CHAPTER II

EQUIVALENCE AND REDUCTION OF BINARY QUADRATIC FORMS

We have already defined the discriminant D of $f(x,y) = ax^2 + bxy + cy^2$ as the quantity $D = \pm d = b^2 - 4ac$ where d is always > 0. D is congruent to 0 or 1 (mod 4) and has the same parity as b. So, b is even only when $D \equiv 0 \pmod 4$.

By completing the square of $f(x,y)$ we get $4af(x,y) = (2ax + by)^2 - Dy^2$. If $D > 0$ then $f(1,0) = a$ and $f(-b, 2a) = -aD$ have opposite signs unless $a = 0$. Similarly, $f(0,1) = c$ and $f(2c, -b) = -cD$ have opposite signs unless $c = 0$. If $a = c = 0$, then $f(x,y) = bxy$ with $b \neq 0$ since $D \neq 0$. In this case, $f(1,1)$ and $f(-1,1)$ have opposite signs. Therefore, if $D > 0$ then $f(x,y)$ takes on both positive and negative values and is said to be *indefinite*.

If $D < 0$, then $4af(x,y) > 0$ whenever $(x,y) \neq (0,0)$. So, a and $f(x,y)$ have the same sign. The form thus takes on positive values when $a > 0$ and negative values when $a < 0$. Hence, to simplify matters, we only consider positive definite forms, multiplying f through by -1 if necessary. Finally, note $c > 0$ since $ac = (b^2 - D)/4 > 0$.

Let $f(x,y) = x^2 + y^2$ and $F(X,Y) = X^2 + 2XY + 2Y^2$. What can we say about the integers represented by $f(x,y)$ and $F(X,Y)$? Let's try some computations.

$$\begin{aligned} f(1,0) &= F(1,0) = 1; & f(1,1) &= F(0,1) = 2 \\ f(2,1) &= F(1,1) = 5; & f(3,2) &= F(1,2) = 13 \\ f(1,4) &= F(3,1) = 17; & f(5,2) &= F(3,2) = 29 \end{aligned}$$

and so on.

As you can see, the same numbers are represented by both forms. The y-values remain the same while the x-values change. If $n = x^2 + y^2$ then $n = X^2 + 2XY + 2Y^2$ where $X = x - y$ and $Y = y$. Also, if $n = X^2 + 2XY + 2Y^2$ then $n = x^2 + y^2$ where $x = X + Y$ and $y = Y$. So, we have:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

DEFINITION. Two binary quadratic forms $f(x,y)$ and $F(X,Y)$ are said to be *equivalent*, and we write $f \sim F$ if there exists a 2 by 2 invertible matrix U over $\mathbb{Z}$

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \alpha, \beta, \gamma, \delta \in \mathbb{Z}$$

such that $f(x,y) = F(\alpha x + \beta y; \gamma x + \delta y)$. If $\det U = +1$, we say the equivalence is *proper*; otherwise, the equivalence is *improper*.

Later on, it will become clear why we distinguished between proper and improper equivalence. We now restrict our attention to proper equivalence, that is to 2-by-2 matrices with integral coefficients and determinant $+1$. If M and N are matrices with integral coefficients and determinant $+1$ then so are $M \cdot N$ and M^{-1}. This set forms a group under multiplication of matrices. The group of 2-by-2 matrices with integral coefficients and determinant 1 is denoted by $SL(2,\mathbb{Z})$ and is called the *modular group*.

LEMMA 2.1. *Two equivalent binary quadratic forms have the same discriminant.*

Suppose $f(x,y) = ax^2+bxy+cy^2$ and $F(X,Y) = AX^2+BXY+CY^2$ are equivalent with $F(X,Y) = f(\alpha X + \beta Y, \gamma X + \delta Y)$ for some integers $\alpha, \beta, \gamma, \delta$ satisfying $\alpha\delta - \beta\gamma = \pm 1$. Then

$$\begin{aligned} A &= f(\alpha,\gamma) = a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ B &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ C &= f(\beta,\delta) = a\beta^2 + b\beta\delta + c\delta^2 \end{aligned} \tag{2.1}$$

Now, it's easy to check that $B^2 - 4AC = (\alpha\delta - \beta\gamma)^2(b^2 - 4ac)$. Since $\alpha\delta - \beta\gamma = \pm 1$, it follows that the discriminants are equal.

