A CANONICAL QUADRATIC FORM FOR THE RING OF 2-ADIC INTEGERS

By Burton W. Jones

1. **Introduction.** One of the fundamental problems in the theory of quadratic forms is the determination of criteria for the arithmetic or rational equivalence of two forms. Hasse [2] has shown that two quadratic forms with rational coefficients are equivalent in $K(1)$ if they are equivalent in the field of reals and in all $K(p)$ where $K(1)$ is the field of rationals and $K(p)$ is the field of p-adic numbers. (Two forms are equivalent in K, or R below, if one may be taken into the other by a transformation in K, or R, whose inverse is also in K, or R.) Siegel [6] has shown the corresponding result for rings, namely, that two forms with rational integral coefficients are of the same genus if and only if they are equivalent in the field of reals and in every $R(p)$ where $R(p)$ is the ring of p-adic integers. (Two forms are said to be of the same genus if, for any integer q, one form may be taken into the other by a transformation whose determinant is prime to q and the denominators of whose elements are prime to q. For more details see [4].) It will be seen that, if the determinants of two forms are equal, the only $R(p)$ which need to be considered are those for p a prime factor of twice the determinant of the form.

It therefore is of interest to determine criteria for equivalence of forms in $R(p)$ and $K(p)$. Hasse [2] has accomplished this for equivalence in the field of rationals by establishing invariants for $K(p)$ along different lines from Minkowski's earlier development [5]. Minkowski found the generic invariants which, however, have the disadvantage of using not only the form but its various concomitants. The establishment here of a canonical form for $R(p)$ avoids this complication and results in a more manageable criterion for equivalence.

Since the derivation of a canonical form for $R(p)$ with p odd is almost trivial, it is left to the last section; and the bulk of this paper is devoted to finding a canonical form for the ring $R(2)$ of 2-adic integers. We use the term "canonical form" in the strict sense that every form shall be equivalent to a unique canonical form. One invariant is introduced, namely $\lambda(\mathfrak{A})$, which is related to Hasse's invariant $c_2(f_0)$ as follows:

$$\lambda(\mathfrak{A}) = -c_2(\mathfrak{A})\left(\frac{-1}{|\mathfrak{A}|}\right),$$

where $|\mathfrak{A}|$ is the determinant of $\mathfrak{A}$. (Hasse shows the relationship between his invariant and that one of Minkowski denoted by C_2 .)

Received May 15, 1944. Correspondence with Gordon Pall indicates that he has by different methods obtained essentially the results of this paper; his work not having been published.

2. **Preliminary definitions and lemmas.** We denote matrices by capital German letters, vectors by lower case German letters and integers in R by lower case italic letters except that we reserve the letters f and g for quadratic forms with variables x_i and coefficients in R. A form and its matrix are said to be *improperly primitive* if the matrix has some unit element but has no unit element on its diagonal. If a matrix or form has a unit diagonal element it is called *properly primitive*. If $a = 2^k b$, where b is a unit and k a rational integer, we write $v(a) = k$ and call k the *value* of a. $v(\mathfrak{A})$ is defined to be the value of the element of $\mathfrak{A}$ of least value. If $a = t^2 b$, where t is a unit in R, write $a \doteq b$.

If f is equivalent to g in R by the above definition we write $f \cong g$ and if $\mathfrak{F}$ and $\mathfrak{G}$ are the corresponding matrices, $\mathfrak{F} \cong \mathfrak{G}$. We also denote

$$\begin{pmatrix} \mathfrak{F}_1 & 0 \\ 0 & \mathfrak{F}_2 \end{pmatrix}$$

by $\{\mathfrak{F}_1, \mathfrak{F}_2\}$. $\mathfrak{E}$ is the identity matrix. A matrix is called *unimodular* if its elements are in R and its determinant is a unit. Thus two matrices or forms are equivalent if and only if there is a unimodular transformation taking one into the other.

Except in §5, *all theorems relate to the ring of 2-adic integers.*

The following lemmas have been proved elsewhere:

LEMMA 1. *If $\mathfrak{F}$ is a symmetric matrix with elements in R, then $\mathfrak{F}$ is equivalent to a matrix*

$$\mathfrak{A} = \{2^{t_1}\mathfrak{A}_1, 2^{t_2}\mathfrak{A}_2, \cdots, 2^{t_k}\mathfrak{A}_k\},$$

where, for every i, $t_i < t_{i+1}$ and $|\mathfrak{A}_i|$ is a unit. Furthermore each $\mathfrak{A}_i$ is either a diagonal form with unit elements or it is one of the following: $\{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}\}$ or $\{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}, \mathfrak{S}\}$, where

$$\mathfrak{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathfrak{S} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Proof. See [4; Lemma 6].

COROLLARY. *If $\mathfrak{A}$ and $\mathfrak{B}$ are two improperly primitive forms of odd determinant, they are equivalent if and only if their determinants are congruent* (mod 8).

LEMMA 2. *If $\mathfrak{A}$ is of the form in Lemma* 1 *and*

$$\mathfrak{A} \cong \mathfrak{B} = \{2^{s_1}\mathfrak{B}_1, 2^{s_2}\mathfrak{B}_2, \cdots, 2^{s_n}\mathfrak{B}_n\},$$

where $s_i < s_{i+1}$ and the $\mathfrak{B}_i$ are of unit determinant, then $k = n$ and $s_i = t_i$ for $i = 1, \cdots, n$.

Proof. This follows from results of Minkowski [5]. A proof may be found in a paper of W. H. Durfee [1, Lemma 2].

In the next section we establish a canonical form. In §4 we prove it is unique.

3. **The determination of a canonical form.** We proceed to specialize still further the form of Lemma 1, first dealing with those transformations which change each $\mathfrak{A}_i$, if necessary, without changing its neighbors.

