1-1-1980

A study of a positive definite quadratic form over the integers.

Dennis M. Warwick

A STUDY OF A POSITIVE DEFINITE QUADRATIC FORM OVER THE INTEGERS

by

Dennis M. Warwick

A Thesis

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Master of Science

in

Mathematics

Lehigh University

1980

CERTIFICATE OF APPROVAL

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science in Mathematics.

7/25/80
(date)

Professor in Charge

Chairman of the Department

ACKNOWLEDGEMENT

The author wishes to express his sincere appreciation to Professor Clifford S. Queen for his invaluable assistance during the preparation of this thesis. The author also wishes to thank Miss Judy Arroyo for her patience, understanding, and encouragement in typing the final manuscript.

TABLE OF CONTENTS

ABSTRACT

In an attempt to study the theory of both quadratic forms and ideal theory, one must be familiar with some elementary results on quadratic forms. The development of such results were originally illustrated by H. M. Stark in his paper "Values of L-Functions at s = 1". The necessity of familiarity with quadratic forms is emphasized by Stark in a rigorous treatment of such forms in the second section of his paper. Stark relies heavily upon notions of matrix algebra and the elementary algebra of quadratic forms.

This paper is an extension of Stark's ideas to include both the necessary background work and complete any gaps in the proofs provided. Thus the results and preliminary work should allow this treatment to be self-contained.

Chapters III and IV clearly examine the difference between equivalent matrices and equivalent quadratic forms. Thus the notion of equivalence must be viewed in the general scheme of mathematics.

INTRODUCTION

This paper is an extension of the elementary results on quadratic forms begun by Professor H. M. Stark. In order to fully understand and appreciate Stark's work, one should have a complete background of this material. Since Professor Stark begins his work dealing with the matrix algebra of the positive definite quadratic form, this is where our study should begin.

In the two background sections, I attempt to first develop and display the necessary machinery involving matrices, more distinctly 2-by-2 matrices. From there, I try to give a broad concept of the development of the quadratic forms through the use of matrix algebra. The notion of positive definiteness and the importance of the discriminant are introduced and explored. Hopefully the first two sections familiarize the reader with the concepts for his further understanding and appreciation of this paper.

The actual body of this paper occurs in sections III and IV where I study the notion of equivalence as it relates to both matrices and quadratic forms. Professor Stark proposes many relationships of equivalence, some of which can be verified through rigorous treatment of definitions, and others of which must rely upon the build-up of mathematical machinery. I attempt to fill in some of the gaps which develop in the proofs of such propositions, but in some cases I must rely entirely upon the work of Professor Stark.

A complete understanding of our elementary results on quadratic forms can lead to both a further study of quadratic forms and also the study of ideal theory.

I. MATRICES

A matrix is a rectangular array of real numbers. The real numbers that comprise a matrix are called the entries of the matrix. In general, we write a matrix A, with m rows and n columns and entries a_{ij}, in the form

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})$$

Such a matrix A is called an m-by-n matrix.

For our purposes, it will suffice to consider only 2-by-2 matrices. Let $k \in Z$ (integers) and

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} .$$

Addition is defined by

$$A + B = \begin{vmatrix} (a+e) & (b+f) \\ (c+g) & (d+h) \end{vmatrix}$$

and multiplication by

$$AB = \begin{vmatrix} (ae+bg) & (af+bh) \\ (ce+dg) & (ef+dh) \end{vmatrix} ; \; kA = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix} .$$

The transpose of A denoted by A^T is the matrix with the rows and columns interchanged:

$$A^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix} .$$

A matrix is said to be symmetric if and only if $A^T = A$.

A matrix is said to be antisymmetric if and only if $A^T = -A$.

A row matrix C is a 1-by-2 matrix: $C = (a\ b)$, and a column matrix D is a 2-by-1 matrix: $D = \begin{pmatrix} a \\ b \end{pmatrix}$.

A row matrix can only multiply a 2-by-2 matrix on the left with the result being a 1-by-2 matrix.

Ex. 1 $$(a \quad b) \begin{pmatrix} e & f \\ g & h \end{pmatrix} = ((ae+bg) \quad (af+bh)) .$$

A column matrix can only multiply a 2-by-2 matrix on the right with the result being a 2-by-1 matrix

Ex. 2 $$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{vmatrix} (ae+bf) \\ (ag+bh) \end{vmatrix} .$$

Define E as the identity matrix. Thus for

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

and any A, $AE = EA = A$.

Define the determinant of A as $\det(A) = ad-bc = |A|$. Thus for 2-by-2 matrices A, the inverse denoted

A^{-1} such that $AA^{-1} = E$ can be written as

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} .$$

PROOF. Observe that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

$$= \det(A) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

hence $AA^{-1} = E$, and

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} .$$

II. QUADRATIC FORMS, DISCRIMINANTS, POSITIVE DEFINITES

A quadratic polynomial is a polynomial of degree 2. Let

$$g(x) = ax^2 + bx + c, \quad a \neq 0,$$

be a quadratic polynomial with coefficients in the field of complex numbers. Then it is well-known that the polynomial $g(x)$ has roots r_1 and r_2 where

$$r_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}, \quad r_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}.$$

Every non-zero complex number has 2 square roots. Hence, r_1 and r_2 are complex numbers and it is easy to verify by direct calculation that

$$g(x) = a(x-r_1)(x-r_2).$$

It is customary to call b^2-4ac the discriminant of the quadratic polynomial $ax^2 + bx + c$. For convenience, let us designate this discriminant by D. It follows that $r_1 = r_2$ if and only if $D = 0$. $D = 0$ is a necessary and sufficient condition that the polynomial $g(x) = ax^2 + bx + c$ have a double root. If we assume that the quadratic polynomial $g(x)$ has real coefficients, r_1 and r_2 will also be real if and only if $D \geq 0$, for only in this case will D have real square roots.

An (n-ary) quadratic form over a field F is a polynomial f in n variables over F, which is homogeneous of degree 2. It has the general form

$$f(X_1,\ldots,X_n) = \sum_{i,j=1}^{n} a_{ij}X_iX_j \in F[X_1,\ldots,X_n] = F[X].$$

To render the coefficients symmetric, it is customary to rewrite f as

$$f(X) = \sum_{i,j} \tfrac{1}{2}(a_{ij}+a_{ji})X_iX_j = \sum_{i,j} a'_{ij}X_iX_j ,$$

where $a'_{ij} = \frac{1}{2}(a_{ij}+a_{ji})$. In this way, f determines uniquely a symmetric matrix (a'_{ij}), which we may denote by M_f. In terms of matrix notations, we have

$$f(X) = (X_1,\ldots,X_n)\cdot M_f\cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = X^T\cdot M_f\cdot X$$

with X viewed as a column vector.

The notion of congruence is of fundamental importance. Let

$$f = \sum_{i,j=1}^{n} a_{ij}X_iX_j \quad \text{and} \quad g = \sum_{i,j=1}^{n} b_{ij}Y_iY_j$$

be two quadratic forms with real coefficients and $a_{ij} = a_{ji}$, $b_{ij} = b_{ji}$ for all i and j. If there are real numbers t_{ij} such that, when the values of X given by

$$(*) \qquad X_i = \sum_{j=1}^{n} t_{ij}Y_j, \; i = 1,2,\dots,n$$

are substituted in f, the form g results, we say that the linear transformation (*) with real coefficients takes f into g. This transformation is called non-singular if (*) may be solved for Y_i. We call f and g congruent forms and write $f \simeq g$ if there is a non-singular linear transformation with real coefficients taking f into g.

Two congruent forms represent the same numbers since for any number N, a set of values of Y_i making $g = N$ will by (*) yield a set of values of X making $f = N$ and the transformation (obtained by solving (*) for Y_i) taking g into f, will take a solution of $f = N$ into one of $g = N$.

Since we are concerned with the numbers represented by the forms, out of a set of congruent forms only one need be considered just as in geometry. All equilateral triangles of unit side are the same as far as the properties we are interested in are concerned.

