + k + 1$ and we have in $\mathfrak{F}_1$

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t.2</th>
<th>Restrictions</th>
<th>Divisor Represent w.r.t. p</th>
</tr>
</thead>
<tbody>
<tr>
<td>21) $2^{k-1}$</td>
<td>$a \mod 8$</td>
<td>___________</td>
<td>$2^0$ a</td>
</tr>
<tr>
<td>22) $2^{k-1}$</td>
<td>$a \mod 2^m$</td>
<td>___________</td>
<td>$2^0$ a</td>
</tr>
<tr>
<td>23) $2^{k-j}$</td>
<td>$a \mod 8$</td>
<td>$0 &lt; 2j &lt; m - 3$</td>
<td>$2^{2j}$ a</td>
</tr>
<tr>
<td>24) 1</td>
<td>N.G.C.</td>
<td>$k-(\frac{m-1}{2}) = 2j$</td>
<td>$2^{m-1+2j}$ a</td>
</tr>
<tr>
<td>25) $2^{k-(\frac{m-1}{2}+2j+1)}$</td>
<td>$a \mod 8$</td>
<td>$k-(\frac{m-1}{2}) &gt; 2j$</td>
<td>$2^{m-1+2j}$ a</td>
</tr>
<tr>
<td>26) $2^{k-(\frac{m-1}{2}+2j+1)}$</td>
<td>$a+2c' \mod 8$</td>
<td>$k-(\frac{m-1}{2}) &gt; 2j$</td>
<td>$2^{m-1+2j}$ a</td>
</tr>
<tr>
<td>27) 1</td>
<td>N.G.C.</td>
<td>$k = \frac{m+1}{2} + 2j$</td>
<td>$2^{m+2j}$ 2a</td>
</tr>
<tr>
<td>28) $2^{k-(2j+1+\frac{m+1}{2})}$</td>
<td>$2a+c' \mod 8$</td>
<td>$k\geq\frac{m+1}{2} + 2j + 1$</td>
<td>$2^{m+2j}$ 2a</td>
</tr>
<tr>
<td>29) $2^{k-(2j+1+\frac{m+1}{2})}$</td>
<td>$c' \mod 8$</td>
<td>$k\geq\frac{m+1}{2} + 2j + 1$</td>
<td>$2^{m+2j}$ 2a</td>
</tr>
</tbody>
</table>

**Proof:** Parts 21) and 22) follow from Theorem 1. Part 23) is identical in proof to 8) of Theorem 3.

**Divisor $2^{m-1+2j}$.** Since $2\mathfrak{F} + m$ is odd and the exponent of 2 in the divisor and $az^2$ is even we must have
$2\beta + m > m + 1 + 2j$ which implies $\beta \geq j$. Since $k = \alpha + \beta$, we have $k \geq \alpha + j$. For this divisor we also must have $\alpha \geq \frac{m-1}{2} + j$ so we have $k \geq \frac{m-1}{2} + 2j$.

For $\alpha = \frac{m-1}{2} + j$ we have only one form with this divisor and that occurs with $z = 0$. This form represents a mod 8 and a mod p.

Now consider $\alpha = \frac{m-1}{2} + j + 1$. From $k \geq j + \alpha$ we have $k \geq \frac{m-1}{2} + 2j + 1$. So we are concerned with $i = 1, \ldots, k - (\frac{m-1}{2} + 2j)$. This also implies $k - (\frac{m-1}{2} + 1) \geq 2j$.

Since $2^{m+1} + j$ must exactly divide $z$ for this divisor, we have $2^{i-1}$ forms for each $i$. Therefore we have $k - (\frac{m-1}{2} + 2j + 1) - 1$ more forms with $a \text{ mod } 8$ and a mod p and $2^{i-1}$ forms which represent $a + 2c'$ mod 8 and a mod P.

Combining these results yields (24), (25) and (26).

**Divisor $2^{m+2j}$.** From determinant conditions we see that $m + 2j \leq \frac{m-1}{2} + k + 1$ which implies $2j \leq k + 1 - (\frac{m+1}{2})$. For this divisor we also know that $\alpha \geq \frac{m+1}{2} + j$ and $2^{\frac{m+1}{2} + j} \mid z$.

So we must have $m + 2j = m + 2\beta$, i.e. $\beta = j$. Then $\alpha = k - j \geq \frac{m+1}{2} + j$ which implies $k - \frac{m+1}{2} \geq 2j$ or we have no forms with this divisor.

Let $k - \frac{m+1}{2} = 2j$. Necessarily then $2^{\frac{m+1}{2} + j} \mid z$. Since
\( \alpha = \frac{m+1}{2} + j \), we must have \( z = 0 \). This form represents \( c' \mod 8 \) and \( 2a \mod p \).

Now consider \( k - \frac{m+1}{2} \geq 2j + 1 \). Then \( \alpha = k - j \geq \frac{m+1}{2} + 1 \).

For \( 2^j \parallel z \) we get \( 2^{k-2j-1-\frac{m+1}{2}} \) forms which represent \( 2a + c' \mod 8 \) and \( 2a \mod p \). For \( 2^{\frac{m+1}{2}} + j + 1 \parallel z \) we get \( 2^{k-2j-1-\frac{m+1}{2}} \) forms which represent \( c' \mod 8 \) and \( a \mod p \).

Totaling our results finishes the theorem.

**Theorem 5:** For \( \frac{m}{2} < k \), \( m \) even and \( ac' \equiv 3 \mod 8 \), the maximum exponent for a divisor is \( k + \frac{m}{2} + 1 \) and we have in \( \mathfrak{J}_1 \)

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent ( \text{w.r.t.} 2 )</th>
<th>Restrictions</th>
<th>Divisor Represent ( \text{w.r.t.} p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>30) ( 2^{k-1} )</td>
<td>( a \mod 8 )</td>
<td>( m \neq 0 )</td>
<td>( 2^0 )</td>
</tr>
</tbody>
</table>
| 31) \( 2^{k-1} \) | \( a \mod 2^m \) | \( m 
eq 0 \) | \( 2^0 \) | \( a \) |
<p>| 32) ( 2^{k-j} ) | ( a \mod 8 ) | ( 2j &lt; m - 2 ) | ( 2^{2j} ) | ( a ) |
| 33) ( 2^{k-\frac{m}{2}} ) | ( a \mod 8 ) | ( \ldots ) | ( 2^{m-2} ) | ( a ) |
| 34) ( 2^{k-\frac{m}{2}} ) | ( a + 4 \mod 8 ) | ( \ldots ) | ( 2^{m-2} ) | ( a ) |
| 35) ( 1 ) | ( (-1 \parallel \varphi) ), ( a \mod 8 ) | ( k = \frac{m}{2} + 1 ) | ( 2^m ) | ( a ) |
| 36) ( 1 ) | ( (-1 \parallel \varphi) ), ( c' \mod 8 ) | ( k = \frac{m}{2} + 1 ) | ( 2^m ) | ( a ) |
| 37) ( 2 ) | ( 1 \mod 8 ) | ( k \geq \frac{m}{2} + 2 ) | ( 2^m ) | ( a ) |
| 38) ( 2 ) | ( k = \frac{m}{2} + 2 ) | ( 3 \mod 8 ) | ( k \geq \frac{m}{2} + 2 ) | ( 2^m ) | ( a ) |
| 39) ( 2 ) | ( k = \frac{m}{2} + 2 ) | ( 5 \mod 8 ) | ( k \geq \frac{m}{2} + 2 ) | ( 2^m ) | ( a ) |</p>
<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. 2</th>
<th>Restrictions</th>
<th>Divisor w.r.t.p</th>
</tr>
</thead>
<tbody>
<tr>
<td>40) $2^{k-(\frac{m}{2}+1)}$</td>
<td>5 mod 8</td>
<td>$k \geq \frac{m}{2} + 2$</td>
<td>$2^m$</td>
</tr>
<tr>
<td>41) 1</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j - 1, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>42) 3</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>43) 1</td>
<td>$(-1</td>
<td>\psi), 1 \mod 8$</td>
<td>$k = \frac{m}{2} + 2j + 1, j \geq 1$</td>
</tr>
<tr>
<td>44) 1</td>
<td>$(-1</td>
<td>\psi), 3 \mod 8$</td>
<td>$k = \frac{m}{2} + 2j + 1, j \geq 1$</td>
</tr>
<tr>
<td>45) 1</td>
<td>$(-1</td>
<td>\psi), 5 \mod 8$</td>
<td>$k = \frac{m}{2} + 2j + 1, j \geq 1$</td>
</tr>
<tr>
<td>46) 1</td>
<td>$(-1</td>
<td>\psi), 7 \mod 8$</td>
<td>$k = \frac{m}{2} + 2j + 1, j \geq 1$</td>
</tr>
<tr>
<td>47) $3 \cdot 2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>1 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j + 2, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>48) $3 \cdot 2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>3 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j + 2, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>49) $3 \cdot 2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>5 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j + 2, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>50) $3 \cdot 2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>7 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j + 2, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
</tbody>
</table>

**Proof:** It should be first noted that

\[ az_1^2 + c' = a + c' = a^2(a+c') = a(a^2+ac') = 4a = 4 \mod 8. \]

Also parts 30) and 31) follow directly from Theorem 1 and 32) is identical in proof to 8) of Theorem 3.