LEMMA 3. *If* $\mathfrak{x}'\mathfrak{A}\mathfrak{x}$ *is a properly primitive form in r variables and of odd determinant, then, for* $r > 2$,

$$\mathfrak{x}'\mathfrak{A}\mathfrak{x} \cong x_1^2 + x_2^2 + \cdots + ax_{r-2}^2 + bx_{r-1}^2 + cx_r^2 ,$$

where a, b, c take one of the following sets of values:

$$\begin{array}{l} (1, 1, 1) \text{ or } (1, 3, 3) \text{ for } |\mathfrak{A}| \equiv 1 \pmod 8, \\ (1, 1, 5) \text{ or } (1, 3, 7) \text{ for } |\mathfrak{A}| \equiv 5 \pmod 8, \\ (1, 1, 3) \text{ or } (3, 3, 3) \text{ for } |\mathfrak{A}| \equiv 3 \pmod 8, \\ (1, 1, 7) \text{ or } (3, 3, 7) \text{ for } |\mathfrak{A}| \equiv 7 \pmod 8, \end{array} \tag{1}$$

while if $r = 2$, *b and c take one of the following sets of values*

$$\begin{array}{l} (1, 1) \text{ or } (3, 3) \text{ for } |\mathfrak{A}| \equiv 1 \pmod 8, \\ (1, 5) \text{ or } (3, 7) \text{ for } |\mathfrak{A}| \equiv 5 \pmod 8, \\ (1, 3) \qquad \text{for } |\mathfrak{A}| \equiv 3 \pmod 8, \\ (1, 7) \qquad \text{for } |\mathfrak{A}| \equiv 7 \pmod 8. \end{array} \tag{1'}$$

If $r = 1$, $c \equiv |\mathfrak{A}| \pmod 8$ *and c is one of* 1, 3, 5, 7.

Proof. $\mathfrak{A}$ may be assumed to be in diagonal form. The transformation

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \tag{2}$$

takes $x_1^2 + x_2^2 + x_3^2 + x_4^2$ into a form $\equiv -(x_1^2 + x_2^2 + x_3^2 + x_4^2) \pmod 4$. From this it can easily be shown that any form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ with $a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 4$ may be taken into a form $b_1x_1^2 + b_2x_2^2 + b_3x_3^2 + b_4x_4^2$ with $b_1 \equiv b_2 \equiv b_3 \equiv b_4 \equiv -a \pmod 4$. Hence we may make congruent to 1 (mod 4) all but at most three of the coefficients of the form. Also

$$\begin{pmatrix} 1 & -2a/(1 + 4a) \\ 2 & 1/(1 + 4a) \end{pmatrix} \tag{3}$$

takes $x_1^2 + ax_2^2$ into $(1 + 4a)x_1^2 + ax_2^2/(1 + 4a)$ which shows that all but at most one of the coefficients $\equiv 1 \pmod 4$ can be made $\equiv 1 \pmod 8$ and hence equal to 1 since, for every $a \equiv 1 \pmod 8$, $x^2 = a$ is solvable in R. Note also that (3) takes $5x_1^2 + 3x_2^2$ into $x_1^2 + 7x_2^2$ and $7x_1^2 + 7x_2^2$ into $3x_1^2 + 3x_2^2 \pmod 8$. These considerations enable us to complete the proof.

We shall show in §4 that no two such forms are equivalent and hence justify the following

DEFINITION. If (a, b, c) have the values in the first column of (1) or (1') we shall call $\lambda(A) = 1$, if in the second column $\lambda(A) = -1$. Note that $\lambda(A) = 1$ if $A \equiv 3 \pmod 4$ for $r = 2$ or if $r = 1$.

An *equivalent definition* is the following: If $\mathfrak{A}$ is any properly primitive matrix of odd determinant, where $\mathfrak{x}'\mathfrak{A}\mathfrak{x} \cong \sum a_i x_i^2$, then $\lambda(\mathfrak{A})$ is defined to be 1 if $4t$ or $4t + 1$ of the a's are congruent to 3 (mod 4) and -1 if $4t + 2$ or $4t + 3$ are congruent to 3 (mod 4).

Next we consider transformations which change $\mathfrak{A}_i$ at the expense of changing $\mathfrak{A}_k$ for $k > i$.

LEMMA 4. *If $\mathfrak{A}$ is a properly primitive matrix of odd determinant and b is a unit, then*

$$\{\mathfrak{A}, 2b\} \cong \{\mathfrak{A}_1, 2b_1\},$$

where $|\mathfrak{A}_1| \equiv 1 \pmod 4$, $\lambda(\mathfrak{A}_1) = 1$ *and* b_1 *is a unit.*

Proof. The transformation

$$\begin{pmatrix} 1 & -2b/(a+2b) \\ 1 & a/(a+2b) \end{pmatrix} \tag{4}$$

takes $\{a, 2b\}$ into $\{(a + 2b), 2ab/(a + 2b)\}$. Hence, if $\mathfrak{A}$ is in the form of Lemma 3, we can by this means make all its coefficients $\equiv 1 \pmod 4$ and hence $|\mathfrak{A}_1| = \lambda(\mathfrak{A}_1) \equiv 1 \pmod 4$.

LEMMA 5. *If a is a unit,*

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2a \end{pmatrix} \cong \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 10a \end{pmatrix}.$$

Proof. Use the transformation

$$\begin{pmatrix} 1 & 0 & -2a/3 \\ 0 & 1 & -2a/3 \\ 1 & 1 & 1 \end{pmatrix} \tag{5}$$

which takes the first form into $(2 + 2a)x_1^2 + (2 + 2a)x_2^2 + (2 + 4a)x_1x_2 + 2(4a^2/3 + a)x_3^2$. Now $4a^2/3 + a \equiv 4 + a \pmod 8$ and the form may be reduced to the desired form by the transformations used in proving the last part of Lemma 1.

LEMMA 6. *If $\mathfrak{A}$ is a properly primitive matrix of unit determinant and if $\mathfrak{x}'\mathfrak{B}\mathfrak{x} \equiv 4 \pmod 8$ is solvable, then*

$$\{\mathfrak{A}, \mathfrak{B}\} \cong \{\mathfrak{A}_1, \mathfrak{C}\},$$

where $|\mathfrak{A}_1| \equiv 5 |\mathfrak{A}| \pmod 8$ *and if* $\mathfrak{B}$ *is properly primitive so is* $\mathfrak{C}$ *while if* $\mathfrak{B} = 2^t\mathfrak{B}_0$ *and* $\mathfrak{C} = 2^t\mathfrak{C}_0$, *where* $\mathfrak{B}_0$ *and hence* $\mathfrak{C}_0$ *have unit elements with* $t > 0$, *then* $\mathfrak{B}_0$ *and* $\mathfrak{C}_0$ *are both properly primitive or both improperly primitive.*