We define the matrix of a form to be the matrix A whose elements in order are a_{ij}, that is $A = (a_{ij})$, and the determinant of the form to be the determinant of A, which we denote by $\det(A) = |A|$. If we denote the row matrix $(X_1, X_2, \ldots, X_n)$ by X^T and the corresponding column matrix by X, matrix multiplication shows that we may write

$$f = X^T AX .$$

Then, since (*) may be written in matric notation in the form $X = TY$ where T is the matrix whose elements are t_{ij}, we recall that $X^T = Y^T T^T$ and see that the transformation (*) takes f into

$$g = Y^T T^T ATY = Y^T (T^T AT)Y$$

which shows that the matrix B is equal to $T^T AT$ with

$$g = Y^T BY.$$

For example, if f is of the form

$$2x_1^2 + x_1x_2 + 3x_2^2 ,$$

its matrix is

$$A = \begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & 3 \end{pmatrix}$$

and

$$f = (x_1, x_2) \begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} .$$

The transformation $x_1 = 3y_1 + y_2$, $x_2 = 2y_1 - y_2$ takes f into $g = 36y_1^2 - y_1y_2 + 4y_2^2$ since

$$\begin{pmatrix} 3 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 1/2 \\ 1/2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 36 & -1/2 \\ -1/2 & 4 \end{pmatrix} .$$

Notice that if (*) can be solved for Y_i we have in matric notation

$$Y = T^{-1}X \quad \text{and} \quad A = (T^T)^{-1}BT^{-1} .$$

A quadratic form which is positive for all real non-zero values of the variables is called a positive definite form. By changing the sign of every coefficient we obtain a negative definite form.

Example: x^2-xy+y^2 is positive definite
$-x^2+xy-y^2$ is negative definite.

A real symmetric matrix A is called positive definite, if it is the matrix of a positive quadratic form q. Since this form q in suitable coordinates is $q = X_1^2 + \ldots + X_n^2$, with matrix the identity matrix E, it follows that each positive definite A must be congruent to E, that is $A = P^T E P$.

Restated, a real symmetric matrix A is positive definite if and only if there exists a real invertible (transposable) matrix P with $A = P^T P$.

The quadratic forms are related to conic sections, for instance

$$x^2 + y^2 = 1 \quad \text{circle}$$
$$x^2 - y^2 = 1 \quad \text{equilateral hyperbola}$$
$$-x^2 - y^2 = 1 \quad \text{no locus.}$$

No we are ready to study specific quadratic forms.

III. EQUIVALENCE: MATRICES

In this section, we will look at one specific quadratic form, and from it obtain another form. We must use our knowledge of determinants and discriminants and also develop facts about equivalent matrices.

For real numbers a,b,c with $a > 0$ define

$$Q(x,y) = ax^2 + bxy + cy^2 = (x \quad y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

where the discriminant $d = b^2 - 4ac < 0$. For our purposes we will assume $d < -4$. We also assume that the discriminant is non-generative since we are not interested in the case when it is a square. Thus we are dealing with a positive definite form.

$$ax^2 + bxy + cy^2 = a[(x + \frac{b}{2a}y)^2 + (\frac{-b^2+4ac}{4a^2})y^2]$$

$$= a[x + \frac{b}{2a}y + (\sqrt{\frac{-b^2+4ac}{4a^2}})iy][x + \frac{b}{2a}y - (\sqrt{\frac{-b^2+4ac}{4a^2}})iy]$$

$$= a(x+\theta y)(x+\overline{\theta}y)$$

where

$$\theta = \frac{b}{2a} + \sqrt{\frac{-b^2+4ac}{4a^2}}(i)$$

Hence $Q(x,y) = a(x+\theta y)(x+\overline{\theta}y)$.

We will use $Q(x,y)$ of discriminant d and a new matrix M to define $Q_M(X,Y)$, a new form of a quadratic. Let

$$M = \begin{vmatrix} r_M & s_M \\ t_M & u_M \end{vmatrix}, \quad r_M, s_M, t_M, u_M \in Z$$

with determinant of $M = f > 0$. We will replace x,y in Q by

$$(y,x) = (Y,X)M.$$

Using a transformation

$$(x,y) = (t,w)\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$$

we see that

$$Q(t,w) = (t \quad w)\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix}\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}^T \begin{vmatrix} t \\ w \end{vmatrix}.$$

Hence $y = r_M Y + t_M X$ and $x = s_M Y + u_M X$.

What does $Q_M(X,Y)$ look like?

$$(y,x) = (Y,X)M$$

$$\begin{vmatrix} y \\ x \end{vmatrix} = M^T \begin{vmatrix} Y \\ X \end{vmatrix}$$

$$\begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} M^T \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \begin{vmatrix} X \\ Y \end{vmatrix}$$

(by interchanging x,y and using the symmetric matrix

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

we obtain the needed column matrix.) Hence,

$$Q_M(X,Y) = (X \quad Y) \left[\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} M^T \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}\right]^T \times$$

$$\times \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} \left[\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} M^T \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}\right] \begin{vmatrix} X \\ Y \end{vmatrix}.$$

The determinant of $Q(x,y)$ is $ac - \frac{b^2}{4} = \frac{4ac-b^2}{4} = -\frac{1}{4}d$. Thus -4 times the determinant equals the discriminant $d = b^2-4ac$. To obtain the discriminant of $Q_M(X,Y)$, first we must obtain the determinant. The determinant of $Q_M(X,Y)$ is the product of the determinants of its components.

$$\det \left[\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} M^T \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}\right]^T = \det \left[\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} M^T \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}\right]$$

$$= \det M = f$$

and the determinant of $Q(x,y)$ is $-\frac{1}{4}d$. Thus the determinant of $Q_M(X,Y) = (f)(-\frac{1}{4}d)(f) = -\frac{1}{4}f^2d$. If we multiply by -4 we obtain f^2d which is the discriminant of $Q_M(X,Y)$.

Since $Q(x,y) = a(x+\theta y)(x+\bar{\theta}y)$, then

$$Q_M(X,Y) = a(s_MY+u_MX+\theta[r_MY+t_MX]) \times$$
$$\times(s_MY+u_MX+\bar{\theta}[r_MY+t_MX]) .$$

Thus,

$$Q_M(X,Y) = a_MX^2 + b_MXY + c_MY^2$$
$$= a_M[X+\theta_MY][X+\bar{\theta}_MY]$$

with

$$a_M = a\ |u_M+t_M\theta|^2 > 0 \quad \text{because} \quad a > 0.$$

$$\theta_M = \frac{r_M\theta+s_M}{t_M\theta+u_M} = M\theta$$

(which is just the definition of multiplication on the right). It should be noted that

$$Q_{MN}(X,Y) = (Q_N)_M(X,Y).$$

Definition: Let us define Γ as

$$\Gamma = SL_2(Z) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in Z,\ \det = ad-bc = 1\right\} .$$

Definition: Given two quadratic forms Q and Q' of the same discriminant, Q is equivalent (congruent) to Q' ($Q \simeq Q'$) if there is an $A \in \Gamma$ so that $Q_A = Q'$.

Note that $Q_M \simeq Q_N$ if and only if $\det M = \det N = f$ and there is an $A \in \Gamma$ such that $AM = N$.

$$\begin{array}{c} (Q_M)_A = Q_N \\ \| \\ Q_{AM} \end{array}$$

These are equivalence classes of quadratic forms of $Q_M(X,Y)$.

All 2-by-2 matrices $M = \begin{vmatrix} r_M & s_M \\ t_M & u_M \end{vmatrix}$ with integer entries and $\det M = f > 0$ and $(r_M, s_M, t_M, u_M) = 1$ (relatively prime but not necessarily in pairs) form a set of matrices.

Definition. Let $S_1(f)$ be the above set of matrices.