**Divisor $2^{m-2}$:** For this divisor $a \geq \frac{m}{2} - 1$. So let us first consider $a = \frac{m}{2} - 1$. Then $\beta = k - \frac{m}{2} + 1$. Therefore $z = 0$ gives one form which represents a mod 8 and mod p.

Now consider $a = \frac{m}{2} - 1 + i, i = 1, \ldots, k-(\frac{m}{2} - 1)$.

Then we must have $2^{i-1} || z$. So we get $2^{i-1}$ forms for each $k-(\frac{m}{2} - 1)-1 \leq k-\frac{m}{2}$

1. Therefore we have $\sum_{i=1}^{\frac{m}{2} - 1} 2^{i-1} = 2^{\frac{m}{2}} - 1$ more forms
which represent a mod 8 and \(2^{k-m/2}\) forms which represent \(a+4\) mod 8. All of these represent a mod p. So taking these results yields 32) and 33).

**Divisor \(2^m\).** For this divisor we must have \(a \geq m/2\). For \(a = m/2, z = 0\) gives one form which represents a mod 8 and a mod p.

Now consider \(a = m/2 + i, i = 1, \ldots, k - m/2 - 1\). Then \(k - m/2 - 1 \geq 1\) which implies \(k \geq m/2 + 2\) or else these conditions are vacuous. Since \(\beta \geq 1\) we must have \(2^{m/2} || z\). This yields \(2^{i-1}\) forms for each \(i\). So we have \(2^{k-(m/2+2)} \Sigma_{i=1}^{k-(m/2+2)} 2^{i-1} = 2^k - 1\) forms which represent a mod 8 and a mod p and \(2^{k-(m/2+2)}\) forms which represent \(a+4\) mod 8.

Now for \(a = k, \beta = 0\). Then \(2^{m/2+1} || z\). If \(2^{m/2+1} || z\) we have \(2^{k-(m/2+2)}\) forms which represent \(4 + c'\) mod 8 if \(k \geq m/2 + 2\). If \(k \geq m/2 + 2\) and \(2^{m/2+2} || z\) we get \(2^{k-(m/2+2)}\) forms which represent \(c'\) mod 8 and a mod p. If \(k = m/2 + 1\) we get one form which represents \(c'\) mod 8 and has \((-1|\phi)\) as generic character.

Totaling these results and realizing that since \(a, c' \equiv 3\) mod 8, all of \(a, a+4, c',\) and \(c'+4\) are incongruent mod 8 yields 35) - 40).
Divisor $2^{m+2j}$. For this divisor we must have $a \geq \frac{m}{2} + j$ and $\beta \geq j - 1$. So $k = a + \beta \geq \frac{m}{2} + 2j - 1$ or else we have no new forms in this case. From the maximum exponent condition we know $1 \leq j \leq \frac{k+1-2m}{2}$ which is the same as the first condition.

Consider $a = \frac{m}{2} + j$. If $k = \frac{m}{2} + j - 1$ then $\beta = j - 1$. Then if $2^{m+2j-1} \parallel z$ we get one form which represents $a$ mod 8 and mod $p$. But this form has discriminant $-ac' \equiv -3$ mod 8 so it has no generic character with respect to 2. If $k = \frac{m}{2} + 2j$ then $\beta = j$ and $z = 0$ yields one form which represents $a$ mod 8. However the discriminant of this form $\equiv -4ac' \equiv 4$ mod 16 so it has no generic character with respect to 2. If $k = \frac{m}{2} + 2j + 1$ then $\beta = j + 1$ and $z = 0$ yields one form which represents $a$ mod 8. The discriminant of this form $\equiv -16ac' \equiv 32$ mod 32 so we have only $(-1 | a')$. If $k \geq \frac{m}{2} + 2j + 2$ then we have all three characters with respect to 2 and one form with $z = 0$ which represents $a$ mod 8 and mod $p$.

Now consider $a = \frac{m}{2} + j + 1$, $i = 1, \ldots, k - (\frac{m}{2} + j)$. Here $k \geq \frac{m}{2} + j + 1$ or we have no forms in this case. However, since we must also have $\beta \geq j - 1$, we must have $k \geq \frac{m}{2} + 2j$. We will now further sub-divide this case depending on $\beta$.

Let $\beta = j - 1$. Then $i = k - (\frac{m}{2} + 2j - 1)$. Also we
must have $2^{\frac{m}{2}+j-1}$ \parallel z. Then we have $2^{k-(\frac{m}{2}+2j-1)}$ forms. If $k = \frac{m}{2} + 2j$ this gives 2 forms whose discriminant $\equiv 4 \mod 16$. So they have no generic character with respect to 2. If $k = \frac{m}{2} + 2j + 1$ then the discriminant $\equiv -16 \mod 32$. So we have 4 forms representing each of $\frac{a+c'}{4}, \frac{9a+c'}{4}, \frac{25a+c'}{4}$ and $\frac{49a+c'}{4}$. All of these are incongruent mod 8. If $k \geq \frac{m}{2} + 2j + 2$ then we have all 3 characters and each odd residue mod 8 is represented 2 times.

Let $\beta = j$. Then $\alpha = k - j$ and $k \geq \frac{m}{2} + 2j + 1$. Also we must have $2^{\frac{m}{2}+j+1} \parallel z$. If $k = \frac{m}{2} + j + 1$ then $z = 0$ yields one form which represents $c'$ mod 8. The discriminant of this form $\equiv 16 \mod 32$ so we have only $(-1|\phi)$. If $k \geq \frac{m}{2} + 2j + 2$ then we have all three characters. For $2^{\frac{m}{2}+j+2} \parallel z$ we get $2^{k-(\frac{m}{2}+2j+2)}$ forms which represent $c'$ mod 8. For $2^{\frac{m}{2}+j+1} \parallel z$ we get $2^{k-(\frac{m}{2}+2j+2)}$ forms which represent $4 + c'$ mod 8.

Now let $\alpha = \frac{m}{2} + j + 1$, $i = 1, \ldots, k-(\frac{m}{2}+2j+1)$. We must have $k \geq \frac{m}{2} + 2j + 2$. For $2^{\frac{m}{2}+j} \parallel z$ we have $2^{i-1}$ forms for each $i$. So we have $\sum_{i=1}^{k-(\frac{m}{2}+2j+2)} 2^{i-1} = 2^{k-(\frac{m}{2}+2j+2)} - 1$. 
forms which represent a mod 8 and 2 \( k-(\frac{m}{2}+2j+2) \) forms which represent a +4 mod 8.

Totaling these results yields 41)-50).

**Divisor** \( 2^{2x+1} \). For this divisor \( a \geq x+1 \). Also since
\[ ax_1^2 + c' = 4 \mod 8, \] 2\(^x\)|z. So \( 2^{2x+2}|z \cdot z^{a+1} \). Therefore the last coefficient would determine the divisor. However the last coefficient is always divisible by an even power of 2. So there are no forms with this divisor.

**Theorem 6**: For \( \frac{m}{2} < k, m \) even, and \( ac' = 3 \mod 8 \), the maximum exponent for a divisor is \( k+\frac{m}{2} + 1 \) and we have in \( \mathbb{Z}_1 \)