Proof. We may assume $\mathfrak{A}$ to be in the form of Lemma 3 and, by Lemma 1, $\mathfrak{B}_0 = \{\mathfrak{B}_1, 2\mathfrak{B}_2\}$, where $\mathfrak{B}_1$ has a unit determinant and is of the form prescribed in Lemma 1. Let a be some unit element of $\mathfrak{A}$ and $\mathfrak{x}_0$ a solution of $\mathfrak{x}'\mathfrak{B}\mathfrak{x} \equiv 4 \pmod 8$. The transformation

$$\begin{pmatrix} 1 & -\mathfrak{x}_0'\mathfrak{B}/(a + \mathfrak{x}_0'\mathfrak{B}\mathfrak{x}_0) \\ \mathfrak{x}_0 & \mathfrak{B}^{-1}\mathfrak{D} \end{pmatrix}$$

takes $\{a, \mathfrak{B}\}$ into $\{a + \mathfrak{x}_0'\mathfrak{B}\mathfrak{x}_0, \mathfrak{D}\}$, where

$$\mathfrak{D} = \mathfrak{B} - \mathfrak{B}\mathfrak{x}_0\mathfrak{x}_0'\mathfrak{B}/(a + \mathfrak{x}_0'\mathfrak{B}\mathfrak{x}_0).$$

Then if $\mathfrak{A} = \{\mathfrak{A}^{(1)}, a\}$, $\mathfrak{A}_1 = \{\mathfrak{A}^{(1)}, a + \mathfrak{x}_0'\mathfrak{B}\mathfrak{x}_0\}$ we have $|\mathfrak{A}_1| \equiv 5 |\mathfrak{A}| \pmod 8$. If $\mathfrak{B}$ is properly primitive take $\mathfrak{x}_0^1 : (2, 0, \cdots, 0)$ and have $\mathfrak{D} \equiv \mathfrak{B} \pmod 4$ which shows that $\mathfrak{D}$ is properly primitive. On the other hand, if $\mathfrak{B} = 2^t\mathfrak{B}_0$ with $t > 0$, we have $\mathfrak{D}/2^t \equiv \mathfrak{B}_0 \pmod{2^t}$ which completes our proof.

The results of these lemmas are collected in

THEOREM 1. *Every symmetric matrix in* R *is equivalent in* R *to a matrix*

$$\mathfrak{A} = \{2^{t_1}\mathfrak{A}_1, 2^{t_2}\mathfrak{A}_2, \cdots, 2^{t_n}\mathfrak{A}_n\},$$

where, for every i, $t_i < t_{i+1}$ *and* $|\mathfrak{A}_i|$ *is a unit. Furthermore, every* $\mathfrak{A}_i$ *is in the form prescribed in Lemma* 3 *or* $\{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}\}$ *or* $\{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}, \mathfrak{S}\}$ *subject to the following further conditions*:

1. *If* $\mathfrak{A}_{i+1}$ *is properly primitive and* $t_{i+1} = t_i + 1$, *then* $\mathfrak{A}_i = \{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}\}$ *if* $\mathfrak{A}_i$ *is improperly primitive while* $\lambda(\mathfrak{A}_i) = 1 \equiv |\mathfrak{A}_i| \pmod 4$ *if* $\mathfrak{A}_i$ *is properly primitive.*

2. *If* $\mathfrak{A}_i$ *is properly primitive and* $x'\{2^{t_{i+1}-t_i}\mathfrak{A}_{i+1}, 2^{t_{i+2}-t_i}\mathfrak{A}_{i+2}\}x \equiv 4 \pmod 8$ *solvable, then* $|\mathfrak{A}_i| \equiv \pm 1 \pmod 8$.

3. *If the initial conditions for both* 1 *and* 2 *hold with* $\mathfrak{A}_i$ *properly primitive, then* $|\mathfrak{A}_i| \equiv 1 \pmod 8$ and $\lambda(\mathfrak{A}_i) = 1$.

DEFINITION. We call a form or matrix *canonical* if it satisfies the conditions of Theorem 1.

4. **The uniqueness of the canonical form.** To Gordon Pall is due that portion of the following proof preceding the division into cases.

THEOREM 2. *If* a *is a unit and either* $v(\mathfrak{B}) = v(\mathfrak{C}) > 0$ *or* $\mathfrak{B}$ *and* $\mathfrak{C}$ *are both properly primitive or both improperly primitive,* $\{a, \mathfrak{B}\} \cong \{a, \mathfrak{C}\}$ *implies* $\mathfrak{B} \cong \mathfrak{C}$.

Proof. The equation

$$\begin{pmatrix} p & \mathfrak{P}_3' \\ \mathfrak{P}_2' & \mathfrak{P}_4' \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & \mathfrak{B} \end{pmatrix}\begin{pmatrix} p & \mathfrak{P}_2 \\ \mathfrak{P}_3 & \mathfrak{P}_4 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & \mathfrak{C} \end{pmatrix}$$

is equivalent to

$$p^2a + \mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_3 = a, \tag{6}$$

$$pa\mathfrak{P}_2 + \mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4 = (0), \tag{7}$$

$$\mathfrak{P}_2'a\mathfrak{P}_2 + \mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4 = \mathfrak{C}. \tag{8}$$

If $p \neq 0$ we solve (7) for $\mathfrak{P}_2$ and substitute it in (8) to get

$$\mathfrak{P}_4'\mathfrak{B}_0\mathfrak{P}_4 = \mathfrak{C}, \tag{9}$$

where $\mathfrak{B}_0 = \mathfrak{B}\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{B}/p^2a + \mathfrak{B}$. We then seek a matrix $\mathfrak{D}$ such that

$$(\mathfrak{E} + \mathfrak{B}\mathfrak{P}_3\mathfrak{D}'\mathfrak{P}_3')\mathfrak{B}(\mathfrak{E} + \mathfrak{P}_3\mathfrak{D}\mathfrak{P}_3'\mathfrak{B}) = \mathfrak{B}_0 . \tag{10}$$

Substitution of the value of $\mathfrak{B}_0$ shows that this search will be ended if

$$\mathfrak{D}' + \mathfrak{D} + \mathfrak{D}'\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_3\mathfrak{D} = 1/p^2a.$$

If $\mathfrak{D}$ is non-singular, multiply the above on the left by $(\mathfrak{D}')^{-1}$ and on the right by $\mathfrak{D}^{-1}$ to get

$$\mathfrak{D}^{-1} + (\mathfrak{D}')^{-1} + \mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_3 = (\mathfrak{D}\mathfrak{D}')^{-1}/p^2a. \tag{11}$$

If $\mathfrak{D}^{-1} = pa(\pm 1 + p)$, equation (11) is equivalent to (6).