Proposition 3.1 If $M \in S_1(f)$, then

$$M \simeq \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}, \text{ where } r > 0,\ u > 0,\ ru = f$$

and $0 \leq s < u$.

$$\begin{pmatrix} r & s \\ 0 & u \end{pmatrix} \in S_1(f), \text{ i.e. } (r,s,u) = 1.$$

Proof: Let

$$M = \begin{vmatrix} r_M & s_M \\ t_M & u_M \end{vmatrix} \text{ with } r_M \neq 0 .$$

If $r_M \neq 0$, then $t_M = r_M q + r$, $0 \leq r < r_M$. Multiply the top now by $-q$ and add it to the bottom.

$$\begin{vmatrix} r_M & s_M \\ t_M & u_M \end{vmatrix} \simeq \begin{vmatrix} r_M & s_M \\ r & [u_M - S_M q] \end{vmatrix} \simeq$$

$$\simeq \begin{vmatrix} r_M - r & [s_M - u_M + S_M q] \\ r & [u_M - s_M q] \end{vmatrix} \simeq \begin{vmatrix} r_M - r & [s_M - u_M + s_M q] \\ r_M & s_M \end{vmatrix}$$

Set $r_M = (r_M - r)q + r_1$ and keep repeating the process until the entry in the lower left corner is zero. Hence,

$$\simeq \begin{vmatrix} & \\ 0 & \end{vmatrix} .$$

Eventually this process will yield a matrix of the form $\begin{pmatrix} r & t \\ 0 & u \end{pmatrix}$. If we set $t = uq + s$, $0 \leq s < u$, this matrix by the same process is equivalent to $\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$. If r is negative then u is negative and we simply multiply $\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and obtain our desired result, since det $ru = f$ since $M \in S_1(f)$. //

Note. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an integer matrix and $(a,b,c,d) = g$ and $A \in \Gamma$, then if $A\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ then $(a',b',c',d') = g$. Let $A\begin{pmatrix} r & s \\ 0 & u \end{pmatrix} = \begin{pmatrix} r' & s' \\ 0 & u' \end{pmatrix}$ with $A \in \Gamma$, $ru = f$, $r > 0$, $u > 0$, $0 \leq s < u$ and $r'u' = f$, $r' > 0$, $u' > 0$, $0 \leq s' < u'$. $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $ad-bc = 1$. By multiplication of the two matrices on the left side of the equation, we obtain four equations.

$$ar = r' \tag{1}$$

$$as + bu = s' \tag{2}$$

$$cr = 0 \tag{3}$$

$$cs + du = u' \tag{4}$$

Equation (3) says $c = 0$ or $r = 0$, but since $r > 0$ that implies $c = 0$. Hence the equation $ad-bc = 1$ becomes $ad = 1$. Since $(a)(d)$ is the product of two positive primes by definition of Γ, then the only possibility is $a = d = 1$. Hence the four equations above now become

$$r = r' \tag{1'}$$

$$s + bu = s' \tag{2'}$$

$$u = u' \tag{3'}$$

Equation (2') becomes $s'-s = bu$. That implies u divides $(s'-s)$ written $u|(s'-s)$. But $s < u$ and $s' < u' = u$ so that the only possibility is for $s'-s = 0$ which means $s' = s$. Thus $bu = 0$ implies $b = 0$ and the matrix A is now $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hence $(r,s,u) = g$ implies $(r',s',u') = g$.

Let us look at the number of equivalence classes of matrices of $S_1(f)$ for different values of f. Recall $M \in S_1(f)$ implies $M = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$ with $ru = f$, $r > 0$, $u > 0$ and $0 \leq s < u$.

Example 1. Set $f = 5$. Thus $5 = 5 \cdot 1$ and $5 = 1 \cdot 5$.

$\left\{\begin{pmatrix} 1 & s \\ 0 & 5 \end{pmatrix} \middle| 0 \leq s < 5\right\}$ are 5 nonequivalent matrices.

$\left\{\begin{pmatrix} 5 & s \\ 0 & 1 \end{pmatrix} \middle| 0 \leq s < 1\right\}$ one matrix with $s = 0$. Hence there are 6 equivalence classes in $S_1(5)$.

Example 2. Set $f = 6$. Thus $6 = 2 \cdot 3 = 3 \cdot 2 = 1 \cdot 6 = 6 \cdot 1$

$\left\{\begin{pmatrix} 2 & s \\ 0 & 3 \end{pmatrix} \middle| 0 \leq s < 3\right\}$ are 3 nonequivalent matrices.

$\left\{\begin{pmatrix} 3 & s \\ 0 & 2 \end{pmatrix} \middle| 0 \leq s < 2\right\}$ are 2 nonequivalent matrices.

$\left\{\begin{pmatrix} 1 & s \\ 0 & 6 \end{pmatrix} \middle| 0 \leq s < 6\right\}$ are 6 nonequivalent matrices.

$\left\{\begin{pmatrix} 6 & s \\ 0 & 1 \end{pmatrix} \middle| 0 \leq s < 1\right\}$ one matrix with $s = 0$. Hence there are 12 equivalence classes in $S_1(6)$.

Example 3. Set $f = 4$. Thus $4 = 4\cdot 1 = 1\cdot 4 = 2\cdot 2$.

$\left\{\begin{pmatrix}4 & s\\ 0 & 1\end{pmatrix} \mid 0 \le s < 1\right\}$ one matrix with $s = 0$.

$\left\{\begin{pmatrix}1 & s\\ 0 & 4\end{pmatrix} \mid 0 \le s < 4\right\}$ are 4 nonequivalent matrices.

$\left\{\begin{pmatrix}2 & s\\ 0 & 2\end{pmatrix} \mid 0 \le s < 2\right\}$ one matrix with $s = 1$, since if $s = 0$, $(r,u) = 2$ which violates $(r,s,u) = 1$ for matrices which are elements of $S_1(f)$. Hence there are 6 equivalence classes in $S_1(4)$.

Definition. Let $|S_1(f)|$ denote the number of equivalence classes of matrices in $S_1(f)$.

Definition. Define $\phi(u)$ = the number of integers a so that $0 < a < |u|$ and $(a,u) = 1$. Set $\phi(1) = 1$. It is obvious for p = prime number that $\phi(p) = p-1$.

Fact. We can write down a formula for $|S_1(f)|$,

$$|S_1(f)| = \sum_{\substack{ru=f\\ r>0,\,u>0}} \frac{u}{(r,u)}\, \phi((r,u)).$$

Proof. Let $M = \begin{pmatrix}r & s\\ 0 & u\end{pmatrix}$. Hence $(r,u,s) = 1$ implies that $((r,u),s) = 1$. Also $0 \le s < u$. $\phi((r,u))$ = the number of integers λ such that $0 < \lambda < |(r,u)|$ and $(\lambda,(r,u)) = 1$. Hence $\lambda = s$ and it must be less than

(r,u), $\lambda < (r,u)$. Define $s = \lambda + a(r,u)$, $a < \frac{u}{(r,u)}$ since $s < u$. Thus $s = \lambda + a(r,u) < u$, but $\lambda < (r,u)$ hence

$$\begin{aligned} \lambda + a(r,u) &< u \\ (r,u) + a(r,u) &< u \\ (a+1)(r,u) &< u \\ a+1 &< \frac{u}{(r,u)} \\ a &< \frac{u}{(r,u)} - 1 . \end{aligned}$$

Thus $[\frac{u}{(r,u)}]$ are the number of elements for each $\lambda < |(r,u)|$ and $\phi((r,u))[\frac{u}{(r,u)}]$ are the number for each partition of f. Hence

$$\sum_{\substack{ru=f \\ r>0,u>0}} \frac{u}{(r,u)} \phi((r,u)) = |S_1(f)|. \qquad //$$

<u>Proposition 3.2</u>. If $B \in \Gamma$, $M \in S_1(f)$, then $MB \in S_1(f)$. Further if $N,M \in S_1(f)$, then there exists a $B \in \Gamma$ so that $M \simeq NB$, i.e., there exists $A \in \Gamma$ so that $M = ANB$.

<u>Proof</u>. $M = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$, $(r,s,u) = 1$. Suppose that $(r,s) = 1$, then there are integers x,y so that $rx + sy = 1$.

[If $(a,b) = g \Rightarrow g = ax + by$.