It is probably easiest to keep track of what is going with suitable matrix arithmetic rather than the complicated formulae displayed above. With a slight abuse of notation

$$\begin{aligned} ax^2 + bxy + cy^2 &= (x,y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \\ &= (X,Y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix} \end{aligned}$$

since $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$. Therefore

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

so Lemma 2.2 follows by taking determinants.

`Exercise.` Suppose $f \sim g$. Show that n is properly represented by f if and only if n is properly represented by g.

The notion of proper equivalence as we defined it is an equivalence relation: that is it is reflexive, symmetric and transitive. Therefore, it partitions the set of binary quadratic forms into equivalence classes. Since we have infinitely many 2-by-2 integer matrices with determinant 1, we have infinitely many forms in each equivalence class. The natural thing to do is to pick a natural representative form from each equivalence class. This is what we call a "*reduced form*". But before we introduce reduction of forms, it is important to point out that since indefinite forms present greater complications than definite forms, we focus our discussion on definite forms (though many of the ideas carry through to indefinite forms).

DEFINITION. A binary quadratic form $ax^2+bxy+cy^2$ with negative discriminant $-d = b^2 - 4ac$ is said to be *reduced* if $-a < b \le a < c$ or $0 \le b \le a = c$.

If $f(x,y) = ax^2 + bxy + cy^2$ is reduced then $|b| \le a \le c$, which implies that

$$3a^2 \le 4ac - a^2 \le 4ac - b^2 = d$$

so that $a \le \sqrt{\frac{d}{3}}$.

`Exercise.` Show that there are no more than $2d/3$ equivalence classes of quadratic form of discriminant $-d < 0$.

We now find all reduced forms of discriminant -4: if $ax^2 + bxy + cy^2$ is reduced of discriminant -4 then $0 \le a \le \sqrt{\frac{4}{3}}$ and so $a = 0$ or $a = 1$.

(i) If $a = 0$ then $b = 0$. This can't happen since $-4 = b^2 - 4ac$.
(ii) If $a = 1$ then $b = 0$ or $b = 1$. If $b = 0$ then $ac = 1$ i.e. $c = 1$. In this case, we get the reduced form $x^2 + y^2$. If $b = 1$ then $c = \frac{5}{4}$; and this is impossible since we are dealing with forms having integral coefficients. Therefore $x^2 + y^2$ is the only reduced form of discriminant -4.

`Exercise.` Show that $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are the only reduced forms of discriminant -20.

$f(x,y) = ax^2 + bxy + cy^2$ is said to be *primitive* if $\gcd(a,b,c) = 1$; otherwise f is *imprimitive*.

`Exercise.` Make a table of *all* reduced binary quadratic forms of discriminant $-d$ for each $d < 200$. Note that $a \le \sqrt{200/3} < 9$. So run through values of a and b in the range $-a < b \le a \le 8$ and select each $c \ge a$ so that $0 < 4ac - b^2 \le 200$.

(i) For which d do we have just one class of forms?
(ii) Would you expect there to be many more such d? Justify your answer.
(iii) For which d do we have reduced imprimitive forms of discriminant $-d$? Can you "classify" these forms in some way?

D is called a *fundamental discriminant* if there are *no* imprimitive quadratic form of discriminant D. Prove that integer D is a fundamental discriminant if and only $D \equiv 1 \pmod 4$, or $D \equiv 8$ or $12 \pmod{16}$ and D is not divisible by the square of any odd prime.

We have already pointed out that if D is the discriminant of a binary quadratic form then $D \equiv 0$ or $1 \pmod 4$. The converse is also true since we always have the *principal* form of discriminant D:

$$\begin{aligned} x^2 - \frac{D}{4}y^2 \quad & \text{if } D \equiv 0 \pmod 4 \\ x^2 + xy + \left(\frac{1-D}{4}\right)y^2 \quad & \text{if } D \equiv 1 \pmod 4. \end{aligned}$$

Note that these are reduced as defined.