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. 2</th>
<th>Restrictions</th>
<th>Divisor Represent w.r.t. p</th>
</tr>
</thead>
<tbody>
<tr>
<td>51) ( 2^{k-1} )</td>
<td>a mod 8</td>
<td>m ≠ 0</td>
<td>( 2^0 ) a</td>
</tr>
<tr>
<td>52) ( 2^{k-1} )</td>
<td>a mod ( 2^m )</td>
<td>m ≠ 0</td>
<td>( 2^0 ) a</td>
</tr>
<tr>
<td>53) ( 2^{k-j} )</td>
<td>a mod 8</td>
<td>2j &lt; m-2</td>
<td>( 2^{2j} ) a</td>
</tr>
<tr>
<td>54) ( 2^{k-m} )</td>
<td>a mod 8</td>
<td></td>
<td>( 2^{m-2} ) a</td>
</tr>
<tr>
<td>55) ( 2^\frac{m}{2} )</td>
<td>a+4 mod 8</td>
<td></td>
<td>( 2^{m-2} ) a</td>
</tr>
<tr>
<td>56) 1</td>
<td>((-1</td>
<td>k), a mod 8 )</td>
<td>( k = \frac{m}{2}+1 )</td>
</tr>
<tr>
<td>57) 1</td>
<td>((-1</td>
<td>\varphi), c' \mod 8 )</td>
<td>( k = \frac{m}{2} + 1 )</td>
</tr>
<tr>
<td>58) ( 2^{k-(\frac{m}{2}+2)} )</td>
<td>l mod 8</td>
<td>( k \geq \frac{m}{2} + 2 )</td>
<td>( 2^m ) a</td>
</tr>
<tr>
<td>Number of forms</td>
<td>Represent w.r.t. 2</td>
<td>Restrictions</td>
<td>Divisor</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>59) $2^{k-(\frac{m}{2}+2)}$</td>
<td>$3 \text{ mod } 8$</td>
<td>$k \geq \frac{m}{2} + 2$</td>
<td>$2^m$</td>
</tr>
<tr>
<td>60) $2^{k-(\frac{m}{2}+2)}$</td>
<td>$5 \text{ mod } 8$</td>
<td>$k \geq \frac{m}{2} + 2$</td>
<td>$2^m$</td>
</tr>
<tr>
<td>61) $2^{k-(\frac{m}{2}+2)}$</td>
<td>$7 \text{ mod } 8$</td>
<td>$k \geq \frac{m}{2} + 2$</td>
<td>$2^m$</td>
</tr>
<tr>
<td>62) $2^j$</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>63) $2^j$</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j+1, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>64) $j$</td>
<td>(-1,0), 3 mod 8</td>
<td>$k = \frac{m}{2} + 2j+2, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>65) $j$</td>
<td>(-1,0), 1 mod 8</td>
<td>$k = \frac{m}{2} + 2j+2, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>66) $j$</td>
<td>(-1,0), 5 mod 8</td>
<td>$k = \frac{m}{2} + 2j+2, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>67) $j$</td>
<td>(-1,0), 7 mod 8</td>
<td>$k = \frac{m}{2} + 2j+2, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>68j, $2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>1 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j+3, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>69j, $2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>3 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j+3, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>70j, $2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>5 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j+3, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>71j, $2^{k-(\frac{m}{2}+2j+2)}$</td>
<td>7 mod 8</td>
<td>$k \geq \frac{m}{2} + 2j+3, j \geq 1$</td>
<td>$2^{m+2j+1}$</td>
</tr>
<tr>
<td>72) $2^j-1$</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j-1, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>73) $2^j-1$</td>
<td>N.G.C.</td>
<td>$k = \frac{m}{2} + 2j, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>74) 1</td>
<td>(-1,0), a mod 8</td>
<td>$k = \frac{m}{2} + 2j+1, j \geq 1$</td>
<td>$2^{m+2j}$</td>
</tr>
<tr>
<td>Number of forms</td>
<td>Represent w.r.t. 2</td>
<td>Restrictions</td>
<td>Divisor Represent w.r.t. p</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>--------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>75) 1</td>
<td>((-1</td>
<td>\phi), c' \mod 8)</td>
<td>(k = \frac{m}{2} + 2j + 1, j \geq 1)</td>
</tr>
<tr>
<td>76) j-1</td>
<td>((-1</td>
<td>\phi), l \mod 8)</td>
<td>(k = \frac{m}{2} + 2j + 1, j \geq 1)</td>
</tr>
<tr>
<td>77) j-1</td>
<td>((-1</td>
<td>\phi), 3 \mod 8)</td>
<td>(k = \frac{m}{2} + 2j + 1, j \geq 1)</td>
</tr>
<tr>
<td>78) j-1</td>
<td>((-1</td>
<td>\phi), 5 \mod 8)</td>
<td>(k = \frac{m}{2} + 2j + 1, j \geq 1)</td>
</tr>
<tr>
<td>79) j-1</td>
<td>((-1</td>
<td>\phi), 7 \mod 8)</td>
<td>(k = \frac{m}{2} + 2j + 1, j \geq 1)</td>
</tr>
<tr>
<td>80) ((2j-1)2^{k-(\frac{m}{2}+2j+2)})</td>
<td>1 \mod 8</td>
<td>(k \geq \frac{m}{2} + 2j + 2, j \geq 1)</td>
<td>(2^{m+2j} a)</td>
</tr>
<tr>
<td>81) ((2j-1)2^{k-(\frac{m}{2}+2j+2)})</td>
<td>3 \mod 8</td>
<td>(k \geq \frac{m}{2} + 2j + 2, j \geq 1)</td>
<td>(2^{m+2j} a)</td>
</tr>
<tr>
<td>82) ((2j-1)2^{k-(\frac{m}{2}+2j+2)})</td>
<td>5 \mod 8</td>
<td>(k \geq \frac{m}{2} + 2j + 2, j \geq 1)</td>
<td>(2^{m+2j} a)</td>
</tr>
<tr>
<td>83) ((2j-1)2^{k-(\frac{m}{2}+2j+2)})</td>
<td>7 \mod 8</td>
<td>(k \geq \frac{m}{2} + 2j + 2, j \geq 1)</td>
<td>(2^{m+2j} a)</td>
</tr>
</tbody>
</table>

Proof: It should be first observed that for \(n \geq 3\) there exist \(z_1\)'s such that \(az_1^2 + c' = 0 \mod 2^n\).

Parts 51) and 52) follow from Theorem 1. Part 53) is identical in proof to 8) of Theorem 3. Parts 54) and 55) are the same as 33) and 34) of Theorem 5. Parts 56)-61) are identical to 35) -39) of Theorem 5.

Let us now consider the exponent of the divisor to be \(2x + 1\). Then \(a \geq x + 1\). If \(2x + 1 < m\) then from the last coefficient \(2^{x+1}|z\). So \(2^{2x+3}|az^2 + 1\) and we have no odd
exponent divisor in this case. If $2x + 1 = m$ then, since $a^2 + c \equiv 0 \mod 8$ we must have either $2^m | z$ or $2^{m+1} | z$, both of which give larger exponents than desired in the last coefficient. Then from the middle coefficient $2^{m+2} | 2^{a+1} z$. So this exponent does not occur. Therefore an odd exponent for a divisor must be greater than or equal to $m + 3$.

**Divisor $2^{m+2j+1}, j \geq 1$.** For this divisor $a \geq \frac{m}{2} + j + 1$.

Also we have $k \geq \frac{m}{2} + 2j$ from the maximum exponent condition.

Now let us find the range of $\beta$. Let $z = 2^nz_1$. If the divisor is determined by the middle coefficient then $m + 2j + 1 = \alpha + n + 1$ which implies $\alpha + n = m + 2j$. Also we must have $m + 2j + 1 \leq m + 2\beta$ and $m + 2j + 1 \leq 2n$ or else $m + 2\beta = 2n < m + 2j + 1$. The first condition does not occur since it would imply $m + 2j + 1 = \alpha + 1 + n \geq \alpha + 1 + \frac{m}{2} + j + 1 \geq \frac{m}{2} + j + 1 + 1 + \frac{m}{2} + j + 1 = m + 2j + 3$. Let us now consider $m + 2\beta = 2n < m + 2j + 1$. Since $\alpha + n = m + 2j$ we have $k = \frac{m}{2} + 2j$. Also $\beta = k - \alpha = \frac{m}{2} + 2j - \alpha \leq \frac{m}{2} + 2j - \left(\frac{m}{2} + j + 1\right) = j - 1$. So if the middle coefficient determines the divisor we have $k = \frac{m}{2} + 2j$ and $\beta \leq j - 1$.

If the last coefficient determines the divisor then $2\beta + m \leq 2j + 1 + m - 3$ which implies $\beta \leq j - 1$.

Now consider $0 \leq \beta \leq j - 1$. If $2^{\beta} || z$ and $k \geq \frac{m}{2} + 2j$
then \( \alpha \geq \frac{m}{2} + j + 1 \). Now further restrict this case by taking \( k = \frac{m}{2} + 2j \). Then we see that \( 2^{m+2j+1} || z \) \( 2^{\alpha+1} \).

So we must count the \( z_1 \)'s such that \( az_1^2 + c' \equiv 0 \mod 2^{2j+1-2^\beta} \) with \( 0 < z_1 < 2^{2j-2^\beta} \). There are two solutions for each \( \beta \) so there are \( 2j \) solutions altogether.

For \( k = \frac{m}{2} + 2j + 1 \) we have \( \alpha = \frac{m}{2} + 2j + 1 - \beta \).

Also we must have \( 2^{2^\beta} || z \) and \( az_1^2 + c' \equiv 2^{2j+1-2^\beta} \mod 2^{2j+2-2^\beta} \) \( 0 < z_1 < 2^{2j+1-2^\beta} \). Again we have two solutions for each \( \beta \) so we have \( 2j \) forms.

For \( k = \frac{m}{2} + j + 2 \), we have \( \alpha = \frac{m}{2} + 2j + 2 - \beta \). We must have \( 2^{2^\beta} || z \) and \( az_1^2 + c' \equiv 2^{2j+1-2^\beta} \mod 2^{2j+2-2^\beta} \) with \( 0 < z_1 < 2^{2j+2-2^\beta} \). So we have \( j \) forms representing \( 1, j \) representing \( 3, j \) representing \( 5 \) and \( j \) representing \( 7 \) \( m \).

Now take \( k \geq \frac{m}{2} + 2j + 3 \). We must have \( 2^{2^\beta} || z \) and \( az_1^2 + c' \equiv 2^{2j+1-2^\beta} \mod 2^{2j+2-2^\beta} \) with \( 0 < z_1 < 2^{k-\frac{m}{2}-2^\beta} \). So we get four sets of forms, each set containing \( j(2^{k-(\frac{m}{2}+2j+2)}) \) forms and each set representing a different odd residue mod 8.

Totaling these results yields \( 62j - 71j \).
Divisor $2^{m+2j}, j \geq 1$. For this divisor we must have $a \geq \frac{m}{2} + j$. Also the maximum exponent condition implies that $k \geq \frac{m}{2} + 2j - 1$. Let $a = \frac{m}{2} + j$. Then $\beta \geq j - 1$.

If $k = \frac{m}{2} + 2j - 1$ then $\beta = j - 1$ and we must have $2^{\frac{m}{2}+j-1} \parallel z$. So we get one form. If $k \geq \frac{m}{2} + 2j$ then only by taking $z = 0$ do we get a form and this form represents $a \mod 8$ and $a \mod p$.