Proof. Define $S = \{ax+by \mid x,y \in Z\}$ and let $g > 0$ be the smallest positive integer so that $g = ax + by$. Let $c > 0$ so that $c|a$, $c|b \Rightarrow c|g$. Define $a = gq + r$ (assume $g \nmid a$), $0 < r < q$. $r = a-gq = a-(ax+by)q = a-axq-byq = a(1-xq)+byq$. But $a(1-xq)+byq$ is of the form $ax+by$. Since g was chosen to be the smallest a contradiction exists. Hence $g = ax+by \Rightarrow g|a$, $g|b$, i.e. $(a,b) = g$.] Define $B = \begin{pmatrix} s & x \\ -r & y \end{pmatrix}$ with $rx + sy = 1$ the determinant. Hence $B \in \Gamma$. Thus $\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}\begin{pmatrix} s & x \\ -r & y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -ru & uy \end{pmatrix}$. We can use the same type of operations as we did in the proof of Proposition 3.1 to find an equivalent matrix:

$$\begin{vmatrix} 0 & 1 \\ -ru & uy \end{vmatrix} \simeq \begin{vmatrix} 0 & 1 \\ -ru & 0 \end{vmatrix} \simeq \begin{vmatrix} ru & 1 \\ -ru & 0 \end{vmatrix} \simeq \begin{vmatrix} ru & 1 \\ 0 & 1 \end{vmatrix} \simeq \begin{vmatrix} ru & 0 \\ 0 & 1 \end{vmatrix}.$$

Hence,

$$\begin{vmatrix} r & s \\ 0 & u \end{vmatrix}\begin{vmatrix} s & x \\ -r & y \end{vmatrix} \simeq \begin{vmatrix} ru & 0 \\ 0 & 1 \end{vmatrix} = \begin{vmatrix} f & 0 \\ 0 & 1 \end{vmatrix}. \quad //$$

Proposition 3.3. If $M \in S_1(f)$, then for any $B \in \Gamma$, $MB \in S_1(f)$ and further there exists $A, B \in \Gamma$ such that

$$AMB = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof. Recall that if $A'M = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$, then with $(r,s) = 1$ it was shown that there exists A, B so that $AMB = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$. Define $CMD = \begin{pmatrix} r & s' \\ 0 & u \end{pmatrix}$, $(r,s') = 1$ and let

$$A'M = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix} \begin{array}{c} r > 0 \\ ,u > 0 \\ ru = f \end{array}, \quad 0 \leq s < u \ .$$

For our purposes, let $(r,s) = s_1$, and then set $r = r_1 s_1 s_2$, where $(r_1, s) = 1$ and if $p|s_i$ then $p|s$ for any prime p. Use the fact that $(p^2, p) = p$ so that $r = 1 \cdot p \cdot p = r_1 \cdot s_1 \cdot s_2$. With $(r_1, s_1) = 1$, we claim that there exists an integer k so that $k \equiv 0 (\text{mod } r_1)$ and $k \equiv 1 (\text{mod } s_1)$. Simply that $r_1 | k$ and $s_1 | k-1$. ((mod r_1) is just base r_1 in the number system. For example $r_1 = 0$ and any $nr_1 = 0$. So every number t can be factored as such $t = nr_1 + a$ with $0 \leq a < r_1$).

$$(r_1, s_1) = 1 \Rightarrow r_1 x + s_1 y = 1$$
$$r_1 x - 1 = -s_1 y$$

Now we apply the Chinese Remainder Theorem.

[Chinese Remainder Theorem: If $(m_i, m_j) = 1$ for $1 \leq i < j \leq r$, then the system below has as its complete solution a single residue class $(\text{mod } m_1 \ldots m_r)$:

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_r \pmod{m_r}.]$$

With the value of k above we obtain $(r, s+ku) = 1$ since $p|r$, $p|s$ implies $p \nmid u$ and $p \nmid k$ while $p|r$, $p \nmid s$ implies $p|k$. Hence, there are integers q and h such that $rh - (s+ku)g = 1$. Now,

$$A = \begin{pmatrix} -ug & sg-rh \\ 1 & k \end{pmatrix}, \quad B = \begin{pmatrix} s+ku & h \\ -r & -g \end{pmatrix}$$

are in Γ and

$$A\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}B = (rh-sg-kug)\begin{pmatrix} ru & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}. \quad // \ [7]$$

Proposition 3.4. Suppose $f = f_1 f_2$, $(f_1, f_2) = 1$. Then if $M \in S_1(f)$, there exist $M_1 \in S_1(f_1)$, $M_2 \in S_1(f_2)$ so that $M = M_1 M_2$. Further for any M, M_1 can be chosen in any equivalence class of $S_1(f_1)$. $[M = M_1 M_2 = (M_1 C^{-1})(CM_2)]$. Further, the class determined by M_2 in $S_1(f)$ is determined uniquely by M.

<u>Proof</u>: $AMB = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} f_1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} f_2 & 0 \\ 0 & 1 \end{pmatrix}$. Then

$$M = \underbrace{A^{-1}\begin{pmatrix} f_1 & 0 \\ 0 & 1 \end{pmatrix}}_{M_1} \quad \underbrace{\begin{pmatrix} f_2 & 0 \\ 0 & 1 \end{pmatrix}B^{-1}}_{M_2}$$

$[M_2 \simeq \begin{pmatrix} f_2 & 0 \\ 0 & 1 \end{pmatrix}B^{-1} \Rightarrow M_2B \simeq \begin{pmatrix} f_2 & 0 \\ 0 & 1 \end{pmatrix}]$. Let $DM = M_1M_2$.

We want to show that $M \simeq \begin{pmatrix} f_2 & 0 \\ 0 & 1 \end{pmatrix}B^{-1}$. Then $M = D^{-1}M_1M_2$.

Since $\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = AMB$,

$$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = A(D^{-1}M_1)M_2B .$$

But

$$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = A(D^{-1}M_1C^{-1})\begin{pmatrix} r & s \\ 0 & u \end{pmatrix} ,$$

where

$\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$ has $ru = f_2$, $r > 0$, $u > 0$, $0 \leq s < u$, $(r,s,u) = 1$. Thus

$$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$$

and as before we have four equations.

$$xr = f \tag{1}$$

$$xs + yu = 0 \tag{2}$$

$$zr = 0 \tag{3}$$

$$zs + wu = 1 \tag{4}$$

Equation (3) implies $z = 0$, which in turn causes equation (4) to become $wu = 1$, but w, u must be positive integers hence $w = u = 1$. Thus the equations reduce to

$$xr = f \tag{1'}$$

$$xs + y = 0 \tag{2'}$$

$$w = u = 1 \tag{3'}$$

Thus

$$\begin{pmatrix} r & s \\ 0 & u \end{pmatrix} = \begin{pmatrix} f_2 & 0 \\ 0 & 1 \end{pmatrix}, \text{ since } ru = f_2. \qquad //$$

<u>Proposition 3.5</u>. If $f = f_1 f_2$, $(f_1, f_2) = 1$ then $|S_1(f)| = |S_1(f_1)| \cdot |S_1(f_2)|$. Further, if M_i, $1 \leq i \leq |S_1(f_1)|$ is a set of complete representatives of the classes of $S_1(f_1)$, and let N_j, $1 \leq j \leq |S_1(f_2)|$ be a set of complete representatives of the classes of $S_1(f_2)$, then

$$M_i N_j, \ 1 \leq i \leq |S_1(f_1)|, \ 1 \leq j \leq |S_1(f_2)|$$

is a complete set of representatives of the classes of

$S_1(f)$. In particular, $|S_1(f)|$ is a multiplicative function of f and

$$|S_1(f)| = f \prod_{i=1}^{r} (1+p_i^{-1}).$$

Proof: If $\begin{pmatrix} r & s \\ 0 & u \end{pmatrix} = \begin{pmatrix} r_1 & s_1 \\ 0 & u_2 \end{pmatrix}\begin{pmatrix} r_2 & s_2 \\ 0 & u_2 \end{pmatrix}$ with $(r_1, s_1, u_1) = (r_2, s_2, u_2) = 1$, $r_1 u_1 = f_1$, $r_2 u_2 = f_2$, then $(r,s,u) = 1$ also. Thus the matrices $M_i N_j$ are all in $S_1(f)$. Further, by Proposition 3.4, every matrix of $S_1(f)$ is equivalent to one of the $M_i N_j$ and hence it remains to show that the $M_i N_j$ are inequivalent. If

$$M_i N_j = A M_{i'} N_{j'} \quad \text{with} \quad A \in \Gamma,$$

then by Proposition 3.4, N_j is equivalent to $N_{j'}$, and hence they are equal by their definition. Therefore,

$$M_i = A M_{i'}$$

and thus $M_i = M_{i'}$ and the $M_i N_j$ are inequivalent.