The *class number* $h(D)$ is the number of equivalence classes of primitive forms having discriminant D. For convenience we shall henceforth write (a,b,c) to denote the binary quadratic form $ax^2 + bxy + cy^2$.

THEOREM 2.1 (GAUSS'S REDUCTION ALGORITHM). *Every binary quadratic form of negative discriminant is properly equivalent to a reduced form with the same discriminant.*

PROOF. We shall there is no least counterexample (that is with a minimal and then $|b|$).

If $c < a$ apply the transformation $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ to get a form $Ax^2 + Bxy + Cy^2$ with $A = c \quad (B = -b, C = a)$ so that $A < a$.

If $b \le -a$ or $b > a$ then let $B \equiv b \mod 2a$ with $-a < B \le a$. Let $\delta = (b-B)/2a$ so we get the form $ax^2 + Bxy + Cy^2$ from the transformation $\begin{pmatrix} 1 & -\delta \\ 0 & 1 \end{pmatrix}$.

Finally if $a = c$ and $b < 0$ we get $ax^2 - bxy + ay^2$ using the transformation $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

DEFINITION. A form $ax^2 + bxy + cy^2$ is said to be a *left neighbor* to $a'x^2 + b'xy + c'y^2$ of the same determinant if $c = a'$ and $b \equiv -b' \pmod{2c}$. In this case, $a'x^2 + b'xy + c'y^2$ will be a *right neighbor* to $ax^2 + bxy + cy^2$. It is convenient to write this with the notation:

$$\begin{array}{ccccccccc} & & b_1 & & & & b_2 & & \\ a_1 & & & c_1 = a_2 & & c_2 & = & a_3 & \\ & & & & & & & & \end{array} \qquad \begin{array}{ccc} & & b_3 \\ & & \\ c_3 & = & \cdots \end{array}$$

which makes hand computation easy.

EXAMPLES. The form $(5, 8, 6)$ is a right neighbor to the form $(3, 2, 5)$ and the form $(5, 1, 5)$ is a left and right neighbor to its opposite $(5, -1, 5)$.

LEMMA 2.2. *Let $f(x, y) = ax^2+bxy+cy^2$ be a primitive positive definite reduced form. Then a is the smallest non-zero integer represented by f. Either c is the smallest integer represented by f which is not of the form ax^2 or $c = ar^2$ for some $r \ge 1$ and is the smallest integer represented in more than two ways by f.*

PROOF. Note that $f(\pm 1, 0) = a \le c = f(0, \pm 1)$.

$$f(x, y) \ge ax^2 - a|xy| + cy^2 = a\left(|x| - \frac{|y|}{2}\right)^2 + \frac{3cy^2}{4} \ge 3c \text{ if } |y| \ge 2.$$

If $|y| = 1$ then $f(x, y) \ge a(x^2 - |x|) + c \ge c$. Thus if $f(x, y) < c$ we must have $y = 0$ so we have $f(x, 0) = ax^2$. Finally if $c = ar^2$ then $c = f(0, \pm 1) = f(\pm r, 0)$.

`Exercise.` Find all reduced forms of negative discriminant representing 1.

THEOREM 2.2. *If two positive definite reduced forms are properly equivalent then they are equal.*

PROOF. If $f = (a, b, c)$ and $F = (A, B, C)$ are equivalent reduced positive definite forms, then since the numbers represented by f and F are in 1-1 correspondence by Lemma 2.2 we have $a = A$ and $c = C$. Since $B^2 = d + 4ac = d + 4AC = b^2$, therefore $B = -b$. Suppose

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{where} \quad \alpha\delta - \beta\gamma = 1,$$

transforms f to F. Then $a = a\alpha^2 + b\alpha\gamma + c\gamma^2$. By Lemma 2.2, either $\gamma = 0$ or $c = a$. If $\gamma = 0$ then $-b = B = b + 2a\beta$ so $|b| = a$. In each case one of the two forms is not reduced.