Now consider $a = k - j, \beta = j$ and $k > \frac{m}{2} + 2j$. If $k = \frac{m}{2} + 2j + 1$ then $a = \frac{m}{2} + j + 1$. From the last coefficient we see that we must have $2^{\frac{m}{2}+j+1} \parallel z$. Therefore $z = 0$ gives one form which represents $c' \mod 8$. If $k = \frac{m}{2} + 2j + 2$ then $a = \frac{m}{2} + j + 2$ and we must have $2^{\frac{m}{2}+j+2} \parallel z$. Thus we get two forms. One represents $c'$ and the other $4 + c' \mod 8$. If $k \geq \frac{m}{2} + 2j + 3$ then again $2^{\frac{m}{2}+j+1} \parallel z$. If $2^{\frac{m}{2}+j+1} \parallel z$, we have $2^{k-j-(\frac{m}{2}+j+1)-1} = 2^{k-(\frac{m}{2}+2j+2)}$ forms which represent $4 + c' \mod 8$. If $2^{\frac{m}{2}+j+2} \parallel z$ we have $2^{k-(\frac{m}{2}+2j+2)}$ forms which represent $c' \mod 8$.

Now let $a = \frac{m}{2} + j + 1, i = 1, \ldots, k - (\frac{m}{2} + 2j + 1)$. Observe that $k \geq \frac{m}{2} + 2j + 2$ or else there are no forms in
this case. We obviously need $2^{\frac{m+j}{2}} \| z$. So we get

\[2^{i-1} \text{ forms for each } i \text{ and therefore have } \sum_{i=1}^{k-(\frac{m+2j+2}{2})} 2^{j-1} = \sum_{i=1}^{2^{(\frac{m+2j+2}{2})-1}} \text{ forms representing } a \mod 8 \text{ and } 2^{k-(\frac{m+2j+2}{2})} \text{ forms representing } a + 4 \mod 8.

For $\alpha = k - j + 1$ we have $\beta = j - 1$. The only case with these restrictions which has not already been eliminated is $k \geq \frac{m}{2} + 2j$. Then $\alpha \geq \frac{m}{2} + j + 1$. Since we must have $2^{\frac{m+j-1}{2}} \| z$, all coefficients have too large a power of 2 as divisor. So we get no new forms from this case.

For $\alpha = k - j + 1$, $i = 2, \ldots, j$ we have $\beta = j - 1$ and $\beta$ ranges from 0 to $j - 2$. If $k = \frac{m}{2} + 2j - 1$ then $\alpha = \frac{m}{2} + j - l + 1$ and we need $2^{\frac{m+j-1}{2}} \| z$ and $az_1 + c' \equiv 0 \mod 2^{2i}$ with $0 < z_1 < 2^{2i-1}$ since the middle coefficient determines the divisor here. We have 2 such $z$'s for each $i$ and therefore have $2(j - l)$ forms.

If $k = \frac{m}{2} + 2j$ then $\alpha = \frac{m}{2} + j + 1$. We want $2^{\frac{m+j-1}{2}} \| z$ and $az_1 + c' \equiv 2^{2i} \mod 2^{2i+1}$ with $0 < z_1 < 2^{2i}$. We have two solutions for each $i$ and therefore have $2(j - 1)$ forms.

If $k \geq \frac{m}{2} + 2j + 1$ then $\alpha \geq \frac{m}{2} + j + 1 + l$ and again we want $2^{\frac{m+j-1}{2}} \| z$ and $az_1 + c' \equiv 2^{2i} \mod 2^{2i+1}$ with $0 < z_1 < 2^{(k+2i-(\frac{m+2j}{2}))-(2i+1)}$. This yields $2^{2i-(2i-(\frac{m+2j}{2})-(2i+1))}=$
\[2^{k-(\frac{m}{2}+2j+1)}(j-1)^2 \] forms for each \(i\). Obviously all odd residues mod 8 are equally represented. So we have
\[k-(\frac{m}{2}+2j+1)\] forms representing 1 mod 8 and the same number representing each of 3, 5 and 7 mod 8.

Totaling these results finishes the theorem.

Now we will consider a form \(f\) which is not diagonalizable modulo a high power of 2 but is primitive. This form is equivalent to a form of the type \([a, a, c]\) modulo a high power of 2. Let \(\gamma = \left\{ \{\begin{array}{ll} 2^\alpha & z \\ 0 & 2^\beta \end{array}\right\} \left| k = \alpha + \beta \right. \) and \(0 \leq z < 2^a\}. \) Let \(\gamma^*\) consist of the elements of \(\gamma\) for which \(\beta \neq 0\). Let \(\gamma' = \left\{ \{\begin{array}{ll} 2^\alpha & z \\ 0 & 2^\beta \end{array}\right\} \left| a + \beta = k - 1 \right. \) and \(0 \leq z < 2^a\).\)

Let \(\nu = \left\{ \{\begin{array}{ll} 2^\alpha & z \\ 0 & 1 \end{array}\right\} \left| 0 \leq z < 2^k \right. \). For \(U \in \gamma^*\) we see that \(U = \left\{ \begin{array}{ll} 2^\alpha & z \\ 0 & 2^\beta \end{array}\right\} \) with \(\beta \neq 0\). So if \(V = \left[ \begin{array}{ll} 1 & 0 \\ 0 & 2 \end{array}\right] \) we have that \(U = V \left\{ \begin{array}{ll} 2^\alpha & z \\ 0 & 2^\beta-1 \end{array}\right\} \). If \(g\) is the form obtained by applying \(V\) to \(f\) then \(g\) is of the type \([a, 2a, 4c]\) and \(g\) is obviously equivalent to a diagonalized form \(g'\). Therefore if we consider what happens to \(g'\) and thus to \(g\) under the transformations from \(\gamma'\) and add to this what happens to \(f\) under the transformations from \(\gamma\) then we know the number of forms, obtained by applying the transformations from \(\gamma\) to \(f\), with any given divisor and what they
represent mod 8 and mod p. Therefore we need to consider $f = [a, a, 2^mc']$ under applications from $\mathcal{H}$. On applying one of these transformations we obtain $[a2^{2k}, a2^k(2z+1), az(z+1) + c'2^m]$. Also since for $m \neq 0$, $[a, a, 2^mc']$ is equivalent to $[a_1, a_1, 2^x c_1]$ with $x$ any positive integer we will divide our discussion into two cases: $m \neq 0$, $k \leq m$ and $m = 0$. In the following $\mathcal{J}_2$ will designate the set of forms obtained by applying the transformations in $\mathcal{H}$ to $f$.

**Theorem 7:** For $k \neq 0$ and $m \neq 0$ we have in $\mathcal{J}_2$

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. 2</th>
<th>Restrictions</th>
<th>Divisor Represent w.r.t. p</th>
</tr>
</thead>
<tbody>
<tr>
<td>84) 0</td>
<td></td>
<td></td>
<td>$2^0$</td>
</tr>
<tr>
<td>85) $2^{k-(x+2)}$</td>
<td>1 mod 8</td>
<td>$1 \leq x \leq k-3$</td>
<td>$2^x a \cdot 2^{2k-x}$</td>
</tr>
<tr>
<td>86) $2^{k-(x+2)}$</td>
<td>3 mod 8</td>
<td>$1 \leq x \leq k-3$</td>
<td>$2^x a \cdot 2^{2k-x}$</td>
</tr>
<tr>
<td>87) $2^{k-(k+2)}$</td>
<td>5 mod 8</td>
<td>$1 \leq x \leq k-3$</td>
<td>$2^x a \cdot 2^{2k-x}$</td>
</tr>
<tr>
<td>88) $2^{k-(x+2)}$</td>
<td>7 mod 8</td>
<td>$1 \leq x \leq k-3$</td>
<td>$2^x a \cdot 2^{2k-x}$</td>
</tr>
<tr>
<td>89) 2</td>
<td>$(-1 \mid p), 1 \text{ mod } 4$</td>
<td></td>
<td>$2^{k-2} a \cdot 2^{k+2}$</td>
</tr>
<tr>
<td>90) 2</td>
<td>$(-1 \mid p), 3 \text{ mod } 4$</td>
<td></td>
<td>$2^{k-2} a \cdot 2^{k+2}$</td>
</tr>
<tr>
<td>91) 2</td>
<td>N.G.C.</td>
<td></td>
<td>$2^{k-1} a \cdot 2^{k+1}$</td>
</tr>
<tr>
<td>92) 2</td>
<td>N.G.C.</td>
<td></td>
<td>$2^k a \cdot 2^k$</td>
</tr>
</tbody>
</table>

**Proof:** Part 82) is obvious since $z(z+1)$ is even.

Divisor $2^x$, $1 \leq x \leq k-3$. For this divisor we must have
$2^x \parallel az(z+1)$. Therefore $2^x \parallel z$ or $2^x \parallel z+1$. Let us first consider $z = 2^x z_1$. Then $z_1 < 2^{k-x}$. So this yields $2^{k-1}(x+1)$ forms which represent a number of the type $az_1(z^* z_1+1)$. Numbers of this type are equally often congruent to 1, 3, 5 or 7 mod 8. Therefore we have each odd residue mod 8 represented by $2^{k-1}(x+3)$ forms. For $2^x h = z + 1$ with $(h,2) = 1$ we have $2^x h - 1 = z < 2^k$ and again we have $2^{k-1}(x+1)$ forms each of which represents a number of the type $a(2^x h - 1) h$ and these also are equally often congruent to 1, 3, 5 or 7 mod 8. So each odd residue mod 8 is represented by $2^{k-1}(x+3)$ forms. Totaling these results yields 85–88).

