POSITIVE DEFINITE BINARY QUADRATIC FORMS

by

RUSHTON ERIC DAVIS

B. A., Hendrix College, 1965

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1967

Approved by:

Major Professor

TABLE OF CONTENTS

INTRODUCTION

The purpose of this paper is to investigate and exhibit various properties of positive definite binary quadratic forms. It will be shown that the equivalence of binary quadratic forms is actually an equivalence relation which divides the set of positive definite forms into mutually exclusive equivalence classes. Once these equivalence classes are established, methods will be developed for determining the minimum positive integer represented by all the forms of a given equivalence class. Then methods will be established for determining whether or not a given positive integer has a proper representation by a positive definite form; and, in the case of the sum of two squares, the actual number of proper representations will be determined without having to exhibit them.

It is assumed that the reader has a sufficient knowledge of the theory of numbers; however, in the following paragraphs definitions, theorems, and problems which will be used throughout this paper are presented.

We will accept without proof the following division algorithm. For any two integers a and b, $b \neq 0$, there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < |b|$.

When we speak of a common divisor, we will mean a positive common divisor.

Two integers a and b are said to be relatively prime if their greatest common divisor is unity. Also, there exist integers x and y such that $1 = ax + by$. We note that x and y are not unique by considering $1 = ax + kab - kab + by$

$= a(x + kb) + b(y - ka)$. Since k can be any integer, there are infinitely many x's and y's which will satisfy $1 = ax + by$.

If m is a positive integer, then we say "a is congruent to b modulo m" and write $a \equiv b \pmod{m}$ if and only if $a - b = km$ for some integer k.

If a and m are relatively prime and the congruence $x^2 \equiv a \pmod{m}$ has a solution, we say that a is a quadratic residue of m. If no solution exists, a is called a quadratic nonresidue of m.

We also accept without proof the fact that $x^2 \equiv a \pmod{m}$ has no solution if $x^2 \equiv a \pmod{p}$, where p is some odd prime divisor of m, has no solution.

The integer -1 is a quadratic residue of primes of the form $4k + 1$ and a quadratic nonresidue of primes of the form $4k + 3$.

Two roots, r_1 and r_2, of the congruence $f(x) \equiv 0 \pmod{m}$ are said to be incongruent if $r_1 \not\equiv r_2 \pmod{m}$.

When we refer to the number of roots of a congruence, we mean the number of incongruent roots.

Theorem I-1. If $m_1, \ldots, m_t$ are relatively prime in pairs and if m is their product, the number of roots of $f(x) \equiv 0 \pmod{m}$ is equal to the product of the number of roots of $f(x) \equiv 0 \pmod{m_1}, \ldots, f(x) \equiv 0 \pmod{m_t}$.

Theorem I-2. If p is an odd prime not dividing c, $x^2 \equiv c \pmod{p^n}$ has no root or exactly two roots. The number of roots is the same for all positive integers n.

TRANSFORMATIONS AND EQUIVALENT FORMS

Obtaining a solution to the equation $9 = 2x^2 + xy + 3y^2$ is equivalent to solving the equation $9 = 3X^2 + 5XY + 4Y^2$ which is obtained from the first equation by the linear transformation $x = -Y$, $y = X + Y$. Once a solution for either equation has been found, a solution to the other one is easily obtained with the aid of this linear transformation or its inverse $X = x + y$, $Y = -x$. In a like manner, there are infinitely many equations which are equivalent to $9 = 2x^2 + xy + 3y^2$. It is readily seen that to solve all such equations would be laborious and time-consuming. For this reason we find it beneficial to study linear transformations and equivalences.

Definition 1. A binary quadratic form is a function

(1) $$q = ax^2 + bxy + cy^2$$

where a, b, and c are constants and x and y are independent variables from the integral domain of integers.

If there exist integers x_0 and y_0 such that $m = ax_0^2 + bx_0y_0 + cy_0^2$, m is said to be represented by the form $q = ax^2 + bxy + cy^2$.

It should be noted here that the letters which are employed as independent variables in the quadratic form have no particular significance in themselves. By this we mean that $m = ax^2 + bxy + cy^2$ and $m = au^2 + buv + cv^2$ have the same solutions. Thus it becomes apparent that the constants a, b, and c actually determine the form q given by equation (1). Therefore we will use the notation $q = [a, b, c]$ or just $[a, b, c]$ to denote the form q given by equation (1).

Definition 2. The discriminant of the binary quadratic form given by equation (1) is $d = b^2 - 4ac$.

The linear transformation

$$(2)\qquad T_0: \begin{array}{l} x = \alpha X + \beta Y \\ y = \gamma X + \delta Y \end{array} \qquad \lambda_0 = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0$$

replaces the form $q = [a, b, c]$ by the form $Q = [A, B, C]$ where

$$(3)\qquad \begin{array}{ll} A = a\alpha^2 + b\alpha\gamma + c\gamma^2 & C = a\beta^2 + b\beta\delta + c\delta^2 \\ B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \ . & \end{array}$$

We also say that q is transformed into Q by T_0.

We call $\lambda_0 = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma \neq 0$ of the transformation T_0 in equation (2) the determinant of T_0.