Then, from (9) and (10), we see that $\mathfrak{T} = \mathfrak{P}_4 + \mathfrak{P}_3\mathfrak{D}\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4$ takes $\mathfrak{B}$ into $\mathfrak{C}$. Since the hypothesis of the theorem implies $|\mathfrak{B}| \doteq |\mathfrak{C}|$ we see that $\mathfrak{T}$ has unit determinant and if we can show that its elements are in R we will have $\mathfrak{B} \cong \mathfrak{C}$. This will be shown if $v(\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4) \geq v[pa(\pm 1 + p)] = v(pa) + v(\pm 1 + p)$. We now divide our proof into cases.

1. If $v(p) > 0$ and $p \neq 0$, we have $v(\pm 1 + p) = 0$ and (7) shows $v(pa) = v(\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4) \leq v(\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4)$.

2. If $v(p) = 0$ and $v(\mathfrak{B}) > 0$, we can choose the ambiguous sign in $\mathfrak{D}^{-1}$ so that $v(\mathfrak{D}^{-1}) = 1$ and hence $v(\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4) \geq v(\mathfrak{D}^{-1})$.

3. If $p = 0$, (6) and (7) reduce to $\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_3 = a$ and $\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4 = 0$. The former equation implies $v(\mathfrak{P}_3) = 0$ which allows us to construct a unimodular matrix $\mathfrak{K}$ whose first column is $\mathfrak{P}_3$. $\mathfrak{K}$ takes $\mathfrak{B}$ into a form $\mathfrak{B}_1$ whose leading element is a, and a transformation of the form $\begin{pmatrix} 1 & q \\ 0 & \mathfrak{E} \end{pmatrix}$ takes $\mathfrak{B}_1$ into $\{a, \mathfrak{B}_2\}$. Thus

$$\mathfrak{S} = \mathfrak{K}\begin{pmatrix} 1 & q \\ 0 & \mathfrak{E} \end{pmatrix}$$

takes $\mathfrak{B}$ into $\{a, \mathfrak{B}_2\}$ and the first column of $\mathfrak{S}$ is $\mathfrak{P}_3$. Thus the transformation

$$\mathfrak{R} = \begin{pmatrix} 1 & 0 \\ 0 & \mathfrak{S}^{-1} \end{pmatrix}\begin{pmatrix} 0 & \mathfrak{P}_2 \\ \mathfrak{P}_3 & \mathfrak{P}_4 \end{pmatrix}$$

takes $\{a, a, \mathfrak{B}_2\}$ into $\{a, \mathfrak{C}\}$. The first column of $\mathfrak{R}$ is $(0, 1, 0, \cdots, 0)'$ since $\mathfrak{S}^{-1}\mathfrak{P}_3 = (1, 0, \cdots, 0)'$. Since

$$\mathfrak{Q} = \left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathfrak{E}\right\}$$

is an automorph of $\{a, a, \mathfrak{B}_2\}$, the transformation $\mathfrak{Q}\mathfrak{R}$ takes $\{a, a, \mathfrak{B}_2\}$ into $\{a, \mathfrak{C}\}$. Now the first column of $\mathfrak{Q}\mathfrak{R}$ is $(1, 0, \cdots, 0)'$. We may thus write

$$\mathfrak{Q}\mathfrak{R} = \begin{pmatrix} 1 & \mathfrak{R}_3 \\ 0 & \mathfrak{R}_4 \end{pmatrix}$$

with $\mathfrak{R}_4$ unimodular. The equation corresponding to (7) implies $\mathfrak{R}_3 = 0$ and hence $\mathfrak{R}_4$ takes $\{a, \mathfrak{B}_2\}$ into $\mathfrak{C}$, that is, $\mathfrak{B} \cong \mathfrak{C}$.

4. Suppose $v(p) = 0 = v(\mathfrak{B})$. By considering the inverse of the transformation we may assume $\mathfrak{P}_4$ is unimodular. If $v(\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4) > 0$, that is, $v(\mathfrak{P}_2) > 0$, we can use the argument of Case 2 above. Thus we need to consider only $v(\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4) = 0$ which implies $v(\mathfrak{P}_3) = 0$.

Our theorem trivially holds if $\mathfrak{B}$ and $\mathfrak{C}$ have just one variable since $|\mathfrak{B}| \doteq |\mathfrak{C}|$. We assume the theorem for all $\mathfrak{B}$ and $\mathfrak{C}$ smaller than the ones under consideration. Consider $\mathfrak{B}$ and $\mathfrak{C}$ in canonical form.

Since $\mathfrak{P}_4$ is unimodular, $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ represents some unit if $\mathfrak{B}$ is properly primitive and hence if the first r elements of $\mathfrak{B}$ and $\mathfrak{C}$ are units ($r \geq 1$), equation (8) shows that one of the first r elements of $\mathfrak{P}_2$ is a non-unit. Permute the variables in $\mathfrak{B}$ and $\mathfrak{C}$ if necessary to make it the first. Then, b, the leading element of $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$, is congruent (mod 4) to c, the leading element of $\mathfrak{C}$. We postpone until the end the case where $\mathfrak{B}$ and $\mathfrak{C}$ are improperly primitive.

First, if $c \equiv a \pmod 4$, for properly chosen s_i, the transformation

$$\begin{pmatrix} 2s_1 & s_2 & 0 \\ s_3 & 2s_4 & 0 \\ 0 & 0 & \mathfrak{E} \end{pmatrix}$$

is an automorph of $\{a, \mathfrak{C}\}$, for it may be shown [1; Theorem 2] that $a = 4s_1^2a + s_2^2c$ and $c = s_3^2a + 4s_4^2c$ have solutions. Then the transformation

$$\begin{pmatrix} p & \mathfrak{P}_2 \\ \mathfrak{P}_3 & \mathfrak{P}_4 \end{pmatrix} \begin{pmatrix} 2s_1 & s_2 & 0 \\ s_3 & 2s_4 & 0 \\ 0 & 0 & \mathfrak{E} \end{pmatrix}$$

takes $\{a, \mathfrak{B}\}$ into $\{a, \mathfrak{C}\}$ and has a non-unit as its leading element. Then as in Case 1 or Case 3 we can prove $\mathfrak{B} \cong \mathfrak{C}$.