Divisor $2^{k-2}$. Parts 89) and 90) follow directly from the preceding paragraph when we let $x = k-2$ and realize that the discriminant of the new forms is congruent to 16 mod 32 so that we have only $(-1|\varphi)$ and that $z_1$ and $h$ are determined mod 4.

Divisor $2^{k-1}$. The discriminant implies that we have no generic characters with respect to 2. The preceding considerations then apply for $z_1 = h = 1$.

Divisor $2^k$. Since $2^k$ precisely divides the middle coefficient we need only that $z^2 + z = z(z+1) \equiv 0 \mod 2^k$. So we have two forms, one with $z = 0$ and the other with $z = 2^k - 1$. The discriminant implies that they have no generic character with respect to 2.
Theorem 8: For \( m = 0 \) all \( 2^k \) forms in \( \mathcal{J}_2 \) have divisor prime to 2. Furthermore, for \( k = 1 \) there is no character with respect to 2, for \( k = 2 \) we have only \((-1|\varphi)\) and the odd residues mod 4 are represented equally often, and for \( k \geq 3 \) we have all three generic characters with respect to 2 and the odd residues mod 8 are represented equally often. All forms represent a \( \mod p \).

Proof: Since \( az(z + 1) \) is even we see that all \( 2^k \) forms in \( \mathcal{J}_2 \) have divisor prime to 2.

For \( k = 1 \), the discriminant is congruent to 4 mod 16 so we have no character with respect to 2.

For \( k = 2 \) the discriminant is congruent to 16 mod 32 so we have only \((-1|\varphi)\). For \( z = 0 \) or 3 the form represents \( c' \mod 4 \) and for \( z = 1 \) or 2 the form represents \( 2a + c' \equiv 2 + c' \mod 4 \).

For \( k \geq 3 \) we have all three characters with respect to 2 since the discriminant is congruent to 0 mod 32. When \( 2^3 \mid z \) we have \( 2^{k-3} \) forms which represent \( c' \mod 8 \). When \( 2^2 \| z \) we have \( 2^{k-3} \) forms which represent \( 4 + c' \mod 8 \).

When \( 2 \| z \) then since we have an equal number of such \( z \)'s such that \( z \equiv 2 \mod 8 \) and \( z \equiv 6 \mod 8 \), we have \( 2^{k-3} \) forms which represent \( 6a + c' \) and \( 2^{k-3} \) forms which represent \( 2a + c' \mod 8 \). If \( (2, z) = 1 \) then since we have an equal number of such \( z \)'s congruent to 1, 3, 5 or 7 mod 8, each of
2a + c', c', 4a + c' and 6a + c' is represented $2^{k-3}$ more times. So altogether each of 1, 3, 5, and 7 mod 8 is represented $2^{k-2}$ times.

Now let us concern ourselves with odd primes $p$. Since all forms are diagonalizable modulo large powers of $p$ we will take $f = [a, 0, c'p^m]$ where discriminant of $f$ is $-4ac'p^m$. Let $\gamma = \{[p^\alpha \atop \beta] | \alpha + \beta = k \text{ and } 0 \leq z < p^\alpha \}$ where $k$ is fixed. On applying a transformation from $\gamma$ to $f$ we get $[ap^{2\alpha}, 2azp^\alpha, az^2 + c'p^{2\beta + m}]$. Denote the totality of forms thus obtained for a fixed $k$ by $\mathfrak{F}_3$. We would like to know how many forms we have in $\mathfrak{F}_3$ with a given power of $p$ as divisor and what these forms represent mod 8 and mod $p$. From the discriminant and coefficients we see that if one of these forms has $2^x$ as divisor then $x \leq 2k$ and $x \leq \frac{m}{2} + k$. 
Theorem 9: For $\frac{m}{2} \geq k$, the maximum exponent of a divisor is $2k$ and we have in $\mathbb{F}_3$

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. $p$</th>
<th>Restrictions</th>
<th>Divisor w.r.t. $2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>93) 0</td>
<td></td>
<td></td>
<td>$p^{2x+1}$</td>
</tr>
<tr>
<td>94) $p^k$</td>
<td>$a$</td>
<td></td>
<td>$p^0$</td>
</tr>
<tr>
<td>95) $p^{k-j}$</td>
<td>$a$</td>
<td>$j=1, \ldots, k$</td>
<td>$p^{2j}$</td>
</tr>
</tbody>
</table>

Proof: We see that if $p^{2x+1}$ divides a form then $2m \geq 2k \geq 2a \geq 2x+1$ which implies that $m \geq a \geq x+1$. From this we see that $p^{x+1} | z$. Therefore $p^{x+1+a} | zp^a$. This implies that $p^{2x+2} | zp^a$. Therefore we can have no odd exponent divisors.

Divisor prime to $p$. If $a = 0$ then $z = 0$ and we have one form with no divisor which represents $a \mod p$ and $a \mod 8$. If $a \neq 0$ then we need $(p, z) = 1$. So we have $p^a - p^{a-1}$ forms with no divisor for each $a$. Each represents $a \mod p$ and $a \mod 8$. Therefore we have $\sum_{a=1}^{k} p^a - p^{a-1} = p^k - 1$ more forms with divisor prime to $p$. Combining these results yields 94).

Divisor $p^{2j}, j = 1, \ldots, k$. For this case we must have $a \geq j$. If $a = j$ then $z = 0$ yields one form which represents $a \mod p$ and $a \mod 8$.

Now let $a = j + i; i = 1, \ldots, k-j$. We then need $p^i \parallel z$. 


Therefore let \( z = p^jz_1 \). Then \( p^jz_1 < p^{j+1} \) implies \( z_1 < p^1 \). Since \( (z_1, p) = 1 \) we have \( p^i - p^{i-1} \) forms for each \( i \). So we have \( \sum_{i=1}^{k-j} p^i - p^{i-1} = p^{k-j} - 1 \) more forms.

Combining these results yields 95).

**Theorem 10:** For \( \frac{m}{2} < k, m \) odd we have in \( \mathcal{E}_3 \)

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. ( p )</th>
<th>Restrictions</th>
<th>Divisor w.r.t. ( 2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>96) ( p^k )</td>
<td>a</td>
<td>( p^0 )</td>
<td>( a \mod 8 )</td>
</tr>
<tr>
<td>97) ( p^{k-j} )</td>
<td>a</td>
<td>( 0 &lt; j \leq \frac{m-1}{2} ) ( p^{2j} )</td>
<td>( a \mod 8 )</td>
</tr>
<tr>
<td>98) ( p^{k-(\frac{m+1}{2}+2j+1)} )</td>
<td>a</td>
<td>( k \geq \frac{m+1}{2} + 2j + 1 ) ( p^{m+2j+1} )</td>
<td>( a \mod 8 )</td>
</tr>
<tr>
<td>99) ( p^{c-(\frac{m+1}{2} + 2j)} )</td>
<td>c</td>
<td>( k \geq \frac{m+1}{2} + 2j ) ( p^{m+2j} )</td>
<td>( a \mod 8 )</td>
</tr>
</tbody>
</table>

**Proof:** The proof of 96) is identical to the proof of 94) of Theorem 9. The proof of 97) involves the same details as 93) of Theorem 9.

**Divisor** \( p^{m+1+2j} \). We must have \( a \geq \frac{m+1}{2} + j \) and \( b \geq j + 1 \).

Therefore \( k \geq \frac{m+1}{2} + 2j + 1 \). This condition is consistent with the maximum divisor condition.

If \( a = \frac{m+1}{2} + j \) then \( z = 0 \) gives one form which represents a mod \( p \) and mod 8.

If \( a = \frac{m+1}{2} + j + 1, i = 1, \ldots, p^{k-(\frac{m+1}{2} + 2j+1)} \) then
we need \( \frac{m+1}{2} + j \parallel z \). So we have \( \sum_{i=1}^{k-(\frac{m+1}{2}+2j+1)} p^i - p^{i-1} = \)

\( k-(\frac{m+1}{2}+2j+1) \) - 1 more forms each representing a mod \( p \) and mod 8. Totaling these results yields 98).

Divisor \( p^{m+2j} \). We must have \( a \geq \frac{m+1}{2} + j \) and \( p^{\frac{m+1}{2}+j} \parallel z \).

So \( \beta = j \). Therefore \( k \geq \frac{m+1}{2} + 2j \) and \( p^{\frac{m+1}{2}+j} \parallel z_2 < p^{k-j} \)

which implies \( z_2 < p \). So we have \( p \)
forms and these represent \( c' \) mod \( p \) and a mod 8.