If we replace the form Q by F with the transformation

$$(4)\qquad T_1: \begin{array}{l} X = ru + sv \\ Y = pu + qv \end{array} \qquad \lambda_1 = \begin{vmatrix} r & s \\ p & q \end{vmatrix} \neq 0$$

and then eliminate the variables X and Y between the equations (2) and (4), we obtain

$$(5)\ T_2: \begin{array}{l} x = \alpha(ru+sv) + \beta(pu+qv) = (\alpha r+\beta p)u + (\alpha s+\beta q)v \\ y = \gamma(ru+sv) + \delta(pu+qv) = (\gamma r+\delta p)u + (\gamma s+\delta q)v. \end{array}$$

We now look at the product of the coefficient matrices of the transformations T_0 and T_1,

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} r & s \\ p & q \end{bmatrix} = \begin{bmatrix} \alpha r + \beta p & \alpha s + \beta q \\ \gamma r + \delta p & \gamma s + \delta q \end{bmatrix} .$$

Also note that

$$(6) \qquad \lambda_2 = \begin{vmatrix} \alpha r + \beta p & \alpha s + \beta q \\ \gamma r + \delta p & \gamma s + \delta q \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \begin{vmatrix} r & s \\ p & q \end{vmatrix} = \lambda_0\lambda_1 \neq 0 .$$

Hence the equations (5) are a linear transformation which replaces the form q by F; and as we have observed, T_2 has the same effect upon q as was obtained by first applying T_0 and then T_1. The transformation T_2 is called the product of T_0 and T_1 and is denoted by T_0T_1.

From matrix theory we know that the set of all 2 x 2 matrices is associative under multiplication. From the preceding discussion it follows that if three linear transformations T_1, T_2, and T_3 with nonzero determinants are applied successively to a form q, then $(T_1T_2)T_3 = T_1(T_2T_3)$.

Henceforth we will consider only integral linear transformations of determinant +1.

Definition 3. The binary quadratic form q is said to be properly equivalent to the binary quadratic form Q if and only if there exists a linear transformation T of determinant +1, which replaces q by Q. If the determinant of T is -1, q is said to be improperly equivalent to Q.

For the remainder of this paper we will use the word equivalent to mean properly equivalent.

We write $q \sim Q$ whenever q is equivalent to Q.

Let $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ be the coefficient matrix of the transformation T_0 given by equations (2) and let T_0 have determinant +1. Now consider the matrix product

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} = \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus the transformation given by equations (2) replaces the form $q = [a, b, c]$ by $Q = [A, B, C]$ and the transformation

$$T_1: \begin{array}{l} X = \delta r - \beta s \\ Y = -\gamma r + \alpha s \end{array} \qquad \lambda_1 = \begin{vmatrix} \delta & -\beta \\ -\gamma & \alpha \end{vmatrix} = \alpha\delta - \beta\gamma = 1$$

replaces Q by q since T_0T_1, the identity transformation, replaces q by q. By definition, Q is equivalent to q since $\lambda_1 = +1$. The transformation T_1 is called the inverse of T_0 and is denoted by T_0^{-1}. Here we note that the coefficient matrix of the inverse transformation may be obtained from the coefficient matrix of the original transformation by exchanging the main diagonal elements and changing the algebraic sign of the off diagonal elements whenever the determinant of the original transformation is +1.

Theorem 1. Equivalent forms have the same discriminant.

Let $q = [a, b, c]$ be equivalent to $Q = [A, B, C]$; then there exists a transformation T of determinant +1 which replaces $[a, b, c]$ by $[A, B, C]$ where A, B, and C are given by equations (3). The discriminant of Q is $D = B^2 - 4AC$, or

$$D = \begin{vmatrix} B & 2C \\ 2A & B \end{vmatrix} = \begin{vmatrix} \delta & \beta \\ \gamma & \alpha \end{vmatrix} \begin{vmatrix} b\alpha + 2c\gamma & b\beta + 2c\delta \\ 2a\alpha + b\gamma & 2a\beta + b\delta \end{vmatrix}$$

$$= \begin{vmatrix} \delta & \beta \\ \gamma & \alpha \end{vmatrix} \begin{vmatrix} b & 2c \\ 2a & b \end{vmatrix} \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$$

$$= (\alpha\delta - \beta\gamma)(b^2 - 4ac)(\alpha\delta - \beta\gamma)$$

$$= b^2 - 4ac = d \ .$$

If $q \sim Q$ and $Q \sim F$, then there exist transformations T_1 and T_2, each of determinant unity, which replace q by Q and Q by F, respectively. By equations (2), (4), and (5) the product transformation $T_3 = T_1T_2$ replaces q by F; and by expression (6) the determinant of T_3 is +1. Therefore, $q \sim F$.

Theorem 2. $(\sim)$ is an equivalence relation.

The identity transformation has determinant unity and replaces q by q. Hence $q \sim q$. If $q \sim Q$, then there exists a transformation T of determinant unity which replaces q by Q. The transformation T^{-1} has determinant unity and replaces Q by q. Hence $Q \sim q$. If $q \sim Q$ and $Q \sim F$, then there exist transformations T_1 and T_2 of determinant unity which replace q by Q and Q by F, respectively. The transformation T_1T_2 has determinant unity and replaces q by F. Hence $q \sim F$.

Thus all binary quadratic forms equivalent to a binary quadratic form q are equivalent to each other and are said to form an equivalence class.

<u>Theorem 3</u>. Equivalent binary quadratic forms represent the same integral values.

Suppose $q \sim Q$; then there exists a transformation

$$T: \begin{array}{l} x = \alpha X + \beta Y \\ y = \gamma X + \delta Y \end{array} \qquad \lambda = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1$$

which replaces $q = [a, b, c]$ by $Q = [A, B, C]$ where A, B, and C are given by equations (3). Let m be any integer represented by Q. This implies that there exist integers X_0, Y_0 such that $m = AX_0{}^2 + BX_0Y_0 + CY_0{}^2$. From the above we get $x_0 = \alpha X_0 + \beta Y_0$ and $y_0 = \gamma X_0 + \delta Y_0$. Thus

$$ax_0{}^2 + bx_0y_0 + cy_0{}^2$$

$$= a(\alpha X_0 + \beta Y_0) + b(\alpha X_0 + \beta Y_0)(\gamma X_0 + \delta Y_0) + c(\gamma X_0 + \delta Y_0)$$

$$= (a\alpha^2 + b\alpha\gamma + c\gamma^2)X_0{}^2 + \left[2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta\right]X_0Y_0$$

$$+ (a\beta^2 + b\beta\delta + c\delta^2)Y_0{}^2$$

$$= AX_0{}^2 + BX_0Y_0 + CY_0 = m.$$

Similarly, $Q \sim q$ since we have shown $(\sim)$ to be an equivalence relation. Hence, by the same argument, if m is represented by q, it is represented by Q.