Hence, $|S_1(f)|$ is multiplicative. By using the class representatives given by Fact (pg 21), we see that

$$|S_1(f)| = \sum_{ru=f} \frac{u}{(r,u)} \phi((r,u)) .$$

If in particular $f = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, for p a prime power, then

$$|S_1(f)| = |S_1(p^\alpha)| = \begin{cases} 1 & \alpha = 0 \\ p+1 & \alpha = 1 \\ p^\alpha + p^{\alpha-1}(1-p^{-1}) + \ldots + p(1-p^{-1}) + 1 & \alpha > 1 \end{cases}$$

$[|S_1(p^\alpha)| = p^\alpha(1+p^{-1})$ $\alpha \geq 1$ by induction]. Thus

$$|S_1(f)| = \prod_{i=1}^{r} |S_1(p_i^{\alpha_i})| = \prod_{i=1}^{r} p_i^{\alpha_i}(1+p_i^{-1})$$

$$= \prod_{i=1}^{r} f(1+p_i^{-1}) = f \prod_{i=1}^{r} (1+p_i^{-1}). \quad // \; [7]$$

<u>Proposition 3.6.</u> Suppose that $(m,n,f) = 1$ with $f > 0$ and m,n integers, then there is a unique class of matrices M so that $M \in S_1(f)$ and the equation

$$(n,m) = (Y,X)M$$

has integer solutions (Y,X).

<u>Proof</u>. Let $(n,m,f) = 1$. Thus if $(n,m) = g$ then $(g,f) = 1$. Thus we have

$$nw - mz = gf \tag{1}$$

and

$$nx - my = g \tag{2}$$

Multiplying (2) by f, we obtain $nxf - myf = gf$. Hence if we have one solution, we can find all other solutions.

$$\begin{array}{r} nw_1 - mz_1 = gf \\ -\quad nw - mz = gf \\ \hline n(w_1-w) - m(z_1-z) = 0 \end{array}$$

Our claim is that for w,z in equation (1) we have

$$w = w_1 + \frac{tm}{g} \; ; \; z = z_1 + \frac{tn}{g} \quad ,$$

to obtain all possible solutions. [We have $nx-my = 0$. One solution is $n(m) + m(-n) = 0$. For t an integer, we have $ntm + m(-tn) = 0$. Hence we have $n(\frac{tm}{g}) + m(\frac{-tn}{g}) = 0$. Thus our claim follows for equation (2), $nx-my = g$.] Thus we have

$$\begin{pmatrix} n & m \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ t/g & 1 \end{pmatrix} \begin{pmatrix} n & m \\ z_1 & w_1 \end{pmatrix}$$

which has determinant gf, then is in $S_1(gf)$. By Proposition 3.4, we have

$$\begin{pmatrix} n & m \\ z_1 & w_1 \end{pmatrix} = M_1M_2$$

where $M_1 \in S_1(g)$ and $M_2 \in S_1(f)$, $nw_1-mz_1 = gf$.

The class of M_2 is determined uniquely by the class of $\begin{pmatrix} n & m \\ z_1 & w_1 \end{pmatrix}$, so M_2 fulfills $(n,m) = (Y,X)M_2$.

We now have matrices that obey $(n,m) = (Y,X)M$, so that M is equivalent to M_2.

Since $(n,m) = g$, then $(Y,X) = g$. Now we can find $u,v \in Z$ such that $uY - Xv = g$.

$$\begin{pmatrix} n & m \\ z & w \end{pmatrix} = \underset{\det = g}{\begin{pmatrix} Y & X \\ v & u \end{pmatrix}} \underset{\det = f}{M}$$

Thus $\det\begin{pmatrix} n & m \\ z & w \end{pmatrix} = nw - nz = gf$. Hence

$$\begin{pmatrix} n & m \\ z_1 & w_1 \end{pmatrix} = \left[\begin{pmatrix} 1 & 0 \\ -t/g & 1 \end{pmatrix}\begin{pmatrix} Y & X \\ v & u \end{pmatrix}\right]M .$$

Since $(Y,X) = g$, the matrix in brakets is a matrix of integers of determinant g and by Proposition 3.4, M_2 and M are equivalent. // [7]

IV. EQUIVALENCE: QUADRATIC FORMS

In the previous section, we investigated various types of equivalence of matrices. The point was to aid us in determining under what conditions different quadratic forms are also equivalent. The matrix M used primarily throughout the last section is a key in our determination.

Definition: A polynomial Q is primitive if the greatest common divisor of its coefficients is 1. A matrix M is primitive if the greatest common divisor of its entries is 1.

We will make use of the following Proposition to answer two questions which naturally arise from the preceding section.

Proposition 4.1. Let $Q_1(x_1,y_1) = a_1x_1^2+bx_1y_1+cy_1^2$ and $Q_2(x_2,y_2) = a_2x_2^2 + b_2x_2y_2 + c_2y_2^2$ are positive definite parabolic forms when $a_1 > 0$, $a_2 > 0$ and $b_1^2-4a_1c_1 = b_2^2 -4a_2c_2$. Recall: $Q(x,y) = ax^2 + bxy + cy^2 = a|x+\theta y|^2 = a(x+\theta y)(x+\bar{\theta}y)$ where

$$\theta = \frac{-b+\sqrt{b^2-4ac}}{2a} .$$

$$(y,x) = (Y,X)M \Rightarrow M = \begin{pmatrix} r_M & s_M \\ t_M & u_M \end{pmatrix}, \ \det M = f.$$

$$\begin{aligned} Q_M(X,Y) &= a_M X^2 + b_M XY + c_M Y^2 \\ &= a_M |X+\theta_M Y|^2 \end{aligned}$$

where

$$a_M = a|t_M\theta+u_M|^2 .$$

$$\theta_M = M\theta = \frac{r_M\theta+s_M}{t_M\theta+u_M} .$$

$Q_1(x_1,y_1) \simeq Q_2(x_2,y_2)$ if and only if $\theta_1 \simeq \theta_2$, (i.e. there exists $A \in \Gamma$ so that $A\theta_1 = \theta_2$).

<u>Proof</u>: Let $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ and recall $A\alpha = \frac{r\alpha+s}{t\alpha+u}$. Thus $(y_2,x_2) = (y_1,x_1)A$ if $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$. Assume $Q_1 \simeq Q_2$. Let

$$\begin{aligned} Q_1(x_1,y_1) &= Q_2(sy_1+ux_1, ry_1+tx_1) \\ &= a_2|(sy_1+ux_1)+(ry_1+tx_1)\theta_2|^2 \\ &= a_2|t\theta_2+u|^2 \cdot |x_1 + \frac{r\theta_2+s}{t\theta_2+u} y_1|^2 , \end{aligned}$$

but $\frac{r\theta_2+s}{t\theta_2+u} = A(\theta_2)$. Hence

$$Q_1(x_1,y_1) = a_2|t\theta_2+u|^2 \cdot |x_1+A(\theta_2)y_1|^2$$

since

$$(x_1,y_1) = a_1|x_1+\theta_1 y_1|^2 \quad \text{and} \quad \det A > 0,$$

$$\theta_1 = A\theta_2 .$$

Now assume $\theta_1 = A\theta_2$, then with A as above

$$A\theta_2 = \frac{r\theta_2+s}{t\theta_2+u} = \theta_1 .$$

Now $(y_2,x_2) = (y_1,x_1)A$ transforms

$$Q_2(x_2,y_2) = a_2|t\theta_2+u|^2 \cdot |x_1+A\theta_2 y_1|^2$$

$$= a_2|t\theta_2+u|^2|x_1+\theta y_1|^2$$

$$= a_2|t\theta_2+u|a_1^{-1}(Q_1(x_1,y_1)).$$

Since $a_2|t\theta_2+u|^2 a_1^{-1}$ is positive and Q_1 and Q_2 have the same discriminant, $a_2|t\theta_2+u|^2 a_1^{-1} = 1$. Hence $Q_2(x_2,y_2)$ transforms to $Q_1(x_1,y_1)$. // [7]

Question #1. If Q is primitive and M is primitive with $\det M = f > 0$, is $Q_M(X,Y)$ primitive?