**Theorem 11**: For \( \frac{m}{2} < k, m \) even, and \( (-ac'|p) = -1 \) we have in \( \mathbb{F}_3 \)

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t.( p )</th>
<th>Restrictions</th>
<th>Divisor</th>
<th>Represent w.r.t.( 2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>100) ( p^k )</td>
<td>a</td>
<td>( m \not</td>
<td>0 )</td>
<td>( p^0 )</td>
</tr>
<tr>
<td>101) ( \frac{p+1}{2} \cdot p^{k-1} )</td>
<td>( \phi(p) = 1 )</td>
<td>( m = 0 )</td>
<td>( p^0 )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>102) ( \frac{p+1}{2} \cdot p^{k-1} )</td>
<td>( \phi(p) = -1 )</td>
<td>( m = 0 )</td>
<td>( p^0 )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>103) ( p^{k-j} )</td>
<td>a</td>
<td>( 0 &lt; j \leq \frac{m}{2} - 1 )</td>
<td>( p^{2j} )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>104) 0</td>
<td></td>
<td></td>
<td>( p^{2x+1} )</td>
<td></td>
</tr>
<tr>
<td>105) 1</td>
<td>N.G.C.</td>
<td>( k = \frac{m}{2} + 2j )</td>
<td>( p^{m+2j} )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>106) ( \frac{p+1}{2} \cdot k-(\frac{m+2j+1}{2}) )</td>
<td>( \phi(p) = 1 )</td>
<td>( m+j \not</td>
<td>0 )</td>
<td>( p^{m+2j} )</td>
</tr>
</tbody>
</table>
67

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t. p</th>
<th>Restrictions</th>
<th>Divisor</th>
<th>Represent w.r.t. 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(107\frac{p+1}{2})</td>
<td>(\varphi</td>
<td>p) = -1)</td>
<td>(m+j \notdiv 0)</td>
<td>(p^{m+2j})</td>
</tr>
<tr>
<td>(p^k - (\frac{m}{2} + 2j + 1))</td>
<td>(k \geq \frac{m}{2} + 2j + 1)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Proof: Divisor prime to \(p\). If \(m \notdiv 0\) then 100) follows from the proof of 96) of Theorem 10.

Let us now consider \(m = 0\). If \(a = 0\) then \(z = 0\) yields one form with no divisor. For \(1 \leq a \leq k-1\) we must have \((z, p) = 1\). There are \(p^a - p^{a-1}\) such \(z\)'s for each \(a\). Therefore we have \(\sum_{a=1}^{k-1} p^a - p^{a-1} = p^{k-1} - 1\) more forms with no divisor which represent \(a \mod p\) and \(\mod 8\). For this it should be noted that \(k \geq 2\). For \(a = k\) and \(s = 0\) any \(z\) yields a form with no divisor. If \(p|z\) then the form represents \(c' \mod p\). If \(p \nmid z\) then the form represents \(az^2 + c' \mod p\). This, coupled with the discussion of divisor \(p^{m+2j}\) yields \(\frac{p+1}{2} \cdot p^{k-1}\) forms with generic character \((\varphi|p) = 1\) and \(\frac{p+1}{2} \cdot p^{k-1}\) forms with generic character \((\varphi|p) = -1\).

Divisor \(p^{2j}, 0 < j \leq \frac{m}{2} - 1\). For \(a = j\) we must have \(z = 0\) and therefore have one form which represents \(a \mod p\) and \(\mod 8\).

Let \(a = j+1; i = 1, \ldots, k-j\). Then we must have \(p^{j} \|| z\). So we have \(p^{i} - p^{i-1}\) forms for each \(i\). Therefore
we have \[ \sum_{i=1}^{k-j} (p-1)p^{i-1} = p^{k-j} - 1 \] more forms representing a mod p and mod 8. Totaling these results yields 103).

Divisor \( p^{2x+1} \). For this divisor we must have \( \alpha \geq x + 1 \) and \( p^{x+1} \mid z \) in order for \( p^{2x+1} \) to divide the first and last coefficients. Therefore \( p^{2x+2} \) divides the middle coefficient and we see that this divisor is impossible.

Divisor \( p^{m+2j}, m+j \not\equiv 0 \). For this divisor we must have \( \alpha \geq \frac{m}{2} + j \) and \( \beta \geq j \). Therefore \( k \geq \frac{m}{2} + 2j \) and this corresponds to the maximum exponent condition.

For \( k = \frac{m}{2} + 2j \) we have \( \alpha = \frac{m}{2} + j \) and \( \beta = j \). So \( z = 0 \) yields one form which represents a mod p and mod 8.

Now consider \( k \geq \frac{m}{2} + 2j + 1 \). For \( \alpha = \frac{m}{2} + j + i; i = 1, \ldots, k-(\frac{m}{2} + 2j + 1) \) we obviously need \( p^{\frac{m}{2}+j} \parallel z \). So we have \( p^{i-1} - p^{i-1} \) forms for each \( i \).

\[ \text{Therefore we have } \sum_{i=1}^{k-(\frac{m}{2}+2j+1)} (p-1)p^{i-1} = p^{k-(\frac{m}{2}+2j+1)} - 1 \] more forms which represent a mod p and mod 8. Our last case is now \( \alpha = k-j, \beta = j \). If \( p^{\frac{m}{2}+j} \parallel z \) we have

\[ p^{k-(\frac{m}{2}+2j+1)} \] forms which represent numbers of the form \( az_1^2 + c \) mod p. So for each \( z_1 \) such that \( 0 < z_1 < p \)

\[ k-(\frac{m}{2}+2j+1) \] we have \( p^{k-(\frac{m}{2}+2j+1)} \) forms which represent \( az_1^2 + c \) mod p.
If \( p^{m+2j+1} \mid z \) the form represents \( c' \mod p \) and we have 
\[
\frac{k-(m+2j+1)}{p} \text{ such forms. All of these forms previously discussed represent a } \mod 8.
\]

Now let us consider \( az_1^2 + c' \).

We know \((az_1^2 + c'|p) = (a|p)\) for \( \frac{p-1}{2} \) values of \( z_1 \)
\[-(a|p)\) for \( \frac{p+1}{2} \) values of \( z_1 \)
where \( 0 \leq z_1 < p \). Our \( z_1 \)'s however are prime to \( p \).

Suppose \( p \equiv 1 \mod 4 \). Then \((-ac'|p) = -1\) implies
\((a|p) = -(c'|p)\). Also
\[
(az_1^2 + c'|p) = (a|p) \text{ for } \frac{p-1}{2} \text{ values of } z_1
\]
\[-(a|p) \text{ for } \frac{p+1}{2} \text{ values of } z_1 \]
where \( 0 < z_1 < p \). So altogether we have
\[
k-(\frac{m}{2}+2j+1) \text{ forms}
\]
which represent a number \( t \) such that \((t|p) = (a|p)\). We also have
\[
k-(\frac{m}{2}+2j+1) \text{ forms}
\]
which represent numbers \( t \) such that \((t|p) = -(a|p)\).

Now suppose \( p \equiv 3 \mod 4 \). Then \((a|p) = (c'|p)\). Also
\[
(az_1^2 + c'|p) = (a|p) \text{ for } \frac{p-3}{2} \text{ values of } z_1
\]
\[-(a|p) \text{ for } \frac{p+1}{2} \text{ values of } z_1 \]
where \( 0 < z_1 < p \). So altogether we have
\[
2 \cdot p^{-\left(\frac{m+2j+1}{2}\right)} \cdot p^{-\frac{3}{2}} \cdot p^{-\left(\frac{m+2j+1}{2}\right)} = p^{\frac{1}{2}} \cdot p^{-\left(\frac{m+2j+1}{2}\right)}
\]
forms which represent numbers \( t \) such that \((t|p) = (a|p)\). Also we have \( p^{\frac{1}{2}} \cdot p^{-\left(\frac{m+2j+1}{2}\right)} \) forms which represent numbers \( t \) such that \((t|p) = -(a|p)\). This finishes 106) and 107).

**Theorem 12:** For \( \frac{m}{2} < k, m \) even, and \((-ac'|p) = 1\) we have in \( \mathfrak{I}_3 \)

<table>
<thead>
<tr>
<th>Number of forms</th>
<th>Represent w.r.t.( p )</th>
<th>Restrictions</th>
<th>Divisor</th>
<th>Represent w.r.t.( 2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>108) ( p^k )</td>
<td>( a )</td>
<td>( m \not\equiv 0 )</td>
<td>( p^0 )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>109) ( p^{k-j} )</td>
<td>( a )</td>
<td>( 0 &lt; j \leq \frac{m}{2} - 1 )</td>
<td>( p^j )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>110) ( 2j + 1 )</td>
<td>( \text{N.G.C.} )</td>
<td>( k = \frac{m}{2} = 2j )</td>
<td>( p^{m+2j} )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>111) ( \frac{p-1}{2} \cdot (1+2j) \cdot (\varphi</td>
<td>p) = 1 ) ( k \geq \frac{m}{2} + 2j+1 )</td>
<td>( \frac{p-1}{2} \cdot (1+2j) \cdot (\varphi</td>
<td>p) = 1 ) ( k \geq \frac{m}{2} + 2j+1 )</td>
<td>( p^{m+2j} )</td>
</tr>
<tr>
<td>112) ( \frac{p-1}{2} \cdot (1+2j) \cdot (\varphi</td>
<td>p) = -1 ) ( k \geq \frac{m}{2} + 2j+1 )</td>
<td>( \frac{p-1}{2} \cdot (1+2j) \cdot (\varphi</td>
<td>p) = -1 ) ( k \geq \frac{m}{2} + 2j+1 )</td>
<td>( p^{m+2j} )</td>
</tr>
<tr>
<td>113) ( 2(j+1) )</td>
<td>( \text{N.G.C.} )</td>
<td>( k = \frac{m}{2} + 2j+1 )</td>
<td>( p^{m+2j+1} )</td>
<td>a mod 8</td>
</tr>
<tr>
<td>114) ( (p-1)(j+1) \cdot (\varphi</td>
<td>p) = 1 ) ( k \geq \frac{m}{2} + 2j+2 )</td>
<td>( (p-1)(j+1) \cdot (\varphi</td>
<td>p) = 1 ) ( k \geq \frac{m}{2} + 2j+2 )</td>
<td>( p^{m+2j+1} )</td>
</tr>
<tr>
<td>115) ( (p-1)(j+1) \cdot (\varphi</td>
<td>p) = -1 ) ( k \geq \frac{m}{2} + 2j+2 )</td>
<td>( (p-1)(j+1) \cdot (\varphi</td>
<td>p) = -1 ) ( k \geq \frac{m}{2} + 2j+2 )</td>
<td>( p^{m+2j+1} )</td>
</tr>
</tbody>
</table>
Proof: First it should be noted that if \( m = 0 \) then the number of divisors prime to \( p \) is found in (111) and (112).