REDUCED FORMS

Let $q = [a, b, c]$ be a binary quadratic form with negative discriminant. If $\Delta = -d$, then Δ is positive, $a \neq 0$, and

$$(7) \qquad \begin{aligned} 4aq &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (4a^2x^2 + 4abxy + b^2y^2) + (4ac - b^2)y^2 \\ &= (2ax + by)^2 + \Delta y^2 . \end{aligned}$$

If the form q is restricted to representing nonzero integral values, then by equation (7) the product 4aq will necessarily be positive. Because a quadratic form is determined by its constant coefficients, a will determine the sign of the integers representable by q. In other words, if a is positive, q will assume only positive integral values and for this reason is called a positive form. Should a be negative, negative integral values will be assumed by q, and q will be called a negative form. Both positive and negative forms are called definite forms. It should be pointed out that the multiple of q used in equation (7) could have been 4c as well as 4a. Had this been the case, c would have been said to determine the sign of q. However, as the case may be a and c will necessarily have the same sign in a definite form. This becomes apparent when it is recalled the discriminant, $b^2 - 4ac$, must be negative.

When d is positive, equation (7) shows that q may take on both positive and negative integral values since Δ is negative. In this instance q is said to be an indefinite form.

From this point on, only positive definite binary quadratic forms will be discussed.

Let m be an integer greater than zero. Look at all integers less than or equal to m which are represented by the form $q = [a, b, c]$. By equation (7), we have

$$(8) \qquad (2ax + by)^2 + \Delta y^2 \leq 4am$$
$$\Delta y^2 \leq 4am - (2ax + by)^2 .$$

Because $-(2ax + by)^2$ is at most equal to zero,

$$(9) \qquad y^2 \leq 4am/\Delta .$$

There are but a finite number of integral values for which y will satisfy the relation (9), and for each of those values there are but a finite number for which x will satisfy the inequalities (8). Hence there are but a finite number of ways of representing the positive integers less than or equal to the integer m by the form q. Note that each positive integer less than or equal to m is not necessarily represented by q. All that is implied is that the number of integral values represented is finite and that each has a finite number of representations.

<u>Definition</u> 4. A positive form $q = [a, b, c]$ is said to be reduced if

$$(10) \qquad c \geq a \geq b > -a \quad \text{and} \quad b \geq 0 \quad \text{when} \quad c = a.$$

Definition 5. A positive form $q = [a, b, c]$ is said to be semi-reduced if

$$c \geq a \geq |b| . \tag{11}$$

Any integer b which satisfies $a \geq b > -a$ necessarily satisfies $a \geq b \geq -a$; however, the converse is not true. Thus any reduced form is semi-reduced; but a semi-reduced form need not be reduced.

Theorem 4. Every positive form is equivalent to a reduced form.

Let $q = ax^2 + bxy + cy^2$ be a positive form. The integer a is represented by q when $x = \pm 1$ and $y = 0$. Therefore $q = [a, b, c]$ represents at least one positive integer, and hence a minimum positive integer. Call this minimum integer A. There exist relatively prime integers α and γ such that $A = a\alpha^2 + b\alpha\gamma + c\gamma^2$. If α and γ were not relatively prime, we could write $\alpha/D = \alpha_1$ and $\gamma/D = \gamma_1$, where $D > 1$ and α_1 and γ_1 are integral. Then it would follow that $a\alpha_1{}^2 + b\alpha_1\gamma_1 + c\gamma_1{}^2 = a(\alpha/D)^2 + b(\alpha/D)(\gamma/D) + c(\gamma/D)^2 = A/D^2$, which contradicts the fact that A is the minimum positive integral value represented by q. Thus α and γ are relatively prime, and there exist integers β and δ such that $\alpha\delta - \beta\gamma = 1$. Hence the transformation given by equations (2) replaces q by the equivalent form $Q = [A, k, n]$. Transform Q into the equivalent form $F = [A, B, C]$ with the transformation $X = u + tv$, $Y = v$. Since $B = k + 2At$, a proper choice for t yields $-A < B \leq A$. Because C is represented by F, and F and q are equivalent, C is represented by q. Hence $C \geq A$. If $C > A$ or $C = A$ and $B \geq 0$, then F is reduced. If $C = A$ and $B < 0$, then the transformation $u = \eta$, $v = -\xi$ replaces F by $[A, -B, A]$ which is reduced.

Theorem 5. Any two equivalent and distinct semi-reduced, positive forms are one of the two pairs:

$$(12) \qquad [a,\ a,\ c],\ [a,\ -a,\ c];$$

$$(13) \qquad [a,\ b,\ a],\ [a,\ -b,\ a].$$

Let $q = [a, b, c]$ and $Q = [A, B, C]$ be any two distinct and equivalent semi-reduced, positive forms; then there exists a transformation, given by equations (2), of determinant unity which replaces q by Q. The integers A, B, and C are given by equations (3).