From the above theorem, it follows that if $-d < 0$ then the reduced form in a given equivalence class is unique. In this case, the class number $h(-d)$ is the number of reduced forms having discriminant $-d$.

COROLLARY 2.3. *Let D be a negative discriminant having class number one. If $D \equiv 0 \pmod 4$ then $x^2 - \frac{D}{4}y^2$ is the only reduced form of discriminant D. If $D \equiv 1 \pmod 4$ then $x^2 + xy + \frac{1-D}{4}y^2$ is the only reduced form of discriminant D.*

EXAMPLE. Odd prime p is represented by $x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

Solution: Suppose $p = x^2 + y^2$ for some integers x and y. Obviously, x and y cannot have the same parity. If we assume x is even and y is odd we get $x^2 \equiv 0 \pmod 4$ and $y^2 \equiv 1 \pmod 4$. Hence $p \equiv 1 \pmod 4$. Conversely, if $p \equiv 1 \pmod 4$ then $\left(\frac{-1}{p}\right) = 1$. So, there exists a solution b to the congruence $b^2 \equiv -4 \pmod p$, and let $c = \frac{b^2+4}{4p}$. The form $px^2 + bxy + cy^2$ of discriminant -4 represents p. So, p must be represented by a reduced form of the same discriminant. Since $x^2 + y^2$ is the only reduced form of discriminant -4, p must be represented by $x^2 + y^2$.

`Exercise.` What primes are represented by $x^2 + xy + y^2$? By $x^2 + 3y^2$? By $x^2 + xy + 2y^2$?

EXAMPLE. Odd prime p is represented by $x^2 + 5y^2$ if and only if $p = 5$ or $p \equiv 1$ or $9 \pmod{20}$. Odd prime p is represented by $2x^2 + 2xy + 3y^2$ if and only if $p \equiv 3$ or $7 \pmod{20}$.

PROOF. If $p = 5$ then $p = D^2 + 5 \cdot 1^2$. If $p \neq 5$ and $p = x^2 + 5y^2$ for some integers x and y, then $\left(\frac{p}{5}\right) = \left(\frac{-5}{p}\right) = 1$ and so, $p \equiv 1$ or $9 \pmod{20}$. Conversely, $\left(-\frac{5}{p}\right) = 1$ if and only if $p \equiv 1, 3, 7$ or $9 \pmod{20}$. In this case, there exists a solution b to the congruence $b^2 \equiv -20 \pmod p$. Let $c = \frac{b^2+20}{4p}$. The form $px^2 + bxy + cy^2$ of discriminant -20 represents p, and therefore there exists a reduced form of the same discriminant representing p. Since $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are the only reduced forms having discriminant -20, p must be represented by one of them.

(i) If $p = 2x^2 + 2xy + 3y^2$ then $2p = (2x + y)^2 + 5y^2$ and so $\left(\frac{2p}{5}\right) = 1$ and this implies $\left(\frac{p}{5}\right) = -1$ i.e. $p \equiv 3$ or $7 \pmod{20}$.

(ii) If $p = x^2 + 5y^2$, we've already seen that $p \equiv 1$ or $9 \pmod{20}$.

This completes the proof.

We have already seen an example of a negative discriminant Δ with $h(\Delta) = 1$. In fact, it has been proved by Heegner, Stark and Baker that there are exactly nine negative discriminants Δ for which $h(\Delta) = 1$; and these are:

$$\Delta = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Later we will discuss some of the deep proofs of this fact.

What about positive discriminants? Gauss conjectured that there are infinitely many positive discriminants with class number one, a question that is still wide open – we discuss this more later on.

LEMMA 2.3. *Let $f(x,y)$ be a binary quadratic form. If a non-zero integer n is properly represented by f, then there exist integers B and C such that f is properly equivalent to $nx^2+Bxy+Cy^2$.*

PROOF. Since n is properly represented by $f(x,y)$, there exist coprime integers α and γ, such that $n=f(\alpha,\gamma)$. Let β and δ be integers satisfying $\alpha\delta-\beta\gamma=1$. The matrix $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ transforms f to a binary quadratic form $Ax^2+Bxy+Cy^2$ where $A=f(\alpha,\gamma)=n$. The result now follows.