Second, if $c \not\equiv a \pmod 4$, it follows that $b \not\equiv a \pmod 4$. There will then be a unimodular transformation $\mathfrak{Q}$, whose first column and row $\equiv (1, 0, \cdots, 0) \pmod 2$, taking $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ into $\{b, \mathfrak{B}_1\}$. If $\mathfrak{B}_1$ has a unit diagonal element we may by a unimodular transformation $\equiv \mathfrak{E} \pmod 2$ take $\{b, \mathfrak{B}_1\}$ into $\{c_1, \mathfrak{B}_2\}$ where $c_1 \equiv c \pmod 8$ and [1; Theorem 3] we can then by a unimodular transformation $\equiv \mathfrak{E} \pmod 2$ take $\{c_1, \mathfrak{B}_2\}$ into $\{c, \mathfrak{B}_3\}$. Thus we have a transformation $\mathfrak{Q}_1$ taking $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ into $\{c, \mathfrak{B}_3\}$. Then it may be seen that the transformation

$$\mathfrak{R} = \begin{pmatrix} p & \mathfrak{P}_2 \\ \mathfrak{Q}_1^{-1}\mathfrak{P}_4^{-1}\mathfrak{P}_3 & \mathfrak{Q}_1^{-1} \end{pmatrix}$$

takes $\{a, c, \mathfrak{B}_3\}$ into $\{a, c, \mathfrak{C}_1\}$ where $\mathfrak{C} = \{c, \mathfrak{C}_1\}$. Equation (8) with the leading element of $\mathfrak{P}_2$ a non-unit and that of $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ a unit implies that the first column of $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ is congruent to $(1, 0, \cdots, 0) \pmod 2$. Then, writing equation (7) in the form

$$pa\mathfrak{P}_2 + \mathfrak{P}_3'\mathfrak{P}_4^{-1'}\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4 = 0, \tag{12}$$

we see that the leading element of $\mathfrak{P}_3'\mathfrak{P}_4^{-1'}$ is a non-unit. Furthermore, since the first row and column of $\mathfrak{Q}_1$ are congruent to $(1, 0, \cdots, 0) \pmod 2$, the same is true of $\mathfrak{Q}_1^{-1}$. This shows that the second row and column of $\mathfrak{R}$ are congruent to $(0, 1, 0, \cdots, 0) \pmod 2$. Then the transformation

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \mathfrak{E} \end{pmatrix} \mathfrak{R} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \mathfrak{E} \end{pmatrix}$$

takes $\{c, a, \mathfrak{B}_3\}$ into $\{c, a, \mathfrak{C}_1\}$ and, in this transformation, the first row $\equiv (1, 0, \cdots, 0) \pmod 2$, that is, the new $\mathfrak{P}_2$ has positive value which, by the third sentence of this Case 4, shows $\{a, \mathfrak{B}_3\} \cong \{a, \mathfrak{C}_1\}$. Then since $\mathfrak{B}_3$ has a unit diagonal element if $\mathfrak{B}_1$ has, we see by the hypothesis of the induction that $\mathfrak{B}_3 \cong \mathfrak{C}_1$. Then, by retracing various steps we find $\mathfrak{B} \cong \mathfrak{C}$.

It remains to consider what happens when $b \equiv c \not\equiv a \pmod 4$ and $\mathfrak{B}_1$ is improperly primitive. Then (8) shows that the first r elements of $\mathfrak{P}_2$ are congruent to $(0, 1, \cdots, 1) \pmod 2$, where the largest principal minor of odd determinant in C and hence in $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ has r rows. Thus (8) implies that the leading r by r minor of $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 1 & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & 1 & 1 & \cdots & 1 & 0 \end{pmatrix} \pmod 2.$$

Then equation (12) shows that the first r elements of $\mathfrak{P}_3'(\mathfrak{P}_4')^{-1}$ are congruent to $(0, t, \cdots, t)$ (mod 2) for $t = 1$ or 0. Furthermore, the transformation

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

takes $bx_1^2 + 2dx_2^2 + 2x_2x_3 + 2dx_3^2$ into a form $\equiv -bx_1^2 + ex_2^2 + hx_3^2$ (mod 4) and hence there is a transformation

$$\mathfrak{R} \equiv \begin{pmatrix} 1 & 1 & 1 & \mathfrak{N} \\ 1 & 1 & 0 & \\ 1 & 0 & 1 & \\ & \mathfrak{N}' & & \mathfrak{E} \end{pmatrix} \pmod 2,$$

where $\mathfrak{N}$ is a null matrix, taking $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ into $\{b_1, \mathfrak{B}_2\}$, where $\mathfrak{B}_2$ is properly primitive and $b_1 \equiv -b \equiv a$ (mod 4). Hence the transformation

$$\mathfrak{T}_1 = \begin{pmatrix} p & \mathfrak{P}_2 \\ \mathfrak{R}^{-1}\mathfrak{P}_4^{-1}\mathfrak{P}_3 & \mathfrak{R}^{-1} \end{pmatrix}$$

takes $\{a, b_1, \mathfrak{B}_2\}$ into $\{a, c, \mathfrak{C}_1\}$, where, in virtue of the fact that the first r elements of $\mathfrak{P}_3'\mathfrak{P}_4^{-1'}$ are congruent to $(0, t, \cdots, t)$ (mod 2), the leading element of $\mathfrak{R}^{-1}\mathfrak{P}_4^{-1}\mathfrak{P}_3$ is a non-unit. Then, since we can find an automorph

$$\begin{pmatrix} 2s_1 & s_2 \\ s_3 & 2s_4 \end{pmatrix}$$

of $\{a, b_1\}$ we have a transformation

$$\mathfrak{T}_2 = \begin{pmatrix} 2s_1 & s_2 & \mathfrak{N} \\ s_3 & 2s_4 & \\ & \mathfrak{N}' & E \end{pmatrix} \mathfrak{T}_1$$

taking $\{a, b_1, \mathfrak{B}_2\}$ into $\{a, c, \mathfrak{C}_1\}$, where the leading element of $\mathfrak{T}_2$ is a non-unit. We proceed then as in Case 1 or Case 3.