Without loss of generality we assume $a \geq A$. Since $(|\alpha| - |\gamma|)^2 \geq 0$, $\alpha^2 + \gamma^2 \geq 2|\alpha\gamma|$. Because q is semi-reduced, $c \geq a \geq |b|$ which implies $b \geq -a$. If $\alpha\gamma \geq 0$, then $\alpha\gamma = |\alpha\gamma|$ and $b\alpha\gamma \geq -a|\alpha\gamma|$. If $\alpha\gamma \leq 0$, then $\alpha\gamma = -|\alpha\gamma|$. Since $a \geq |b|$ also implies $a \geq b$, $-a|\alpha\gamma| \leq b\alpha\gamma$. Thus

$$(14) \quad a \geq A = a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a\alpha^2 - a|\alpha\gamma| + a\gamma^2$$

$$= a(\alpha^2 + \gamma^2) - a|\alpha\gamma| \geq a|\alpha\gamma| .$$

Hence $1 \geq |\alpha\gamma|$.

If $|\alpha\gamma| = 0$, $a \geq A = a\alpha^2 + c\gamma^2 \geq a(\alpha^2 + \gamma^2) \geq a$, since both α and γ are not zero in $\alpha\delta - \beta\gamma = 1$. Thus $a = A$. If $|\alpha\gamma| = 1$, then from the relations (14) $a = A$.

Let $c > a$ or $C > A$. Without disturbing $a = A$ and without loss of generality, we choose $c > a$. Suppose $\gamma \neq 0$; then $c\gamma^2 > a\gamma^2$ and from the relations (14) $a = A > a\alpha^2 - a|\alpha\gamma| + a\gamma^2 \geq a|\alpha\gamma|$. Hence $1 > |\alpha\gamma|$; therefore $\alpha\gamma = 0$, and since $\gamma \neq 0$, $\alpha = 0$. Now $a = A = c\gamma^2 > a\gamma^2 \geq a$. This contradiction shows that $\gamma = 0$. Thus from $\alpha\delta - \beta\gamma = 1$, we get $\alpha\delta = 1$ or $\alpha = \delta = \pm 1$. From equations (3), $B = 2a\alpha\beta + b$, or

$$(15) \qquad B - b = 2a\alpha\beta \, .$$

Now $a \geq |b| = |-b|$ and $a = A \geq |B|$ or $a \geq -b \geq -a$ and $a \geq B \geq -a$. Therefore, $2a \geq B - b \geq -2a$, or $|B - b| \leq 2a$; but from equation (15), $|B - b| = 2a|\alpha\beta| = 2a|\beta|$. This implies $|\beta| \leq 1$. If $\beta = 0$, then we have $a = A$, $b = B$, and, since the discriminants of q and Q must be equal, $c = C$. Thus q and Q are equal and not distinct. Hence $|\beta| = 1$ and $|B - b| = 2a$. From this, one of b or B is a while the other is $-a$. Again, $c = C$ since the discriminants of q and Q are equal. This is the pair given by the expression (12).

Suppose $c = a$ and $C = A$. With $a = A$ and $b^2 - 4ac = B^2 - 4AC$, we get $b^2 = B^2$. Either $B = b$ or $B = -b$. If $B = b$, the two forms are not distinct. Therefore $B = -b$ and we get the pair given by the expression (13).

Theorem 6. Each equivalence class of positive forms contains one and only one reduced form.

Suppose two reduced positive forms are equivalent. The reduced forms are also semi-reduced and must be one of the pairs given by expressions (12) and (13). The second form in expression (12) is not a reduced form; and since a = c in both forms given by expression (13), one of the forms is not reduced. Hence the two reduced forms are not equivalent and must belong to different equivalence classes. Since every positive form is equivalent to a reduced form, each equivalence class contains a reduced form.

NEIGHBORING FORMS

We see from Theorems 4 and 6 that to obtain the minimum integral value represented by a positive definite form $q = [a, b, c]$ we first obtain the reduced form, $R = [A, B, C]$, of its equivalence class and then let $X = 1$, $Y = 0$ in $R = AX^2 + BXY + CY^2$ to get A, the minimum integral value. Upon substituting $X = 1$, $Y = 0$ into the transformation which replaces q by R, we obtain one pair of integers for the independent variables in q which will yield A.

Thus we find it necessary to devise a method for obtaining a transformation which replaces the form q by the reduced form of its equivalence class.

First we introduce the following notation. A transformation

$$x = \alpha X + \beta Y$$
$$y = \gamma X + \delta Y$$

will be written as

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} .$$

This notation will be used throughout this report.

Hence the following definition is necessitated.

Definition 6. A form Q is said to be a right neighboring form to a form q if there exists a transformation

$$\begin{bmatrix} 0 & 1 \\ -1 & \delta \end{bmatrix} \tag{16}$$

which replaces q by Q. The form q is called a left neighboring form to Q.

The transformation given by the expression (16) is of determinant unity and replaces the form $q = [a, b, a_1]$ by the equivalent form $q_1 = [a_1, b_1, a_2]$ where

$$b_1 = -b - 2a_1\delta \quad \text{and} \quad a_2 = a + b\delta + a_1\delta^2. \tag{17}$$

With the aid of neighboring forms we give the following proof of Theorem 4.