LEMMA 2.4. *Let $f(x)=x^2+x+\frac{1-D}{4}$ with $D\equiv 1 \pmod 4$ and let $ax^2+bxy+cy^2$ be any form of the same discriminant D. For any odd prime p dividing a, there exists an integer x, $0\le x\le \frac{p-1}{2}$ such that $f(x)\equiv 0 \pmod p$.*

PROOF. Since $a\equiv 0 \pmod p$, we have $D\equiv b^2 \pmod p$ that is $\left(\frac{D}{p}\right)\neq -1$. Let $b\equiv y \pmod p$ with $0\le y\le p$. Since p is odd, one of y and $p-y$ must be odd. So, we may assume that there exists an odd number $2x+1$ with $1\le 2x+1\le p$ (that is $0\le x\le \frac{p-1}{2}$) satisfying $D\equiv (2x+1)^2 \pmod p$. Now, we have

$$D\equiv 4x^2+4x+1 \pmod p, \quad \text{or} \quad 4\left(x^2+x+\frac{1-D}{4}\right)\equiv 0 \pmod p.$$

As $p\neq 2$, we get $f(x)=x^2+x+\frac{1-D}{4}\equiv 0 \pmod p$.

LEMMA 2.5. *Let $ax^2+bxy+cy^2$ be a form of discriminant D. If 2 divides a then $\frac{1-D}{4}\equiv 0 \pmod 2$.*

PROOF. Since $2\mid a$, we have $D\equiv b^2\equiv 1 \pmod 8$. So, $8\mid 1-D$ that is $\frac{1-D}{4}\equiv 0 \pmod 2$.

THEOREM 2.4. *Let D and n be given integers with $n\neq 0$. n is properly represented by some binary quadratic form of discriminant D if and only if D is a quadratic residue $\pmod{4|n|}$.*

PROOF. Suppose there exists an integer b satisfying the congruence $b^2\equiv D \pmod{4|n|}$. Let $c=\frac{b^2-D}{4n}$. The form $f=nx^2+bxy+cy^2$ of discriminant D represents n properly, with $n=f(1,0)$. Conversely, if n is properly represented by a form f of discriminant D, then $f(x,y)$ will be equivalent to $nx^2+Bxy+Cy^2$ for some integers B and C (by Lemma 2.3). Since the discriminants of equivalent forms are equal, we have $D=B^2-4nC$, and so $D\equiv B^2 \pmod{4|n|}$.

COROLLARY 2.5. *Odd prime p divides $f(x,y)$ with $(x,y)=1$ for some form f of discriminant D if and only if $\left(\frac{D}{p}\right)=0$ or 1.*

PROOF. By (1.2), p divides

$$4af(x,y)=(2ax+by)^2+dy^2, \quad \text{so} \quad \left(\frac{-d}{p}\right)=1 \quad \text{if} \quad y\not\equiv 0 \mod p.$$

If $y\equiv 0 \pmod p$ then $2ax+by\equiv 0 \pmod p$ so p divides $2ax$. Now $(x,y)=1$ so p does not divide x. This p divides $2a$, which divides $4ac=b^2+d$ so $(\frac{-d}{p})=0$ or 1.

LEMMA 2.6. *If a non-zero integer n is represented by a reduced form $ax^2+bxy+cy^2$ of discriminant $-d$ then $n = ax^2$ if $y = 0$ and $n \geq \frac{\sqrt{3d}}{4}$ if $y \neq 0$. In particular, a is the only square-free integer less than $\frac{\sqrt{3d}}{4}$ represented by f.*

If $y \neq 0$ then $4af(x,y) = (2ax+by)^2 + dy^2 \geq 0^2 + d.1^2 = d$, so $f(x,y) \geq d/4a \geq \sqrt{3d}/4$.