Let $Q(x,y) = 8x^2 + 113xy + 400y^2$ (primitive form)

$$d = -31, \; f = 8 .$$

Define

$$M = \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix} \quad ; \quad N = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix} .$$

$Q(x,y) = 8|x+\theta y|^2$ where $\theta\bar{\theta} = \frac{400}{8}$. Hence

$$\begin{aligned} \theta_M(X,Y) &= 8|X+8\theta Y|^2 \\ &= 8(X^2-113XY+8\cdot 400Y^2), \end{aligned}$$

$[a_M = 8|1| = 8,\ \theta_M = 8\theta/1 = 8\theta]$ and Q_M is not primitive because every coefficient is divisible by 8.

Question #2. If Q is a quadratic form and $M, N \in S_1(f)$ and $Q_M \simeq Q_N$, is it true that $M \simeq N$? Use the above conditions and define $A = \begin{pmatrix} 49 & -50 \\ 1 & -1 \end{pmatrix}$. M and N are inequivalent by analysis of $S_1(8)$ similar to that done for $S_1(4)$, $S_1(5)$, and $S_1(6)$. With the A given as above, Q_N is transformed to Q_M by

$$Q_{AN} = (Q_N)_A = Q_M.$$

Hence it is not true that under the conditions given that N must be equivalent to M.

Proposition 4.2. If M, N are matrices with integer entries of determinant $f > 0$ and one of Q_M or Q_N

is primitive, then $Q_M \simeq Q_N$ if and only if $M \simeq N$. (Assume discriminant $d < -4$).

Proof. Assume that $Q_M \simeq Q_N$ and that one of them is primitive. Therefore both are primitive.

[Q primitive $\Rightarrow Q_A$ primitive. Let

$$Q(x,y) = ax^2 + bxy + cy^2 \qquad \text{(primitive)}$$
$$2Q(x,y) = 2ax^2 + 2bxy + 2cy^2 .$$

Thus $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ is the integer matrix for $2Q(x,y)$.

Using the fact that $(2Q)_A = 2\cdot Q_A$ and

$$(y,x) = (Y,X)A$$
$$(x,y)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (X,Y)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}A$$
$$(x,y) = (X,Y)\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}A\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right],$$

call the matrix in the brakets B. Thus

$$(2Q)_A = 2\cdot Q_A(X,Y) = (X,Y)\left[B\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}B^T\right]\begin{pmatrix} X \\ Y \end{pmatrix}$$

The greatest common divisor of the above matrix in brackets is just the greatest common divisor of the integer matrix. The greatest common divisor = $\begin{cases} 2 & \text{if } b \text{ is even} \\ 1 & \text{if } b \text{ is odd} \end{cases}$. Hence we have $2(a_AX^2+b_AXY+c_AY^2)$

whose product matrix is $\begin{pmatrix} 2a_A & b_A \\ b_A & 2c_A \end{pmatrix}$. Thus $Q \simeq Q_A$ implies Q_A primitive.] Since both Q_M and Q_N are primitive, then $\theta_M = M\theta$, $\theta_N = N\theta$, and by Proposition 4.1, θ_M and θ_N are equivalent under Γ. Thus there exists a matrix A in Γ such that

$$\theta_M = A\theta_N$$

$$\theta_M = AN\theta, \text{ but } \theta = M^{-1}\theta_M$$

hence
$$\theta_M = [ANM^{-1}]\theta_M$$

and $[ANM^{-1}]$ has rational entries with

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} , \quad M^{-1} = \frac{1}{f} \begin{pmatrix} u & -s \\ -t & r \end{pmatrix} .$$

Thus $\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix} [ANM^{-1}]\theta_M = \theta_M$, and

$$fANM^{-1} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

with $ru - ts = f^2$ and

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}\theta_M = \theta_M .$$

Hence

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}\theta_M = \frac{r\theta_M+s}{t\theta_M+u} = \theta_M$$

$$r\theta_M+S = t\theta_M^2 + u\theta_M$$

$$t\theta_M^2 + (u-r)\theta_M-S = 0$$

which is in the form

$$tX^2 + (u-r)X - s = 0.$$

so for $t \neq 0$,

$$\theta_M = \frac{r-u \pm \sqrt{(u-r)^2+4ts}}{2t}$$

and the discriminant of the polynomial is

$$\begin{aligned}(u-r)^2 + 4ts &= u^2 - 2ru + r^2 + 4ts \\ &= u^2 + 2ru + r^2 + 4(ts-ur) \\ \text{(discriminant)} &= (u+r)^2 - 4f^2 .\end{aligned}$$

But $Q_M(X,Y)$ is a primitive form

$$\begin{aligned}Q_M(X,Y) &= a_M X^2 + b_M XY + c_M Y^2 \\ &= a_M(X+\theta_M Y)(X+\overline{\theta}_M Y).\end{aligned}$$

If

$$\begin{aligned}f(x) = Q_M(X,-1) &= a_M X^2 - b_M X + c_M \\ &= a_M(X-\theta_M)(X+\overline{\theta}_M),\end{aligned}$$

where the two roots are θ_M, $\overline{\theta}_M$, define

$$g(x) = tX^2 + (u-r)X - S = t(X+\theta_M)(X-\overline{\theta}_M) .$$

Thus

$$\frac{g(x)}{f(x)} = \frac{t}{a_M} .$$

If $t = a_M$ then $g/f = 1$. Otherwise $t = \lambda a_M$ (where λ divides all factors of g.) Thus the discriminant of $g(x)$ must be less than or equal to the discriminant of $f(x) = Q_M(X,-1)$, hence discriminant is df^2. So

$$(u+r)^2 - 4f^2 \leq df^2$$

$$d \geq \left(\frac{u+r}{f}\right)^2 - 4$$

but this is impossible under the assumption $d < -4$. Therefore $t = 0$. Since θ_M is irrational $s = 0$, and $r = u$, and

$$fANM^{-1} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

but $r \cdot r = f^2$ implies $r = \pm f$, therefore

$$fANM^{-1} = \pm \begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix}$$

$$ANM^{-1} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$AN = \pm M$$

$$(\pm A)N = M$$

hence

$$N \simeq M. \quad //$$

Notice. If $Q(x,y) = ax^2 + bxy + cy^2$ is primitive and $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, $\det M = f$ and suppose that Q_M is not primitive, then we have

$$(y,x) = (Y,X)M$$

$$(y,x)\, M^{-1} = (Y,X)$$

$$(y,x)\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix} = (Y,X)M\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix}$$

[given the fact that $M\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix}M$.]

$$(y,x)\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix} = (fY, fX)M$$

$$(y,x)\left[\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix}M^{-1}\right] = (fY, fX)$$

(where the matrix in the brackets has integer entries). Therefore

$$Q(fX, fY) = Q_M(x,y) = gQ_{M'}(x,y)$$

where $Q_{M'}$ is primitive, but

$$Q(fX, fY) = f^2Q(X,Y)\ .$$

Thus

$$f^2Q(X,Y) = gQ_{M'}(x,y)$$

so

$$g \mid f^2\ .$$

Definition. Let $S(f,Q)$ denote those matrices M of determinant f such that Q_M is primitive.

$S(f,Q)$ contains several complete equivalence classes of matrices. Let $|S(f,Q)|$ denote the number of equivalence classes of such matrices M. It is obvious that $S_1(f) \geq S(f,Q)$. Question #1 provides an example where $|S_1(f)| > |S(f,Q)|$. It further shows that $S(f,Q)$ depends on Q since $\begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}$ is in $S(8,Q')$, where $Q'(x,y) = x^2 + xy + 8y^2$ is equivalent to Q.