Among the right neighboring forms $q_1 = [a_1, b_1, a_2]$ to $q = [a, b, a_1]$ there exists one in which $a_1 \geq |b_1|$. To see this, we divide $-b$ by $2a_1$ to obtain a quotient δ and a remainder $|r| \leq a_1$. Then

$$-b = 2a_1\delta + b_1 \quad \text{where} \quad b_1 = r, \ |r| \leq a_1 .$$

Now if a_2 given by equation (17) is greater than or equal to a_1, q_1 is semi-reduced. If $a_1 > a_2$, then there exists a right neighboring form $q_2 = [a_2, b_2, a_3]$ to q_1 in which $a_2 \geq |b_2|$. Again, if $a_3 \geq a_2$, q_2 is semi-reduced. But if $a_2 > a_3$, we continue the process. In a finite number of steps we obtain a semi-reduced form $Q = [A, B, C]$. This occurs since a_1, a_2, a_3, . . ., is a finite decreasing sequence of positive integers. If $C \neq A$ and $A \geq B > -A$ or if $C = A$ and $A \geq B \geq 0$, Q is reduced. However, if $B = -A$, the transformation $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ replaces Q by $[A, A, C]$ which is reduced. If $C = A$ and $0 > B > -A$, the transformation $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ replaces Q by $[A, -B, A]$ which is also reduced.

Recalling the discussion following Definition 2, we find that the transformation which replaces a form q by the reduced form of its equivalence class is the product of the successive transformations employed to produce the right neighboring forms in the preceding paragraph and one of the transformations $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ if it is warranted.

ASCERTAINMENT OF REDUCED FORMS

Theorem 7. There are a finite number of reduced forms with discriminant $-\Delta$.

Using Definition 4 we obtain

$$4a^2 \leq 4ac = (4ac - b^2) + b^2 \leq \Delta + a^2 ,$$

where Δ was previously shown to be positive.

Hence $3a^2 \leq \Delta$, and

$$a \leq \sqrt{\Delta/3} \text{ .} \tag{18}$$

Thus for a given discriminant $-\Delta$ there are but a finite number of integral values for a which will satisfy relation (18); and since we must have -a   b _ a, there are but a finite number of integral b's. For each pair of a's and b's there is at most one integral c which satisfies $-\Delta = b^2 - 4ac$.

Hence the theorem follows.

There is an expedient method for obtaining all the reduced forms with a given discriminant, but first we need the following theorem.

Theorem 8. Let $-\Delta$ be the discriminant of a positive form. Then $\Delta \equiv 0$ or $3 \pmod 4$.

Since $4ac \equiv 0 \pmod 4$ in $\Delta = 4ac - b^2$, we see that b^2 determines the value to which Δ is congruent modulo four. If b is even, then $b = 2k$, $b^2 = 4k^2$, and $\Delta \equiv 0 \pmod 4$. If b is odd, then $b = 2k + 1$, $b^2 = 4k^2 + 4k + 1$, and $\Delta \equiv -1 \equiv 3 \pmod 4$.

To obtain the reduced forms with discriminant $-\Delta$ let F be the greatest positive integer such that $F \leq \sqrt{\Delta/3}$. Depending upon whether $\Delta \equiv 3$ or $0 \pmod 4$, let the possible values for b be the odd or even integers, respectively, whose absolute values are less than or equal to F. If $b = 2k$, then $\Delta = 4j$ and $(b^2 + \Delta)/4 = k^2 + j$. If $b = 2k + 1$, then $\Delta = 4j + 3$ and $(b^2 + \Delta)/4 = k^2 + k + j + 1$. In either case $ac = (b + \Delta)/4$

is an integer. Write $(b^2 + \Delta)/4$ in as many ways as possible as a product of a and c, remembering that $c \geq a \geq |b|$. Omit all cases in which $b = -a$; and if $c = a$, accept only the cases in which $b \geq 0$.

To illustrate, consider the cases $\Delta = 3$ and $\Delta = 4$. When $\Delta = 3$, $F = 1$, $\Delta \equiv 3 \pmod 4$, and $b = \pm 1$. If $b = 1$, $ac = 1$. Hence $a = c = 1$. We exclude the case $b = -1$, since $a = c = 1$. For the case $\Delta = 4$, $F = 1$, $\Delta \equiv 0 \pmod 4$, and $b = 0$. Since $ac = 1$, $a = c = 1$. Therefore the reduced forms with discriminants -3 and -4 are $[1, 1, 1]$ and $[1, 0, 1]$, respectively.

AUTOMORPHS

Definition 7. A transformation T of determinant unity is said to be an automorph of a form q if T transforms q into q.

Theorem 9. If the automorphs, A, of a form q are known and if T is a transformation which replaces a form h by q, then the automorphs of h are given by TAT^{-1}. Equivalent forms have the same number of automorphs.

The transformation T replaces h by q, A replaces q by q, and T^{-1} replaces q by h. Hence TAT^{-1} replaces h by h. Suppose T_1 is an automorph of h. The transformation $T^{-1}T_1T$ leaves q unaltered. Hence it is an automorph, A, of q. Thus we get $T^{-1}T_1T = A$ or $T_1 = TAT^{-1}$.

Theorem 10. The only automorphs of $a(x^2 + y^2)$ are

$$A = \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{bmatrix} .$$

The only automorphs of $a(x^2 + xy + y^2)$ are

$$A, \; C = \begin{bmatrix} 0 & \mp 1 \\ \pm 1 & \pm 1 \end{bmatrix}, \quad C^{-1} = \begin{bmatrix} \pm 1 & \pm 1 \\ \mp 1 & 0 \end{bmatrix} .$$

If q is any reduced form other than these, its only automorphs are A.

Let $c > a$ and $q = Q$. From Theorem 5, the case $c > a$, $\gamma = 0$. Since $\alpha\delta - \beta\gamma = 1$, $\alpha = \delta = \pm 1$. $B = b$, since $q = Q$. Thus from equations (3), $B = 2a\alpha\beta + b$. This implies that $2a\alpha\beta = 0$ or $\beta = 0$. Hence the only automorphs of q are A.