Now, if $a \leq \sqrt{\frac{3d}{4}}$ and $-d$ is a quadratic residue $\pmod{4a}$ then there exists a reduced form $ax^2 + Bxy + Cy^2$ with discriminant $-d$. So,

$$h(-d) \geqq \# \left\{ a \leq \frac{\sqrt{3d}}{4} : -d \quad \text{is a quadratic residue} \pmod{4a} \right\}$$

`Exercise.` Deduce that if $h(-d) = 1$ and p is an odd prime less than $\frac{\sqrt{3d}}{4}$ then $\left(\frac{-d}{p}\right) = -1$.

If $-d \equiv 1 \pmod 4$ and $d = rs$ with $0 < r < s$ then $a = \frac{r+s}{4}$ and $b = \frac{s-r}{2}$ are positive integers. (Exercise: Prove this.) $ax^2 + bxy + ay^2$ is a form of discriminant $-d$. Moreover it is reduced if $r \geqq s/3$.

THEOREM 2.6 (RABINOWICZ 1912). *Let d be positive integer with $-d \equiv 1 \pmod 4$ and let $A = \frac{d+1}{4}$. Then $h(-d) = 1$ if and only if $n^2 + n + A$ is prime for all $0 \leq n \leq A-2$.*

PROOF. $\Rightarrow$: If an odd prime p divides $f(x,y)$ for some binary quadratic form f of discriminant $-d$ then $\left(\frac{-d}{p}\right) = 0$ or 1 (by Corollary 2.5). So, p is represented by a form of discriminant $-d$ by Theorem 2.4. Since $h(-d) = 1$ and $-d \equiv 1 \pmod 4$, $x^2 + xy + Ay^2$ is the only reduced form having discriminant $-d$. Hence, there exist integers x_0 and $y_0 \neq 0$ such that $p = x_0^2 + x_0y_0 + Ay_0^2 = \left(x_0 + \frac{1}{2}\right)^2 + \left(A - \frac{1}{4}\right) y_0^2 \geq A - \frac{1}{4}$. Therefore, $p \geq A$.

For $0 \leq n \leq A-2$, we have $n^2 + n + A \leq (A-1)^2 + 1 < A^2$. If $n^2 + n + A$ is composite for some $0 \leq n \leq A-2$, then there is a prime $q < A$ which divides n^2+n+A, giving a contradiction. Therefore, n^2+n+A is prime for all $0 \leq n \leq A-2$.

$\Leftarrow$: Suppose $n^2 + n + A$ is prime for $0 \leq n \leq A-2$. If $p < A$ and $\left(\frac{-d}{p}\right) = 1$ then $\#\{n : 0 \leq n \leq A-2,\ p \mid n^2 + n + A\} \geq \#\{n : 0 \leq n \leq p-1,\ p \mid n^2 + n + A\} = 2$. Obviously, this leads to a contradiction since a prime can divide (that is, equal) $n^2 + n + A$ for at most one $0 \leq n \leq A-2$ as $n^2 + n + A$ is an increasing sequence. So, if $p < A$ then $\left(\frac{-d}{p}\right) = 0$ or -1.

Now, suppose $h(-d) > 1$ and let $ax^2 + bxy + cy^2$ be a non-principal reduced form of discriminant $-d$. Then $a \leq \sqrt{\frac{d}{3}} < A$, and $-d$ is a quadratic residue mod $4a$ by the Theorem above. If p is an odd prime dividing a then $\left(\frac{-d}{p}\right) = 0$ or 1 and so, by the above, p must divide d.

Now if p divides d with $p \leq 2A-3$ then $n^2 + n + A \equiv \left(n + \frac{1}{2}\right)^2 \pmod p$ and so p divides $n^2 + n + A$ exactly when $n \equiv \frac{p-1}{2} \pmod p$. But then $n^2 + n + A > p$ and so is not prime giving a contradiction.

EXAMPLE. Since $h(-163) = 1$, $x^2 + x + 41$ is prime for all $0 \le x \le 39$. (This is the very famous example of Legendre.) Find 8 other examples of such polynomials.[1]

`Exercise.` Prove an analogous result for $-d \equiv 0 \pmod 4$.