Proposition 4.3. The value of $|S(f,Q)|$ depends upon f and d and in fact

$$|S(f,Q)| = f \prod_{p|f} (1-(\tfrac{d}{p})p^{-1}).$$

Proof. If $Q(x,y) = ax^2 + bxy + cy^2$ is a primitive form, first consider the case that f is a prime power, $f = p^n$. Proposition 3.1 will allow us to consider Q_M with M in one of the three forms:

(i) $M = \begin{pmatrix} 1 & s \\ 0 & p^n \end{pmatrix}$, $0 \leq s < p^n$,

(ii) $M = \begin{pmatrix} p^j & s \\ 0 & p^k \end{pmatrix}$, $0 \leq s < p^k$, $j+k = n$, $0 < j < n$,

(iii) $M = \begin{pmatrix} p^n & 0 \\ 0 & 1 \end{pmatrix}$.

Since Q is primitive, Q_M will be primitive if and only if $p \nmid (a_M, b_M, c_M)$. Thus, it suffices to examine $Q_M \pmod p$.

(i') $(y,x) \equiv (Y,X)\begin{pmatrix} 1 & s \\ 0 & 0 \end{pmatrix} \equiv (Y, SY)$

$$\begin{aligned} Q_M(X,Y) &\equiv Q(SY,Y) \\ &\equiv as^2Y^2 + bsY^2 + cY^2 \\ &\equiv (as^2+bs+c)Y^2 \pmod p. \end{aligned}$$

(ii') $(y,x) \equiv (Y,X)\begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} \equiv (0, SY)$

$$\begin{aligned} Q_M(X,Y) &\equiv Q(SY,0) \\ &\equiv as^2Y^2 \pmod p. \end{aligned}$$

(iii') $(y,x) \equiv (Y,X)\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \equiv (0,X)$

$$\begin{aligned} Q_M(X,Y) &\equiv Q(X,0) \\ &\equiv ax^2 \pmod p. \end{aligned}$$

From (i'), (ii'), (iii') and the conditions on s, if $p \nmid a$, then

$$|S(p^n,Q)| = p^{n-1}(p-1-(\tfrac{d}{p})) + \sum_{k=1}^{n-1} p^{k-1}(p-1) + 1$$
$$= p^n(1-(\tfrac{d}{p}))p^{-1}),$$

while if $p|a$ so that $(\frac{d}{p}) = (\frac{b^2}{p}) = 1$ if $p \nmid b$ and $(\frac{d}{p}) = (\frac{b^2}{p}) = 0$ if $p|b$. It is apparent that $p|b$ if and only if $p|d$ and then $p \nmid c$. Thus

$$|S(p^n,Q)| = p^{n-1}(p-(\tfrac{d}{p})) + 0 + 0 = p^n(1-(\tfrac{d}{p})p^{-1}),$$

and the Proposition is proven for $f = p^n$. It should be noted that

$$(\tfrac{d}{p}) = \begin{cases} 0 & \text{if } p|d \\ 1 & \text{if } d \text{ is a square (mod p)} \\ -1 & \text{if } d \text{ is not a square (mod p).} \end{cases}$$

The proof for the Proposition can be completed as follows. Since it is true for prime powers, it will suffice to show that if it is true for f_1 and f_2 with $(f_1,f_2) = 1$, then it will be true for $f = f_1f_2$. From Proposition 3.4, if M_i, $1 \leq i \leq |S_1(f_1)|$, and N_j, $1 \leq j \leq |S_1(f_2)|$ give a complete set of representatives of $S_1(f_1)$ and $S_1(f_2)$ respectively, then M_iN_j give a complete set of representatives of $S_1(f)$.

Clearly $Q_{M_i N_j}$ is primitive if and only if first Q_{N_j} is primitive and then $(Q_{N_j})_{M_i}$ is primitive. By hypothesis, exactly

$$f_2 \prod_{p|f_2} (1-(\frac{d}{p})p^{-1})$$

of the Q_{N_j} are primitive, and for a fixed primitive Q_{N_j}, exactly

$$f_1 \prod_{p|f_1} (1-(\frac{df_2^2}{p})p^{-1})$$

of the $(Q_{N_j})_{M_i}$ are primitive. Hence, exactly

$$f_2 \prod_{p|f_2} (1-(\frac{d}{p})p^{-1}) \cdot f_1 \prod_{p|f_1} (1-(\frac{df_2^2}{p})p^{-1}) = f \prod_{p|f} (1-(\frac{d}{p})p^{-1})$$

of the $Q_{M_i N_j}$ are primitive and hence the Proposition is satisfied. // [7]

Proposition 4.4. If $Q(x,y)$ is a primitive form of a quadratic and n is a given positive integer then there exists a form

$$Q'(x,y) = a'x^2 + b'xy + c'y^2$$

equivalent to Q such that $(a',n) = 1$. Furthermore if $n^2|d$ and $\frac{d}{n^2}$ is a discriminant, then $Q'(x,y)$ may be chosen so that $n|b'$ and $n^2|c'$.

Proof. From Proposition 4.3, $|S(n,Q)| > 0$. Therefore there exists a matrix $M \in S_1(n)$ such that $Q_M(X,Y)$ is primitive. From Propositions 3.1 and 3.2, there exist $A, B \in \Gamma$ such that

$$AMB = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} .$$

Then $Q' = Q_{B^{-1}}$. Note that

$$Q'_{AMB} = Q_{AMBB^{-1}} = Q_{AM} = (Q_M)_A$$

is equivalent to Q_M and hence is primitive. But

$$(y,x) = (Y,X)\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = (nY,X).$$

Hence

$$Q'_{AMB}(X,nY) = a'X^2 + b'nXY + c'n^2Y^2$$

and thus $(a',n) = 1$:

Now if $n^2|d$ and d/n^2 is a discriminant, then $2|n$ implies $2|b'$ and hence, there is an integer t such that

$$b'+2a't \equiv \begin{cases} 0 \pmod{n} & \text{if } n \text{ is odd} \\ 0 \pmod{2n} & \text{if } n \text{ is even, } \frac{d}{n^2} \equiv 0 \pmod{4} \\ n \pmod{2n} & \text{if } n \text{ is even, } \frac{d}{n^2} \equiv 1 \pmod{4}. \end{cases}$$

If we let $Q''(x,y) = Q'(x+ty,y)$, we have

$$
\begin{aligned}
Q'(x+ty,y) &= a'(x+ty)^2 + b'(x+ty)y + c'(y)^2 \\
&= a'x^2 + 2a'txy + a't^2y^2 \\
&\quad + b'xy + b'ty^2 + c'y^2 \\
&= a'x^2 + (2a't+b')xy + (a't^2+b't+c')y^2
\end{aligned}
$$

let $a' = a''$, $b'' = 2a't + b'$, $c'' = a't^2 + b't + c'$. Thus

$$Q'(x+ty,y) = Q''(x,y) = a''x^2 + b''xy + c''y^2 .$$

Now Q'' is equivalent to Q' which implies it is equivalent to $\bar{Q}$. Note that $a'' = a'$ so that $(a'',n) = 1$ and $n|b'' = b' + 2a't$. Finally

$$
\begin{aligned}
(b'')^2-4a''c'' &= d \\
\frac{(b'')^2-4a''c''}{n^2} &= \frac{d}{n^2} \\
\frac{4a''c''}{n^2} &= \left(\frac{b''}{n}\right)^2 - \frac{d}{n^2} .
\end{aligned}
$$

If n is odd, $n^2|c''$, while if n is even, we have

$$\frac{4a''c''}{n^2} \equiv 0 \pmod 4$$

hence again $n^2|c''$. //

We now arrive at our fifth Proposition involving equivalence of various forms of the quadratic.