Let $a = c$. According to Definition 4, $b \geq 0$. Again, from Theorem 5, $|\alpha\gamma| = 0$ or 1. Now $(|\beta| - |\delta|)^2 \geq 0$ so that $\beta^2 + \delta^2 \geq 2|\beta\delta|$. In a manner similar to that of Theorem 5, it can be shown that $b\beta\delta \geq -c|\beta\delta|$. Thus

$$\begin{aligned} c = C = a\beta^2 + b\beta\delta + c\delta^2 &\geq c\beta^2 - c|\beta\delta| + c\delta^2 \\ &\geq c|\beta\delta| . \end{aligned}$$

Hence $|\beta\delta| = 0$ or 1. If $\gamma = 0$, then as in the previous paragraph, $\alpha = \delta = \pm 1$ and $\beta = 0$. If $\beta = 0$, then again $\alpha = \delta = \pm 1$, and, from equations (3), $B = b + 2c\gamma\delta$ so that $2c\gamma\delta = 0$. Thus $\gamma = 0$. In either case we get A.

Suppose $\delta = 0$. From $\alpha\delta - \beta\gamma = 1$, we get $-\beta\gamma = 1$ or $\beta = -\gamma = \pm 1$. From $q = Q$ and equations (3), $b = B = 2a\alpha\beta - b$. Hence $b = a\alpha\beta$. If $\alpha = 0$, then $b = 0$ and $q = ax^2 + ay^2$, and we get B. If $\alpha \neq 0$, then $|\alpha\gamma| = |\alpha||\gamma| = 1$; that is, $|\alpha| = |\gamma| = 1$. Hence $\alpha\beta \neq 0$. Since $a \geq b \geq 0$, $b = a\alpha\beta$ implies that $\alpha\beta = 1$. Thus $\alpha = \beta = -\gamma = \pm 1$. Hence $q = ax^2 + axy + ay^2$ and we get C^{-1}.

If $\alpha = 0$ and $\delta \neq 0$, $\gamma = -\beta = \pm 1$ and $b = B = -b + 2c\gamma\delta$ implies $b = c\gamma\delta$. $\gamma\delta \neq 0$. Since $a = c \geq b \geq 0$, $\gamma\delta = 1$. Hence $-\beta = \gamma = \delta = \pm 1$ and $q = ax^2 + axy + ay^2$, and we get C.

Since $\alpha\delta - \beta\gamma = 1$, the case in which α, β, γ, and δ are all numerically equal to unity is excluded.

Definition 8. A form $[a, b, c]$ is said to be a primitive form if a, b, and c have no common divisors greater than one. A form which is not primitive is imprimitive.

Theorem 11. Each form of an equivalence class is primitive if and only if the reduced form of the equivalence class is primitive.

Let $q = ax^2 + bxy + cy^2 = k(a_1x^2 + b_1xy + c_1y^2)$ be a positive imprimitive form and $k > 1$ the greatest common divisor of a, b, and c. Since a_1 is positive and $b^2 - 4ac = k^2(b_1{}^2 - 4a_1c_1)$ is negative, $q_1 = [a_1, b_1, c_1]$ is a positive form. There exists a transformation T which replaces q_1 by the reduced form Q_1. Also, T replaces q by $Q = kQ_1$, which is necessarily reduced since Q_1 is reduced. Hence if the form q is imprimitive, the reduced form of its equivalence class is imprimitive.

Let T be a transformation which replaces the form q by the reduced form Q. Suppose $Q = kQ_1$ where $k > 1$ is the greatest common divisor of the coefficients in Q. Then T^{-1} replaces Q_1 by some form H. Hence T^{-1} replaces $Q = kQ_1$ by $q = kH$. Therefore the form q is imprimitive if the reduced form of its equivalence class is imprimitive.

Thus a form is imprimitive if and only if the reduced form of its equivalence class is imprimitive. This is equivalent to saying that a form is primitive if and only if the reduced form is primitive.

A combination of Theorem 9 and Theorem 10 shows that all forms equivalent to $a(x^2 + y^2)$ have four automorphs and all forms equivalent to $a(x^2 + xy + y^2)$ have six automorphs. Those forms equivalent to neither of these two have only the automorphs given by A in Theorem 10.

According to the discussion preceding Definition 7, all forms with discriminant -3 or -4 are equivalent to $x^2 + xy + y^2$ or $x^2 + y^2$, respectively. These reduced forms are primitive forms obtained from the forms above by letting $a = 1$. According to Theorem 11, all forms which are equivalent to these two are primitive. Moreover, those which are equivalent to $x^2 + xy + y^2$ have six automorphs and those which are equivalent to $x^2 + y^2$ have four automorphs. Also, all primitive forms not equivalent to one of these two have only the two automorphs given by A in Theorem 10. This proves the following theorem.

<u>Theorem 12</u>. Let w denote the number of automorphs of a primitive form q of discriminant d. If $d = -3$, $w = 6$; if $d = -4$, $w = 4$; and if $d < -4$, $w = 2$.

PROPER REPRESENTATION

An integer m is said to be properly represented by the form $q = [a, b, c]$ if there exist relatively prime integers α, γ such that $m = a\alpha^2 + b\alpha\gamma + c\gamma^2$. In other words, we say that the relatively prime pair (α, γ) is a proper representation of m by $[a, b, c]$.