§2a. Indefinite binary quadratic forms

A form $ax^2+bxy+cy^2$ of discriminant $d > 0$ is said to be "reduced" if $0 < b < \sqrt{d}$, and

$$\sqrt{d} - b < |2a| < \sqrt{d} + b.$$

Notice that if $ax^2 + bxy + cy^2$ is an indefinite reduced form of discriminant d then $\frac{|2c|}{\sqrt{d}+b} = \frac{\sqrt{d}-b}{|2a|} < 1$ and $\frac{|2c|}{\sqrt{d}-b} = \frac{\sqrt{d}+b}{|2a|} > 1$. So,

$$\sqrt{d} - b < |2c| < \sqrt{d} + b$$

and therefore $cx^2 + bxy + ay^2$ is also reduced.

There are only finitely many reduced forms for any given discriminant $d > 0$, since $0 < b < \sqrt{d}$ and $|a| < (\sqrt{d} + b)/2 < \sqrt{d}$, and c is then determined.

THEOREM 2.7. *Any form of discriminant $d > 0$ is properly equivalent to a reduced form (not necessarily unique) of the same discriminant.*

PROOF. Let $ax^2 + bxy + cy^2$ be a non-reduced indefinite form. Since $ax^2 + bxy + cy^2$ is properly equivalent to $cx^2 - bxy + ay^2$, we may assume $|a| \ge |c|$. The transformation

$$U = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix} \text{ where } \delta \text{ is an integer}$$

takes $ax^2+bxy+cy^2$ to $Ax^2+Bxy+Cy^2$ where $A = c$ and (by a suitable choice of δ), B is any integer satisfying $B \equiv -b \pmod{2c}$. We choose B so that $\sqrt{d}-|2A| < B < \sqrt{d}$. By applying the transformation successively, we get a sequence of properly equivalent forms

$$ax^2 + bxy + cy^2 \sim a_1x^2 + b_1xy + c_1y^2 \sim \dots .$$

$|a_i| \ge |c_i|$ for all i, so the sequence $\{|a_i|\}$ is positive and decreasing, which is impossible. We claim that the form $a_mx^2 + b_mxy + c_my^2$ is reduced. Since $\sqrt{d} - |2a_m| < b_m < \sqrt{d}$, we have

$$0 < \sqrt{d} - b_m < 2|a_m| \le 2|c_m| = \frac{d - b_m^2}{2|a_m|} < |\sqrt{d} + b_m|.$$

But $b_m > 0$ since $\sqrt{d} - b_m < |\sqrt{d} + b_m|$ and the result follows.

[1]Even though Rabinowicz's result completely classifies when $n^2 + n + A$ is prime for all $0 \le n \le A - 2$, it is still of interest to find quadratic polynomials that take on many prime values. In

THEOREM 2.8. *Let (a,b,c) and (c,b_1,a_1) be two forms of discriminant d with (a,b,c) reduced. Write $b_1=-b-2\delta a$ for some integer δ. Then (c,b_1,a_1) is reduced if and only if $\delta a>0$ and $|\delta|$ is the greatest integer less than $\left|\frac{2a}{-b+\sqrt{d}}\right|$.*

PROOF. Let $x_1=\frac{-b+\sqrt{d}}{2a}$, $x_2=\frac{-b-\sqrt{d}}{2a}$, $y_1=\frac{-b_1+\sqrt{d}}{2c}$ and $y_2=\frac{-b_1-\sqrt{d}}{2c}$. Notice that

$$y_1=\delta-\frac{1}{x_1} \text{ and } y_2=\delta-\frac{1}{x_2}.$$

Also, since (a,b,c) is reduced x_1 has the sign of a and the opposite sign of x_2.
$\Rightarrow$ If (c,b_1,a_1) is reduced then $\sqrt{d}-b_1<|2c|<\sqrt{d}+b_1$ that is $|y_1|<1$. Hence, δ and x_1 have the same sign and $\left|\delta-\frac{1}{x_1}\right|<1$. Since x_1 and a have the same sign, the result now follows.
$\Leftarrow$ By our choice of δ, y_1 has the opposite sign of x_1 and $|y_1|<1$, this gives $|2c|>|-b+\sqrt{d}|$. Also, since x_1 and x_2 have opposite signs, y_2 is the sum of two integers of the same sign; so $|y_2|>1$ and y_2 has the same sign as δ (that is the opposite sign of y_1). This gives $|2c|<|-\sqrt{d}-b|$. Now, since y_1 and y_2 have opposite signs and $|y_1|<|y_2|$, we get $|-b+\sqrt{d}|<|-b-\sqrt{d}|$ that is $0<b<\sqrt{d}$.