Proposition 4.5. Suppose Q' is a primitive form of discriminant df^2. Then there exists a primitive form Q of discriminant d and a matrix $M \in S(f,Q)$ such that $Q_M = Q'$. Further, if $Q^{(1)}$ has discriminant d and N has determinant f and $Q_N^{(1)}$ is equivalent to Q_M, then $Q^{(1)}$ is equivalent to Q.

Proof. From Proposition 4.4, there is an $A \in \Gamma$ so that Q_A' has the form

$$Q_A'(X,Y) = aX^2 + bfXY + cf^2Y^2, \quad (n=f). \qquad (*)$$

Let

$$Q(x,y) = ax^2 + bxy + cy^2 .$$

Then with

$$F = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}, \quad M = A^{-1}F$$

satisfies the first part of the Proposition since

$$Q_M = Q_{A^{-1}F} = (Q_F)_{A^{-1}} = (Q'_A)_{A^{-1}} = Q' ,$$

i.e.

$$(y,x) = (Y,X)\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = (fY,X)$$

$$Q_M(X,Y) = aX^2 + bfXY + cf^2Y^2$$

$$= Q'(X,Y).$$

In the second part of the Proposition, we are given a form $Q^{(1)}$ of discriminant d, a matrix N of determinant f, and a matrix B in Γ such that

$$Q_N^{(1)} = (Q_M)_B = Q_{BM}$$

and we want to show that $Q^{(1)}$ is equivalent to Q. We note that

$$Q = (Q_{BM})_{(BM)^{-1}} = (Q_N^{(1)})_{M^{-1}B^{-1}} = Q^{(1)}_{M^{-1}B^{-1}N} .$$

Further, $M^{-1}B^{-1}N$ has determinant 1, and thus, it suffices to show that $M^{-1}B^{-1}N$ is a matrix of integers. Since $Q_N^{(1)}$ is equivalent to Q', $Q_N^{(1)}$ is primitive, and, thus, $Q^{(1)}$ is primitive and N is in $S(f,Q^{(1)}) \subset S_1(f)$. Therefore by Propositions 3.1 and 3.2, there are matrices C and D in Γ such that

$$N = CFD.$$

Thus

$$M^{-1}B^{-1}N = M^{-1}B^{-1}CFD,$$

but

$$M = A^{-1}F$$

so

$$M^{-1} = F^{-1}A \quad .$$

Therefore

$$M^{-1}B^{-1}N = F^{-1}AB^{-1}CFD \quad .$$

Let

$$AB^{-1}C = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \quad .$$

We will show that $f \mid s$. Once this is accomplished,

$$F^{-1}AB^{-1}CF = \begin{pmatrix} r & s/f \\ tf & u \end{pmatrix}$$

will already have integral coefficients and we will be done.

Set

$$Q_D^{(1)}(x,y) = a^{(1)}x^2 + b^{(1)}xy + c^{(1)}y^2 \quad ,$$

so that

$$(Q_D^{(1)})_F(X,Y) = a^{(1)}X^2 + b^{(1)}fXY + c^{(1)}f^2Y^2. \qquad (**)$$

Now

$$[(Q_D^{(1)})_F]_{\begin{pmatrix} r & s \\ t & u \end{pmatrix}}$$

can be determined.

$$(y,x) = (Y,X) \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

$$= (rY+tX, sY+uX).$$

Hence

$$[(Q_D^{(1)})_F]_{\begin{pmatrix} r & s \\ t & u \end{pmatrix}} = (Q_D^{(1)})_F(SY+uX, rY+tX)$$

$$= a^{(1)}(uX+sY)^2 + b^{(1)}f(uX+sY)(tX+rY)$$

$$+ c^{(1)}f^2(tX+rY)^2 \qquad (***)$$

But

$$[(Q_D^{(1)})_F]_{\begin{pmatrix} r & s \\ t & u \end{pmatrix}} = (Q_D^{(1)})_{AB^{-1}CF}$$

$$= Q^{(1)}_{AB^{-1}CFD}$$

$$= Q^{(1)}_{AB^{-1}N}$$

$$= (Q_N^{(1)})_{AB^{-1}}$$

$$= (Q_B')_{AB^{-1}}$$

$$= [(Q_B')_{B^{-1}}]_A$$

$$= Q_A' .$$

and thus from (*), (**), (***) we see that

$$a^{(1)}(uX+sY)^2 + b^{(1)}f(uX+sY)(tX+rY) + c^{(1)}f^2(tX+rY)^2$$
$$= aX^2 + bfXY + cf^2Y^2.$$

The equation becomes

$$[a^{(1)}u^2+b^{(1)}fut+c^{(1)}f^2t^2]X^2$$
$$+ [a^{(1)}2us+b^{(1)}f(ur+st)+c^{(1)}f^2(2rt)]XY$$
$$+ [a^{(1)}s^2+b^{(1)}frs + c^{(1)}f^2r^2]Y^2$$
$$= aX^2 + bfXY + cf^2Y^2 .$$

Equating the coefficients of X^2 and XY on both sides yields

$$a^{(1)}u^2 + b^{(1)}fut + c^{(1)}f^2t^2 = a$$
(1) $$a^{(1)}u^2 \equiv a \pmod{f}$$
$$a^{(1)}2us + b^{(1)}f(ur+st) + c^{(1)}f^2(2rt) = bf$$
(2) $$a^{(1)}2us \equiv 0 \pmod{f}.$$

Since Q_A' is primitive, $(a,f) = 1$, and thus from (1), (2) above $(u,f) = 1$ and $(a^{(1)},f) = 1$. Hence, if f is odd, then $f|s$.

However, if f is even, then the coefficients of XY on both sides give

$$2a^{(1)}us + b^{(1)}f(ur+st) \equiv bf \pmod{2f} .$$

But

$$b^2 - 4ac = d = b^{(1)^2} - 4a^{(1)}c^{(1)}$$

and hence

$$b^{(1)} \equiv b \pmod{2} .$$

Further,

$$ur + st = 1 + 2st,$$

and, thus

$$b^{(1)}f(ur+st) \equiv bf \pmod{2f}.$$

Hence,

$$2a^{(1)}us \equiv 0 \pmod{2f}$$

and

$$s \equiv 0 \pmod{f}. \quad // \ [7]$$

The above Proposition is also false without the primitivity conditions. In the first part, if

$$Q'(x,y) = 5(x^2+2y^2) ,$$

then there is no Q of discriminant -8 and M of determinant 5 such that $Q_M = Q'$.

For the second part, let Q and f be chosen such that $|S(f,Q)| \geq 2$. If M and N are inequivalent matrices of $S(f,Q)$, then Q_M and Q_N are inequivalent and

$$Q' = (Q_M)_{fM^{-1}} = (Q_N)_{fN^{-1}}$$

can be derived from two inequivalent forms of the same discriminant.

BIBLIOGRAPHY

[1] Bromwich, T.J.I'A., Quadratic forms and their Classification by means of Invariant-Factors. New York: Hafner Publishing Co., Inc., 1906.

[2] Fox, L., An Introduction to Numerical Linear Algebra. New York: Oxford University Press, 1965.

[3] Jones, Burton W., The Arithmetic Theory of Quadratic Forms. Baltimore: The Waverly Press, 1950.

[4] Lam, T.Y., The Algebraic Theory of Quadratic Forms. Reading, Massachusetts: W.A. Benjamin, Inc., 1973.

[5] LeVeque, William J., Fundamentals of Number Theory. Reading, Massachusetts: Addison-Wesley Publishing Co., 1977.

[6] McCoy, Neal H., Fundamentals of Abstract Algebra. Boston: Allyn and Bacon, Inc., 1972.

[7] Stark, H.M., "Values of L-Functions at $s = 1$", Advances in Mathematics, Vol. 7 (1971), pp. 301-343.

VITA

Dennis M. Warwick, son of Mr. and Mrs. Robert T. Warwick, was born in Trenton, New Jersey on February 20, 1957. He attended Lehigh University where he received a B.A. in Mathematics in 1978. Afterward, he held a teaching assistantship in the Mathematics Department at Lehigh were he completed work toward his M.S. in 1980. Currently he is heading to V.M.I. in Lexington Virginia where he will be an Instructor of Mathematics for 1980-1981.