Theorem 13. Let (α, γ) be a proper representation of $m > 0$ by the form $[a, b, c]$ of discriminant d. Integers β, δ, n can be determined in one and only one way to satisfy $\alpha\delta - \beta\gamma = 1$, $0 \leq n < 2m$, and

$$n^2 \equiv d \pmod{4m} \tag{19}$$

such that the transformation $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ replaces $[a, b, c]$ by the equivalent form $[m, n, k]$ in which k is determined by

$$n^2 - 4mk = d \ . \tag{20}$$

Since α and γ are relatively prime, there exist integers β, δ such that $\alpha\beta - \gamma\delta = 1$. Similarly, there exist other integers β', δ' such that $\alpha\beta' - \gamma\delta' = 1$. Equating the left-hand side of each equation and simplifying yields

$$\alpha(\beta - \beta') = \gamma(\delta - \delta') \ . \tag{21}$$

This implies that α divides $\delta - \delta'$. Hence $\delta = \delta' + \alpha t$. Upon substituting this into equation (21), we get $\beta - \beta' = \gamma t$, or

$\beta = \beta' + \gamma t$. The transformation $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ replaces [a, b, c] by [m, n, k] where, according to equations (3),

$$\begin{aligned} n &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ &= 2a\alpha(\beta' + \gamma t) + b\left[\alpha(\delta' + \alpha t) + (\beta' + \gamma t)\gamma\right] + 2c\gamma(\delta' + \alpha t) \\ &= 2a\alpha\beta' + b(\alpha\delta' + \beta'\gamma) + 2c\gamma\delta' + 2t(a\alpha^2 + b\alpha\gamma + c\gamma^2) \\ &= n' + 2tm\ . \end{aligned}$$

With a proper choice of t, n satisfies $0 \leq n < 2m$ and α and γ are uniquely determined. Since [a, b, c] is equivalent to [m, n, k] , the two forms must have the same discriminant. Hence k is determined from equation (20). Necessarily the congruence (19) is satisfied.

Clearly, if $0 \leq n < 2m$ is a root of the congruence (19), $n + 2m$ is a root. Conversely, n is a root when $n + 2m$ is a root. All n which satisfy the congruence (19) and $0 \leq n < 2m$ are called the minimum roots of the congruence (19). Note that the number of minimum roots is one-half the total number of incongruent roots.

To determine whether or not a positive integer m is properly represented by a form q = [a, b, c] of discriminant d, obtain all minimum roots n of the congruence (19). For each n, determine k from equation (20) and write the form Q = [m, n, k] . If q and Q are not equivalent, Theorem 13 shows that there is no proper representation of m by q belonging to the root n. Let n be a minimum root for which $q \sim Q$. Let A be an automorph of q and T be a transformation which replaces q by Q. Then the product transformation AT replaces q by Q. Conversely, if T_1 is a transformation which replaces q by Q, T_1T^{-1} is an automorph A of q. Thus $T_1T^{-1} = A$ or $T_1 = AT$.

To recapitulate, it is seen that once a transformation T has been found which will replace q by Q, all remaining transformations, which replace q by Q, may be ascertained by forming the product transformations AT, where A denotes the automorphs of q.

If the elements in the first column of the matrices AT are denoted by α and γ, $m = a\alpha^2 + b\alpha\gamma + c\gamma^2$ and m is properly represented by q.

Let (α, γ) be a proper representation of m by the imprimitive form q. Let D be the greatest common divisor of q so that $q = Df$. It is obvious that (α, γ) is a proper representation of the integer m/D by the positive form f. Conversely, if (α, γ) is a proper representation of an integer m_1 by a primitive form f, (α, γ) is a proper representation of $m = Dm_1$ by the imprimitive form $q = Df$. Hence a discussion of proper representation can be reduced to a discussion of proper representation by a primitive form.

The preceding paragraphs and Theorem 12 constitute a proof of the following theorem.

Theorem 14. Let q be a primitive form with discriminant d. Let $w = 6$ if $d = -3$, $w = 4$ if $d = -4$, and $w = 2$ if $d < -4$. Let m be a positive integer. Determine by the congruence (19) and equation (20) all minimum roots n and forms $Q = [m, n, k]$.

If q and Q are not equivalent, then there is no proper representation of m by q belonging to the root n. If $q \sim Q$, there are w representations of m by q belonging to the root n.

Two problems, as yet, have not been considered. The first is how to determine when the forms q and Q of Theorem 14 are equivalent and the second is how to determine a transformation T which replaces q by Q, should they be equivalent.

It has been shown in the section on neighboring forms that there exists a transformation, call it T_1, which replaces q by q_1, the reduced form of q's equivalence class. Similarly, there exists a transformation T_2 which replaces Q by q_2, the reduced form of Q's equivalence class. Should $q_1 = q_2$, then q and Q have the same reduced form, and hence belong to the same equivalence class. Moreover, the product transformation $T_3 = T_1T_2^{-1}$ replaces q by Q.

Suppose that b, in the quadratic form $q = [a, b, c]$, is an even integer; then $b = 2b_1$ and $d = b^2 - 4ac = (2b_1)^2 - 4ac = 4(b_1^2 - ac) = 4d_1$. From equation (20) $n^2 - 4mk = 4d_1$. This implies that n^2 is divisible by 4. Hence we write $n = 2N$, the congruence (19) becomes

$$N^2 \equiv d_1 \pmod{m}, \tag{22}$$

and the condition $0 \leq n < 2m$ becomes $0 \leq N < m$. Necessarily, any root N of the congruence (22) yields a minimum root, $n = 2N$, of the congruence (19).

From Theorems I-1 and I-2 we are led to the following theorem.

Theorem 15. Let b in the form $q = [a, b, c]$ be even. Let m be positive and odd, and let d_1 be relatively prime to m. If d_1 is a quadratic nonresidue for some prime factor p of m, there is no root to the congruence (22). However, if d_1 is a quadratic residue for each of the r distinct prime factors of m, then there are exactly 2^r incongruent roots of the congruence (22).