Part 108) is identical in proof to 100) of Theorem 11. Likewise 109) is identical to 103) of Theorem 11.

Divisor \( p^{m+2j} \). For this divisor we see from the discriminant that \( k \geq \frac{m}{2} + 2j \). We also must have \( a \geq \frac{m}{2} + j \).

Consider \( a = \frac{m}{2} + j \). For \( k = \frac{m}{2} + 2j \) we have \( \beta = j \) and no character mod \( p \). However we do have one form with \( z = 0 \) which represents \( a \mod 8 \). Likewise if \( k \geq \frac{m}{2} + 2j + 1 \) we have one form with \( z = 0 \) and this form represents \( a \mod p \) and \( a \mod 8 \).

Now consider \( a = \frac{m}{2} + j + i; i = 1, \ldots, k - (\frac{m}{2} + 2j + 1) \). For these \( a \)'s, \( \beta \geq j + 1 \). Also we must have \( k \geq \frac{m}{2} + 2j + 2 \). We need now \( p^{2+j} \parallel z \). Therefore we have \( p^{1-p^{1-1}} \) forms for each \( i \). So we have \( \sum_{i=1}^{k-\frac{m}{2}+2j+1} p^{1-p^{1-1}} = p^{k-\frac{m}{2}+2j+1} \) more forms which represent \( a \mod p \) and \( a \mod 8 \).

Let us now consider \( a = k - j \). For this \( a, \beta = j \). Since we have already done this case for \( k = \frac{m}{2} + 2j \), we may restrict \( k \) by \( k \geq \frac{m}{2} + 2j + 1 \). Now for \( p^{2+j+1} \parallel z \) we have \( p^{k-\frac{m}{2}+2j+1} \) forms which represent \( c' \mod p \). If \( p^{2+j} \parallel z \) we must have \( az_0^2 + c' \not\equiv 0 \mod p \) and
z_1 < p^{k-(2j+m)}$. As before we know

\[(az_1^2 + c'|p) = -(a|p) \text{ for } \frac{p-1}{2} \text{ values of } z_1 \]
\[(a|p) \text{ for } \frac{p-3}{2} \text{ values of } z_1 \]

where $0 \leq z_1 < p$. However we need $(z_1, p) = 1$.

For $p \equiv 1 \mod 4$ we have $(a|p) = (c'|p)$. So $z_1 \equiv 0 \mod p$ yields $c'$. Therefore our formula becomes

\[(az_1^2 + c'|p) = -(a|p) \text{ for } \frac{p-1}{2} \text{ values of } z_1 \]
\[(a|p) \text{ for } \frac{p-3}{2} \text{ values of } z_1 \]

where $0 < z_1 < p$. So we have $\frac{p-1}{2} \cdot p^{k-(\frac{m}{2}+2j+1)}$ forms with character $-(a|p)$ and $\frac{p-3}{2} \cdot p^{k-(\frac{m}{2}+2j+1)}$ forms with character $(a|p)$.

If $p \equiv 3 \mod 4$ then $-(a|p) = (c'|p)$ and we have

\[(az_1^2 + c'|p) = -(a|p) \text{ for } \frac{p-3}{2} \text{ values of } z_1 \]
\[(a|p) \text{ for } \frac{p-3}{2} \text{ values of } z_1 \]

where $0 < z_1 < p$. So we have $\frac{p-3}{2} \cdot p^{k-(\frac{m}{2}+2j+1)}$ forms with character $(a|p)$ and $\frac{p-3}{2} \cdot p^{k-(\frac{m}{2}+2j+1)}$ forms with character $-(a|p)$.

Now consider $\alpha = k-(j-1)$, $\beta = j-1$ for $i = 1, \ldots, j$. 
Since \( k > \frac{m}{2} + 2j \) we have \( k > \frac{m}{2} + 2j - 1 \) which implies \( k - (j - 1) > \frac{m}{2} + j \). Therefore \( a \) is large enough. We obviously want \( p^{\frac{m}{2} + j - 1} \parallel z \). For these \( z \)'s we have \( p^{k - \frac{m}{2}} \parallel zp^a \). Consider \( k = \frac{m}{2} + 2j \). Then \( a = \frac{m}{2} + j + 1 \), \( \beta = j - 1 \). Also \( p^{m + 2j} \parallel azp^a \). So we must count the solutions of \( az_1^2 + c' = 0 \) and \( p^{2i} \) with \( 0 < z_1 < p^{2i} \). We have two such solutions for each \( i \) so we have \( 2j \) forms with this divisor but they have no character with respect to \( p \).

Now consider \( k > \frac{m}{2} + 2j + 1 \). Then we must count the solutions of \( az_1^2 + c' = q p^{2i} \) mod \( p^{2i+1} \) with \( 0 < q < p \) and \( 0 < z_1 < p^{k - \frac{m}{2} + 2j - 2i} \). Since \((-ac'\mid p) = 1\) we have 2 solutions mod \( p^{2i+1} \). Therefore we have \( 2 \cdot p^{k - (\frac{m}{2} + 2j + 1)} \) solutions for each \( i \) and the corresponding forms represent \( q \). So we have \( 2j \cdot p^{k - (\frac{m}{2} + 2j + 1)} \) forms with this divisor which represent each \( q \) such that \( 0 < q < p \).

Combining these results yields \( 110 \), \( 111 \), and \( 112 \).

**Divisor** \( p^{m + 2j + 1} \). On examining discriminants we see that we must have \( k > \frac{m}{2} + 2j + 1 \). Also we must have \( a > \frac{m}{2} + 2j + 1 \) and \( \beta > j \). Therefore let \( \beta = j - 1 \), \( a = k - j + 1 \) for \( i = 0, \ldots, j \).

We must have \( p^{\frac{m}{2} + j - 1} \parallel z \). Then \( p^{\frac{m}{2} + j - 1 + k - j + 1} = p^{k + \frac{m}{2}} \parallel azp^a \).

Consider \( k = \frac{m}{2} + 2j + 1 \). Then \( p^{\frac{m}{2} + 2j + 1} \parallel azp^a \). So we
want \( az_1^2 + c^' \equiv 0 \mod p^{2i+1} \) with \( 0 < z_1 < p^{2i+1} \). We have two such \( z_1 \)'s for each \( i \) so we get \( 2j + 2 \) forms with this divisor which represent \( a \pmod 8 \) but have no character \( \pmod p \).

Now consider \( k \geq \frac{m}{2} + 2j + 2 \). Again we want \( p^{2i+1} \parallel z \) and also we must count the \( z_1 \)'s for which \( az_1^2 + c^' \equiv q \cdot p^{2i+1} \mod p^{2i+2} \) with \( 0 < z_1 < p^{k-(\frac{m}{2}+2j-2i)} \) and \( 0 < q < p \). We have two solutions to this congruence \( \pmod p^{2i+2} \) so we have \( 2p^{k-(\frac{m}{2}+2j+2)} \) forms for each \( i \) which represent \( q \pmod p \). So we have \( 2(j + 1) \cdot p^{k-(\frac{m}{2}+2j+2)} \) forms which represent each \( q \) such that \( 0 < q < p \). Since all of these forms have divisors with odd exponents they all represent \( a \pmod 8 \).

Totaling these results finishes the theorem.

We will close this chapter with the brief remark that since we have exhausted all possible cases we know the complete story of how many forms we get with a given divisor and what they represent \( \pmod 8 \) and \( \pmod p \) when our forms are derived by applying Hermite transformations with a fixed determinant to a given form.
CHAPTER III

In this chapter we will demonstrate the usage of the results of Chapter II by showing that $r_4[\text{dB}; r]$ is factorable and by showing how to calculate $r_4[\text{dB}; r]$.

In all of this chapter $B$ will be used to designate either a primitive matrix or a form with a primitive matrix of determinant $b$. We will reduce the problem of finding the number of representation $T$ where $\delta_2(T) = r$ to that of finding the number of primitive representations of a certain set of forms.

To determine $r_4[\text{dB}; r]$ where $r^2|d^2 b$ let us first examine $\frac{V^* d B V^*}{r^2}$ where $V$ is hermite of determinant $r$. Since the number of primitive representations of a form depends only on the order of the form we will need the number of $V_p^{1}$ which give us a certain divisor say $p_{1}^{q_{1j}}$ for $\frac{V^* d B V^*}{r^2}$ where as before $V_p^{1}$ is hermite $p_{1}^{2n_{1}}$ and of determinant $p_{1}^{n_{1}}$ and $p_{1}^{n_{1}}|| r$. Define $\chi_d(e; p_{1})$ to be the number of $V_p^{1}$ which give us divisor $p_{1}^{q_{1j}}$ where $p_{1}^{q_{1j}}|| e$. Then the number of $V$'s such that $\frac{V^* d B V^*}{r^2}$ has
divisor $e$ is $\prod_{p|r} \chi_d(e:p)$. For each possible divisor $e$ let $e \phi_e$ be a form with divisor $e$ which can be represented as $V^* dB V^*$. Then $r_4[dB:r] = \sum_{p|r} \prod_{p|r} \chi_d(e:p) r_4[e \phi_e : 1]$. Since $\phi_e$ can be replaced by any form in the same order without altering the validity of the formula and $\phi_e$ has a primitive matrix of determinant $b \over r^2$ for each $e$ we have $r_4[DB:r] = \sum_{e} \prod_{p|r} \chi_d(e:p) r_4[e \phi : 1]$ where $\phi$ has a primitive matrix of determinant $b \over r^2$. In certain cases this result simplifies even further as in the following theorem.