We now consider the postponed case, namely, $\mathfrak{B}$ and $\mathfrak{C}$ improperly primitive. $\mathfrak{P}_4$ unimodular implies that $\mathfrak{P}_4'\mathfrak{B}\mathfrak{P}_4$ is also improperly primitive. (8) shows that the principal diagonal terms of $\mathfrak{P}_2'\mathfrak{P}_2$ are all of positive value and hence $v(\mathfrak{P}_2) > 0$ which implies $v(\mathfrak{P}_3'\mathfrak{B}\mathfrak{P}_4) > 0$, which can be dealt with as in Case 2.

COROLLARY 1. *If* $\{a, \mathfrak{B}\} \cong \{b, \mathfrak{C}\}$, *where* $\mathfrak{B}$ *and* $\mathfrak{C}$ *satisfy the conditions of the theorem, if* $a \equiv b$ (mod 8) *and* a *and* b *are units, then* $\mathfrak{B} \cong \mathfrak{C}$.

This holds since $ax^2 = b$ then has a solution in $\mathfrak{R}$.

COROLLARY 2. *If* $\{a_1, a_2, \mathfrak{B}\} \cong \{b_1, b_2, \mathfrak{C}\}$, *where* $\mathfrak{B}$ *and* $\mathfrak{C}$ *satisfy the condi-*

tions of the theorem and if $a_1 - b_1 \equiv a_2 - b_2 \equiv 0$ *or* 4 (mod 8) *with* a_i *and* b_i *units, then* $\mathfrak{B} \cong \mathfrak{C}$.

This follows from Corollary 1 if $a_i \equiv b_i \pmod 8$. If $a_i - b_i \equiv 4 \pmod 8$ apply first the transformation (3) which takes $\{a_1 , a_2\}$ into $\{c_1 , c_2\}$ with $c_i \equiv a_i + 4 \equiv b_i \pmod 8$.

If $\mathfrak{A}$ and $\mathfrak{B}$ are the matrices of two equivalent canonical forms we may from Lemmas 1 and 2 write

$$\begin{aligned} \mathfrak{A} &= \{2^{t_1}\mathfrak{A}_1 , 2^{t_2}\mathfrak{A}_2 , \cdots , 2^{t_n}\mathfrak{A}_n\}, \\ \mathfrak{B} &= \{2^{t_1}\mathfrak{B}_1 , 2^{t_2}\mathfrak{B}_2 , \cdots , 2^{t_n}\mathfrak{B}_n\}. \end{aligned} \tag{13}$$

Furthermore, since both or neither form represents a unit multiple of 2^{t_1} it follows that both or neither $\mathfrak{x}'\mathfrak{A}_1\mathfrak{x}$, $\mathfrak{x}'\mathfrak{B}_1\mathfrak{x}$ represent units. We then prove

THEOREM 3. *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are two equivalent canonical matrices* (13) *and* $\mathfrak{A}_1$ *or* $\mathfrak{B}_1$ *represent a unit, then* $\mathfrak{A}_1 = \mathfrak{B}_1$.

Proof. Suppose $\mathfrak{A}_1 \neq \mathfrak{B}_1$ and, for simplicity, take $t_1 = 0$.

First, if $\lambda(\mathfrak{A}_1) \neq \lambda(\mathfrak{B}_1)$ we may assume by condition 1 of Theorem 1 that either $t_2 > 1$ or one of $\mathfrak{A}_2$, $\mathfrak{B}_2$ is improperly primitive. Now if $\mathfrak{B}_2$ were properly primitive and $t_2 = 1$ we could, by the transformation used in Lemma 4, make $\lambda(\mathfrak{B}_1) = \lambda(\mathfrak{A}_1)$ and successive applications of Theorem 2 would show

$$\mathfrak{x}'\{2^{t_2}\mathfrak{A}_2 , \cdots , 2^{t_n}\mathfrak{A}_n\}\mathfrak{x} \cong \mathfrak{x}'\{2^{t_2}\mathfrak{B}_2 , \cdots , 2^{t_n}\mathfrak{B}_n\}\mathfrak{x} \pmod 4$$

which would imply that $\mathfrak{A}_2$ is properly primitive. Hence $\mathfrak{A}_2$ and $\mathfrak{B}_2$ are both improperly primitive or $t_2 > 1$. Then $\mathfrak{x}'\mathfrak{A}_1\mathfrak{x} \cong \mathfrak{x}'\mathfrak{B}_1\mathfrak{x} \pmod 4$ which, by Theorem 2, would lead to $x_1^2 + x_2^2 \cong 3x_1^2 + 3x_2^2 \pmod 4$, which is false.

Second, if $|\mathfrak{A}_1| \neq |\mathfrak{B}_1| \pmod 4$ we proceed as in the above case.

Third, if $\lambda(\mathfrak{A}_1) = \lambda(\mathfrak{B}_1)$ and $|\mathfrak{A}_1| \equiv 5\,|\mathfrak{B}_1| \pmod 8$ we may assume by condition 2 of Theorem 1 that

$$\mathfrak{x}'\{2^{t_2}\mathfrak{A}_2 , 2^{t_3}\mathfrak{A}_3\}\mathfrak{x} \equiv 4 \pmod 8$$

is not solvable and similarly for $\mathfrak{B}$. Then Theorem 2 would lead to

$$\mathfrak{x}'\{a, 2^{t_2}\mathfrak{A}_2 , 2^{t_3}\mathfrak{A}_3 , \cdots\}\mathfrak{x} \cong \mathfrak{x}'\{b, 2^{t_2}\mathfrak{B}_2 , \cdots\}\mathfrak{x}$$

with $a \equiv 5b \pmod 8$. The first form would then represent no numbers congruent to b (mod 8) which would deny the equivalence.

THEOREM 4. *If* $\mathfrak{A}_1$ *and* $\mathfrak{B}_1$ *are improperly primitive equivalent forms of odd determinant and* a *and* b *are units, then* $\{\mathfrak{A}_1 , a, \mathfrak{A}_2\} \cong \{\mathfrak{B}_1 , b, \mathfrak{B}_2\}$ *implies* $\{a, \mathfrak{A}_2\} \cong \{b, \mathfrak{B}_2\}$.