THE SUM OF TWO SQUARES

If we consider the form $q = x^2 + y^2$, we find that $d = -4$ and $d_1 = -1$. In order to determine the proper representations of a positive odd integer m by q, we must first determine the solutions of the congruence (22). Since -1 is a quadratic residue of all primes p of the form $p = 4k + 1$ and a quadratic nonresidue of those primes of the form $p = 4k + 3$, we see that the congruence (22) has solutions if and only if for each prime factor p of m, $p \equiv 1 \pmod 4$.

Suppose each prime p of m satisfies $p \equiv 1 \pmod 4$. Let r denote the number of distinct prime factors of m. By Theorem 15, there are 2^r solutions to the congruence (22). Take each solution and obtain $n = 2N$. Determine the forms $Q = [m, n, k]$ of Theorem 13. Each Q has discriminant -4 and since q is the only reduced form of the set of positive definite forms with discriminant -4, $Q \sim q$. Thus there are no solutions N of the congruence (22) for which Q is not equivalent to q. By Theorem 14 there are four proper representations of m by each root N. Hence there are $4(2^r)$ representations of m by q.

We have proved the following theorem.

Theorem 16. Let m be positive, odd and a product of powers of r distinct primes p. Let $p \equiv 1 \pmod 4$ for each p. Then m has exactly $4(2^r)$ proper representations by $q = x^2 + y^2$. If $p \equiv 3 \pmod 4$ for any prime factor p, there is no proper representation.

Now suppose m is a positive even integer. Since $x^2 \equiv 0, 1 \pmod 4$ and $y^2 \equiv 0, 1 \pmod 4$, we see that $m = x^2 + y^2 \equiv 0, 2 \pmod 4$. If $m \equiv 0 \pmod 4$, x and y are both even and there is no proper representation of m by $[1, 0, 1]$. Thus if m is to be considered for proper representation, m must satisfy the congruence $m \equiv 2 \pmod 4$. However, being congruent to two does not guarantee a solution to $N^2 \equiv -1 \pmod m$. For example, if $m = 6$, $m \equiv 2 \pmod 4$ but -1 is a quadratic nonresidue of three. Also, it is obvious that there are no integers for which $6 = x^2 + y^2$. If $m = 18 = 2(3^2)$, $m \equiv 2 \pmod 4$ and again -1 is a quadratic nonresidue of three. However, although it is not a proper representation, $18 = 3^2 + 3^2$.

Should $m \equiv 2 \pmod 4$, $m = 2 + 4k = 2(1 + 2k)$ for some integer k. Hence two appears as a factor of m only once. The remaining factors are odd. The process of obtaining a solution to $N^2 \equiv -1 \pmod m$ is now reduced to finding an integer N which satisfies both $N^2 \equiv -1 \pmod 2$ and $N^2 \equiv -1 \pmod{(1 + 2k)}$. Obviously the first congruence has only one incongruent root. Thus if there is a solution to the second congruence, the Chinese Remainder Theorem guarantees that the integer N can be found. From the proof of Theorem 16 we see that $N^2 \equiv -1 \pmod{1 + 2k}$ has a solution if and only if all the primes p which divide 1 + 2k are of the form 4q + 1. In other words, an even integer m is properly represented by the form $[1, 0, 1]$ only if $m \equiv 2 \pmod{4}$ and the odd prime divisors of m are congruent to one modulo four.

Since the only incongruent solution to $N^2 \equiv -1 \pmod{2}$ is one, the number of proper representations of m by $[1, 0, 1]$ is $4(2^r)$ where r is the number of distinct odd primes dividing m.

ACKNOWLEDGMENT

The writer of this paper wishes to express his sincere appreciation to Dr. Richard L. Yates for introducing him to the topic of Positive Definite Binary Quadratic Forms. Dr. Yates' counsel and criticism have proved to be invaluable to the completion of this paper.

BIBLIOGRAPHY

Dickson, Leonard Eugene.
Introduction to the Theory of Numbers. Chicago: The University of Chicago Press, 1929.

Dickson, Leonard Eugene.
Modern Elementary Theory of Numbers. Chicago: The University of Chicago Press, 1950.

Stewart, B. M.
Theory of Numbers. New York: The Macmillan Company, 1965.

POSITIVE DEFINITE BINARY QUADRATIC FORMS

by

RUSHTON ERIC DAVIS

B. A., Hendrix College, 1965

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1967

The purpose of this paper was to investigate the methods for determining the minimum positive integer represented by a positive definite binary quadratic form; the proper representations of a given positive integer by a positive definite binary quadratic form; and, in the special case of the sum of two squares, the number of proper representations of an integer without having to exhibit them.

A form $q = [a, b, c]$ was defined to be equivalent to a second form $Q = [A, B, C]$ if and only if there existed a linear transformation of determinant unity which replaced q by Q. With this definition in mind it was shown that the equivalence of forms was actually an equivalence relation and that equivalent forms represented the same integral values. Also, the mutually exclusive equivalence classes of equivalent forms were shown to contain one and only one reduced form. The minimum positive integral value represented by all the equivalent forms of an equivalence class was then obtained from the reduced form.

Neighboring forms were introduced, and with their use a method was developed by which any positive definite form could be replaced by a reduced form.

By introducing congruences, a method was established for determining whether or not a positive integer m could be properly represented by a given form $q = [a, b, c]$. The method involved obtaining forms equivalent to q, obtaining a transformation T which replaced q by one of the equivalent forms, and then forming the product transformations which would exhibit the proper representations. The product transformations were formed from each of the automorphs of q and the transformation T.

The sum of two squares was found to properly represent odd integers which had, as prime divisors, only those primes of the form 4k + 1. Even integers were properly represented only if they were congruent to two modulo four. However, this was but one restriction which had to be placed on the even integers.