Theorem 1: If $B$ is a form with a primitive matrix of determinant $b$, $r^2|d^2b$ and $(d,r) = 1$ then $r_4[DB:r] = r_4[d \phi : 1]$ where $\phi$ has a primitive matrix of determinant $b \over r^2$.

Proof: Since $(d,r) = 1$ we see that $V^* B V^*$ must have divisor $r^2$ to guarantee that $V^* dB V^*$ be integral. Since $r^2|b$ we see that the exponent of $p$ in $b$ is greater than or equal to twice the exponent of $p$ in $r$ for all primes $p|r$. Then theorems 2 and 9 of Chapter II imply that there is only one $V_p$ for each $p|r$. Therefore there is only one $V$. So from our previous discussion if $d \phi = \frac{V^*dBV^*}{r^2}$ we see that $\phi$ has a primitive matrix of determinant $b \over r^2$ and
that \( r_4[\text{dB}:r] = r_4[\text{d} \phi:1] \).

Professor Pall proved in [5] that the number of representations over all possible \( \text{g.c.d.'s} \) was a factorable function in a certain sense. We would like to do this for representations of \( \text{g.c.d.r} \). To do so we will need the following lemmas.

**Lemma:** If \( e \phi \) is representable as \( \frac{V^{'2} \text{dB} V^{'}}{r^2} \) when \( \phi \) has a primitive matrix, \( B \) has a primitive matrix, and \( V \) is hermite of determinant \( r \) then \( e|d \).

**Proof:** We know that \( V^{-1} = \frac{V^{'}}{r} \). Therefore \( \text{dB} = eV\phi V' \).
Since \( B \) has a primitive matrix \( e|d \).

**Lemma:** If \( (d_1,d_2) = 1, e_1|d_1 \) and \( e_2|d_2 \) then
\[
\chi_{d_1d_2}(e_1e_2:p) = \chi_{d_1}(e_1:p) \cdot \chi_{d_2}(e_2:p).
\]

**Proof:** Since \( p \) divides at most one of \( d_1 \) and \( d_2 \) suppose \( p \not| d_2 \). Also let \( p^n || r \). Let us now examine
\[
\frac{\chi_{d_1d_2}(e_1e_2:p)}{p^{2n}}.
\]
Since \( p \not| d_2 \), the exponent of \( p \) in the divisor of this matrix obviously depends only on \( d_1 \) and \( n \). So \( \chi_{d_1d_2}(e_1e_2:p) = \chi_{d_1}(e_1:p) \). Now consider
\[
\frac{\chi_{d_2}(e:p)}{p^{2n}}.
\]
Since \( p \not| d_2 \), theorems 2 and 9 of Chapter II tell us that \( \chi_{d_2}(e:p) = 1 \) and the lemma is proved.
In light of these lemmas it should be noted that we can now write $r_4[\alpha:B:r] = \sum_{e|d} \prod_{p|r} x_d(e:p) r_4[e:\alpha:l]$, where as before $\alpha$ has a primitive matrix of determinant $\frac{b}{r^2}$.

**Theorem 2:** If $r_4[B:r] \neq 0$ and $(d_1, d_2) = 1$ then

$$\frac{r_4[d_1:B:r]}{r_4[B:r]} \cdot \frac{r_4[d_2:B:r]}{r_4[B:r]} = \frac{r_4[d_1d_2:B:r]}{r_4[B:r]}.$$

**Proof:** We know from our previous work that

$$\frac{r_4[d_1:B:r]}{r_4[B:r]} \cdot \frac{r_4[d_2:B:r]}{r_4[B:r]} =$$

$$\sum_{e_1|d_1} \prod_{p|r} x_{d_1}(e_1:p) \frac{r_4[e_1:\alpha:l]}{r_4[\alpha:l]} \cdot \sum_{e_2|d_2} \prod_{p|r} x_{d_2}(e_2:p) \frac{r_4[e_2:\alpha:l]}{r_4[\alpha:l]}$$

where $\alpha$ has a primitive matrix of determinant $\frac{b}{r^2}$. Then since $(d_1, d_2) = 1$ we have that $(e_1, e_2) = 1$ for all possible $e_1|d_1$ and $e_2|d_2$ and now

$$\frac{r_4[d_1:B:r]}{r_4[B:r]} \cdot \frac{r_4[d_2:B:r]}{r_4[B:r]} =$$

$$\sum_{e_1e_2|d_1d_2} \prod_{p|r} x_{d_1}(e_1:p) \frac{r_4[e_1\alpha:l]}{r_4[\alpha:l]} \cdot \sum_{e_1e_2|d_1d_2} \prod_{p|r} x_{d_2}(e_2:p) \frac{r_4[e_2\alpha:l]}{r_4[\alpha:l]}$$

Now let us demonstrate how to find $r_4[p^wB:r]$. 
Theorem 3: If \( B \) has a primitive matrix of determinant \( b, \) \( r^2 | p^2 \) and \( p \mid r \) then \( r_4[\text{p}^w B : r] = r_4[\text{p}^w \phi : 1] \) where \( \phi \) has a primitive matrix of determinant \( \frac{b}{r^2} \).

**Proof:** When we examine \( \frac{V^* p^w B V^*}{r^2} \) we see that \( V^* B V^* \) must have divisor \( r^2 \) in order that \( \frac{V^* p^w B V^*}{r^2} \) be integral. From theorems 2 and 9 of Chapter II we know there exists only one \( V_q \) such that \( V_q^* B V_q^* \) has divisor \( q^{2n} \) for each \( q \) such that \( q \) is a prime and \( q^q \parallel r \). Therefore there exists only one \( V \) such that \( \frac{V^* p^w B V^*}{r^2} \) is integral.

Let \( p^w \phi = \frac{V^* p^w B V^*}{r^2} \) and since \( |\phi| = \frac{|V^*|}{r^4} |B| = \frac{b}{r^2} \) the theorem is proved.

We will now outline a procedure to calculate \( r_4[\text{p}^w B : r] \) when \( p \mid r, b = |B| \) and \( r^2 | p^2 \). In the following \( q \) will be used to designate a prime. We recall that

\[
r_4[\text{p}^w B : r] = \sum_{e \mid r} \chi_{p^w}(e : q) r_4[\text{e} \phi : 1].
\]

Let \( \chi_{p^w} \) be designated by \( \chi_p \). We also know that if \( q \not\mid p \) then \( \chi(e : q) = 1 \).

Using the fact that \( \frac{V^* p^w B V^*}{r^2} \) can only have divisors which are powers of \( p \) we see that the \( e \)'s range over all the possible powers of \( p \) which can occur as divisors. Our formula can now be rewritten as

\[
r_4[\text{p}^w B : r] = \sum_{e \mid r} \chi(e : p) r_4[\text{e} \phi : 1] \]

when \( e \) ranges over all the possible powers of \( p \) which can occur as divisors. Let \( p^n \parallel r \) then
on examining $V_p^* B V_p^* \cdot p^{w-2n}$ we see that the minimum exponent of $p$ occuring in a divisor is determined since $V_p^* B V_p^* \cdot p^{w-2n}$ must be integral. Then the possible e's and the corresponding $\chi(e:p)$'s are found in the theorems of Chapter II and $r_4[e:\phi:1]$ is found from Chapter I.

Let us further demonstrate this method of determining $r_4[p^B:r]$ by finding the $\chi(e:p)$ in a particular example.

Let $p, r$ and $b = |B|$ be odd. Let $p^n \parallel r$ and $p^t \parallel b$. We will consider the case when $t \geq 2n$. We are only interested in the non-negative integers $h$ such that $V_p^* B V_p^*$ has divisor $p^h$ and $h + w - 2n \geq 0$. Let $m = \max(2n-w,0)$. Then from Theorem 9 of Chapter II we see that we have $p^{n-j}$ forms with divisor $p^{2j}$ as $j$ ranges from 0 to $n$. So in this case $r_4[p^B:r] = \sum_{j=0}^{n-1} p^{n-j} r_4[p^{2j+w-2n}\phi:1]$. 

Since we can determine $r_4[p^B:r]$ in each case and $r_4[dB:r]$ is factorable we can determine $r_4[dB:r]$ for any given $d$, $B$, and $r$. 
BIBLIOGRAPHY


81
BIOGRAPHY

John L. Hunsucker was born on July 1, 1941, in Beaumont, Texas. He graduated from Port Neches-Groves High School in 1959 and entered Lamar State College of Technology where he received a Bachelor of Science in Mathematics in June of 1963. In September of 1963 he entered the graduate school of Louisiana State University where he received a Master of Science in Mathematics in August of 1965 and at which he is presently a candidate for the degree of Doctor of Philosophy in Mathematics.
EXAMINATION AND THESIS REPORT

Candidate: John L. Hunsucker

Major Field: Mathematics

Title of Thesis: REPRESENTATIONS OF A BINARY QUADRATIC FORM

Approved:

[Signatures]

Date of Examination: January 9, 1969