Proof. We may identify $\mathfrak{A}_1$ and $\mathfrak{B}_1$ and notice that it is sufficient to prove the theorem for $\mathfrak{A}_1$ a 2 by 2 matrix of one of the forms

$$\mathfrak{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathfrak{S} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

First, suppose $\mathfrak{A}_1 = \mathfrak{T}$. The transformation

$$\begin{pmatrix} 1 & 1 & -a \\ 1 & -a & a+1 \\ 1 & 0 & -a \end{pmatrix}$$

takes $\mathfrak{x}'\{a, \mathfrak{A}_1\}\mathfrak{x}$ into a form $\equiv \mathfrak{x}'\{(a+2), a, -(2+a)\}\mathfrak{x} \pmod 8$ and we have $\{a+2, -(2+a), a, \mathfrak{A}_2\} \cong \{b+2, -(2+b), b, \mathfrak{B}_2\}$. If $b \equiv a \pmod 4$, $(b+2) - (a+2) \equiv -(2+b) + 2 + a \equiv 0$ or $4 \pmod 8$ and Corollary 2 of Theorem 2 applies to prove our theorem. If $b \equiv -a \pmod 4$, $b + 2 + 2 + a \equiv -(2+b) - (a+2) \equiv 0$ or $4 \pmod 8$ and, as before, our proof is complete.

Second, suppose $\mathfrak{A}_1 = \mathfrak{S}$. The transformation

$$\begin{pmatrix} 1 & 1 & -2-3a \\ 1 & -3a & 1+a \\ 1 & 0 & -3a \end{pmatrix}$$

takes $\mathfrak{x}'\{a, \mathfrak{A}_1\}\mathfrak{x}$ into $\mathfrak{x}'\{(a-2), (a+2), -a\}\mathfrak{x} \pmod 8$. We may consider $\mathfrak{A}_2$ and $\mathfrak{B}_2$ both of positive value or having a unit diagonal element since $\{a, \mathfrak{A}_2\}$ is equivalent to $\{a_1, \mathfrak{A}_3\}$, where $\mathfrak{A}_3$ has the property required.

If $b \equiv a \pmod 8$, $b - 2 - (a-2) \equiv b + 2 - (a+2) \equiv 0 \pmod 8$ and, by corollaries 1 and 2 of Theorem 2, $\mathfrak{A}_2 \cong \mathfrak{B}_2$ which implies our theorem.

If $b \equiv 5a \pmod 8$, $b - 2 \equiv a + 2 \pmod 8$ and $b + 2 - (a-2) \equiv -b + a \equiv 0$ or $4 \pmod 8$. Thus Corollary 2 of Theorem 2 implies $\{b-2, \mathfrak{B}_2\} \cong \{a+2, \mathfrak{A}_2\}$ and Corollary 1 implies $\mathfrak{B}_2 \cong \mathfrak{A}_2$ which proves our theorem.

Otherwise, suppose $b \equiv -a \pmod 4$. Then $\lambda\{a, \mathfrak{A}_1\} \neq \lambda\{b, \mathfrak{B}_1\}$. We see first that $\mathfrak{x}'\mathfrak{A}_2\mathfrak{x} \equiv \mathfrak{x}'\mathfrak{B}_2\mathfrak{x} \equiv 0 \pmod 4$ is not possible, for if it were, the proof of Theorem 1 would show that we could put $\{\mathfrak{A}_1, a, \mathfrak{A}_2\}$ and $\{\mathfrak{B}_1, b, \mathfrak{B}_2\}$ into canonical form without altering $\lambda\{\mathfrak{A}_1, a\}$ or $\lambda\{\mathfrak{B}_1, b\}$. This would then contradict Theorem 3. Also suppose $\mathfrak{x}'\{a, \mathfrak{A}_2\}\mathfrak{x} \equiv b \pmod 4$ were solvable; we could find $\{a_1, \mathfrak{A}_3\} \cong \{a, \mathfrak{A}_2\}$ with $a_1 \equiv b \pmod 4$ and deal with it as above.

It thus remains to consider the case $b \equiv -a \pmod 4$, $v(\mathfrak{A}_2) = 0 = v(\mathfrak{B}_2)$ with neither of the following solvable: $\mathfrak{x}'\{a, \mathfrak{A}_2\}\mathfrak{x} \equiv b \pmod 4$ or $\mathfrak{x}'\{b, \mathfrak{B}_2\}\mathfrak{x} \equiv a \pmod 4$. This implies $\mathfrak{x}'\{a, \mathfrak{A}_2\}\mathfrak{x} \equiv ax_1^2 + ax_2^2 \pmod 4$ and $\mathfrak{x}'\{b, \mathfrak{B}_2\}\mathfrak{x} \equiv bx_1^2 + bx_2^2 \pmod 4$. Thus $\mathfrak{x}'\{\mathfrak{A}_1, a, \mathfrak{A}_2\}\mathfrak{x}$ is equivalent to a form $\equiv \mathfrak{x}'\{-a, -a, -a, a\}\mathfrak{x} \pmod 4$ while $\mathfrak{x}'\{\mathfrak{A}_1, b, \mathfrak{B}_2\}\mathfrak{x}$ to a form $\equiv \mathfrak{x}'\{-b, -b, -b, b\}\mathfrak{x} \equiv \mathfrak{x}'\{a, a, a, -a\}\mathfrak{x} \pmod 4$. Thus the λ invariants are not equal and by the above discussion the hypothesis of our theorem is contradicted.

We have the almost obvious

LEMMA 7. *If* $\mathfrak{A} = \{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}, \mathfrak{S}, \cdots, \mathfrak{S}\}$ *and* $\mathfrak{B} = \{\mathfrak{T}, \mathfrak{T}, \cdots, \mathfrak{T}, \mathfrak{S}, \cdots, \mathfrak{S}\}$, *where*

$$\mathfrak{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathfrak{S} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

and, though $\mathfrak{A}$ *and* $\mathfrak{B}$ *are of the same order, one need not contain the same number of* $\mathfrak{T}$*'s as the other, then* $\mathfrak{x}'\mathfrak{A}\mathfrak{x} \equiv \mathfrak{x}'\mathfrak{B}\mathfrak{x} \pmod 4$ *implies* $\mathfrak{A} = \mathfrak{B}$.