COROLLARY 2.9. *Every reduced indefinite quadratic form has one and only one reduced left (right) neighboring form.*

THEOREM 2.10. *Let $g(x)=-x^2+x+m^2$ be a binary quadratic form of discriminant d with $m\geq 2$. Then $h(d)=1$ if and only if $g(x)$ is prime for all $2\leq x\leq m$.*

PROOF. Instead of $g(x)$, let's look at $-g(x+1)=x^2+x-m^2=x^2+x+\frac{1-d}{4}$. Call it $f(x)$. We may rewrite the theorem as $h(d)=1$ if and only if $-f(x)$ is prime for all $1\leq x\leq m-1$.
$\Rightarrow$ If $-f(x)$ is composite for some $1\leq x_0\leq m-1$ then there exists a prime $p\leq\sqrt{-f(x_0)}$ such that $-f(x)\equiv 0 \pmod p$. Since $-f(x)$ is a decreasing function for $x\geq 0$ and $-f(1)=m^2-2$, we have $-f(x_0)<m^2$ that is $p<m$. Now, we have $x_0^2+x_0+\frac{1-D}{4}\equiv 0 \pmod p$ that is $(2x_0+1)\equiv D \pmod{4p}$. Let $b\equiv 2x_0+1 \pmod{2p}$ with $\sqrt{D}-2p<b<\sqrt{D}$. Write $b^2=D-4Kp$ for some integer K. We claim that the form (p,b,K) is reduced for $\sqrt{D}-2p>\sqrt{D}-2m>0$ that is $b>0$ and $2p<2m<2m+b<\sqrt{D}+b$. Also, by our choice of b, $\sqrt{D}-2p<b$. But (p,b,K) is not in the principal class since $p\neq m$ and this contradicts our assumption that $h(d)=1$.
$\Leftarrow$ Let (a,b,c) be a reduced form of discriminant d. By definition of reduced forms, we have $0<b<\sqrt{d}$ that is $0<b\leq 2m$ and $\sqrt{4m^2+1}-b<|2a|<\sqrt{4m^2+1}+b$ that is $|2a|\leq 4m$ or $|a|\leq 2m$. Suppose a is odd and let p be a prime dividing a. By Lemma 2.6, $f(x)\equiv 0 \pmod p$ for some integer x with $0\leq x\leq\frac{p-1}{2}<\frac{2m-1}{2}=m-\frac{1}{2}$, hence $0\leq x\leq m-1$. If $x=0$ then $m^2\equiv 0 \pmod p$ which gives $p=m$ since $-f(m-1)=m$ is prime by our assumption. Also, since $-f(x)$ is a decreasing function for $x\geq 0$ and $-f(m-1)=m$ and $-f(m-2)=3m-2>2m$ we have $-f(x)=p$ for all $1\leq x\leq m-1$. Hence, $p=m$. Therefore, m is the only prime divisor of $|a|$ and so $a=\pm m$ since $|a|\leq 2m$ and a odd. Since $d=4m^2+1$ and $d\equiv b^2 \pmod{4m}$, we have $b\equiv\pm 1 \pmod m$. As $0<b\leq 2m$ and b is odd (since d is odd), the only possible values for b are 1 or $2m-1$. So, we have $a=\pm m$ and $b=1$ or $2m-1$ and this gives the forms $(m,1,-m)$, $(m,2m-1,-1)$, $(-m,1,m)$ and $(-m,2m-1,1)$. Since all of these forms belong to the principal class, it follows

that $h(d) = 1$. If a is even, then $\frac{1-d}{4} \equiv 0 \pmod 2$ by Lemma 2.7 that is $m^2 \equiv 0 \pmod 2$ which gives $m = 2$ as m is prime. Hence, $d = 17$, and this case can be verified.