Proof. $\mathfrak{x}'\mathfrak{A}\mathfrak{x} \equiv \mathfrak{x}'\mathfrak{B}\mathfrak{x} \pmod 4$ implies $\mathfrak{A} - \mathfrak{B} = (0)$.

THEOREM 5. *If* $\mathfrak{A}_1$ *and* $\mathfrak{B}_1$ *are improperly primitive equivalent matrices of odd determinant and*

$$\{\mathfrak{A}_1 , \mathfrak{A}_2\} \cong \{\mathfrak{B}_1 , \mathfrak{B}_2\},$$

then

$$\mathfrak{A}_2 \cong \mathfrak{B}_2$$

provided $v(\mathfrak{A}_2) = v(\mathfrak{B}_2) > 0$ *or* $\mathfrak{A}_2$ *and* $\mathfrak{B}_2$ *are both properly primitive or both improperly primitive.*

Proof. The hypothesis of our theorem implies $\{\mathfrak{A}_1 , a, \mathfrak{A}_2\} \cong \{\mathfrak{B}_1 , a, \mathfrak{B}_2\}$ for any unit a. Then Theorem 4 implies $\{a, \mathfrak{A}_2\} \cong \{a, \mathfrak{B}_2\}$ and the conditions of our theorem with Theorem 2 imply $\mathfrak{A}_2 \cong \mathfrak{B}_2$.

Our principal result is embodied in

THEOREM 6. *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are canonical matrices with*

$$\mathfrak{A} = \{2^{t_1}\mathfrak{A}_1 , 2^{t_2}\mathfrak{A}_2 , \cdots , 2^{t_n}\mathfrak{A}_n\} \cong \mathfrak{B} = \{2^{t_1}\mathfrak{B}_1 , \cdots , 2^{t_n}\mathfrak{B}_n\},$$

then $\mathfrak{A}_i = \mathfrak{B}_i$ *for* $i = 1, \cdots , n$.

Proof. By Theorem 3, $\mathfrak{A}_1 = \mathfrak{B}_1$ if $\mathfrak{A}_1$ or $\mathfrak{B}_1$ represents a unit and by Theorem 2 we have

$$\{2^{t_2}\mathfrak{A}_2 , \cdots , 2^{t_n}\mathfrak{A}_n\} \cong \{2^{t_2}\mathfrak{B}_2 , \cdots , 2^{t_n}\mathfrak{B}_n\},$$

where each matrix is canonical, and so we proceed. Suppose $\mathfrak{A}_i$ is improperly primitive for $i = 1, \cdots , k$ with $1 \leq k < n$ and $\mathfrak{A}_{k+1}$ is properly primitive. If $t_{k+1} = 1 + t_k$, Theorem 1 implies $\mathfrak{A}_k \cong \mathfrak{B}_k$ and Theorem 5 and Lemma 7 apply to show $\mathfrak{A}_i \cong \mathfrak{B}_i$ for $i \leq k$ and

$$\{2^{t_{k+1}}\mathfrak{A}_{k+1} , \cdots , 2^{t_n}\mathfrak{A}_n\} \cong \{2^{t_{k+1}}\mathfrak{B}_{k+1} , \cdots , 2^{t_n}\mathfrak{B}_n\}. \tag{14}$$

Now $\mathfrak{A}$ and $\mathfrak{B}$ canonical imply $\mathfrak{A}_i = \mathfrak{B}_i$ and the forms in (14) are canonical. Hence $\mathfrak{A}_{k+1} = \mathfrak{B}_{k+1}$ and we proceed with the proof.

Finally, if $\mathfrak{A}_1 , \cdots , \mathfrak{A}_n$ are improperly primitive, we have by the above process $\mathfrak{A}_n \cong \mathfrak{B}_n$. In fact, for this case we have the

COROLLARY. *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are of the forms above, where the* $\mathfrak{A}_i$ *and* $\mathfrak{B}_i$ *are not necessarily canonical but are all improperly primitive, then* $\mathfrak{A}_i \cong \mathfrak{B}_i$ *for all* i.

5. **Supplementary results.** It is easily shown along lines similar to the proof of Lemma 1 that, in any $R(p)$, a matrix is equivalent to

$$\{p^{t_1}\mathfrak{A}_1 , p^{t_2}\mathfrak{A}_2 , \cdots , p^{t_n}\mathfrak{A}_n\}, \tag{15}$$

where each $\mathfrak{A}_i$ has determinant prime to p and $t_i < t_{i+1}$ for $i = 1, \cdots, n-1$. Furthermore (see for example [6; Lemma 3]), if p is odd, each

$$\mathfrak{A}_i \cong \{1, 1, \cdots, 1, \mid \mathfrak{A}_i \mid\}. \tag{16}$$

This shows *that any two forms of equal determinants are equivalent in every $R(p)$ for which p is an odd prime not a divisor of the determinant.* Furthermore, since [3] in any $R(p)$, p odd, $\{\mathfrak{A}, \mathfrak{B}\} \cong \{\mathfrak{A}, \mathfrak{C}\}$ implies $\mathfrak{B} \cong \mathfrak{C}$, it may be seen that (15) is made a *unique canonical form* by replacing (16) by the condition

$$\mathfrak{A}_i = \{1, 1, \cdots, 1, q\}, \tag{17}$$

where q is 1 if $\mid \mathfrak{A}_i \mid$ is a quadratic residue of p and the least positive non-residue of p if $\mid \mathfrak{A}_i \mid$ is a non-residue of p.

Bibliography

1. W. H. Durfee, *Congruence of quadratic forms over valuation rings*, this Journal, vol. 11 (1944), pp. 687–697.
2. Helmut Hasse, *Ueber die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen*, Journal für Mathematik, vol. 152(1923), pp. 205–224.
3. B. W. Jones, *An extension of a theorem of Witt*, Bulletin of the American Mathematical Society, vol. 48(1942), pp. 133–142.
4. B. W. Jones, *Related genera of quadratic forms*, this Journal, vol. 9(1942), pp. 723–756.
5. H. Minkowski, *Gesammelte Abhandlungen*, I, Leipzig and Berlin, 1911.
6. C. L. Siegel, *Equivalence of quadratic forms*, American Journal of Mathematics, vol. 63 (1941), pp. 658–680.

Cornell University.