Elementary Number Theory

Section 3.2 Binary Quadratic Forms

Definition 3.2.1 (a) A monomial $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}, a \neq 0$ is said to have degree $k_1 + k_1 + \cdots + k_n$.

(b) The degree of a polynomial is the maximal of the degrees of the monomial terms in the polynomial.

(c) A polynomial is called a form, or is said to be homogeneous if all its monomial terms have the same degree.

(d) A form of degree 2 is called a quadratic form.

(e) A form in two variables is called binary.

(f) The discriminant of a binary quadratic form $f = ax^2 + bxy + cy^2$ is the quantity $d = b^2 - 4ac$.

Remark 3.2.2 Let $f = ax^2 + bxy + cy^2$. Then $4af(x, y) = (2ax + by)^2 - dy^2$.

Theorem 3.2.3 Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integral coefficients and discriminant d.

(a) If d is a square, then the equation $f(x, y) = 0$ has infinitely many solutions in $\mathbb{Z}$.

(b) If $d \neq 0$ and d is not a perfect square, then $a \neq 0, c \neq 0$, and the only solution of the equation $f(x, y) = 0$ in integers is given by $x = y = 0$.

Definition 3.2.4 (a) A form $f(x, y)$ is called indefinite if it takes on both positive and negative values.

(b) The form is called positive (or negative) semidefinite if $f(x, y) \geq 0$ (or $f(x, y) \leq 0$) for all integers x, y.

(c) A semidefinite form is called definite if in addition the only integers x, y for which $f(x, y) = 0$ are $x = 0, y = 0$.

Example 3.2.5 (a) $x^2 - 2y^2$ is indefinite. (b) $x^3 - 2xy + y^2$ is positive semidefinite. (c) $x^2 + y^2$ is positive definite.

Theorem 3.2.6 Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integral coefficients and discriminant d.

(a) If $d > 0$ then $f(x, y)$ is indefinite.

(b) If $d = 0$ then $f(x, y)$ is semidefinite but not definite.

(c) If $d < 0$ then a and c have the same sign and $f(x, y)$ is either positive definite or negative definite according as $a > 0$ or $a < 0$.

Theorem 3.2.7 Let $d \in \mathbb{Z}$. There exists at least one binary quadratic form in $\mathbb{Z}[x, y]$ with discriminant d, if and only if $d \equiv 0$ or $1 \pmod 4$.

Definition 3.2.8 (a) We say that a quadratic form $f(x, y)$ represents an integer n if there exist integers x_0 and y_0 such that $F(x_0, y_0) = n$.

(b) Such a representation is called proper if $(x_0, y_0) = 1$; otherwise it is improper.

Remark 3.2.9 The representations of n by f may be found by determining the proper representations of $\frac{n}{g^2}$ for those g such that $g^2|n$.

Theorem 3.2.10 Let n, d be integers with $n \neq 0$. There exists a binary quadratic form of discriminant d that represents n properly if and only if the congruence $x^2 \equiv d(\text{mod } 4|n|)$, has a solution.

Corollary 3.2.11 Suppose that $d \equiv 0$ or $1(\text{mod } 4)$. If p is an odd prime, then there is a binary quadratic form of discriminant d that represents p, if and only if $p|d$ or $\left(\frac{d}{p}\right) = 1$.

Theorem 3.2.12 Let $M = \begin{bmatrix} M_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ be a matrix with real entries and put $\begin{bmatrix} u \\ v \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix}$. The the following are equivalent:

(i) The linear transformation defines a permutation of lattice points;

(ii) the matrix M has integral coefficients and $\det(M) = \pm 1$.

Definition 3.2.13 (a) The group of 2×2 matrices with integral coefficients and determinants 1 is denoted by Γ, and is called the modular group.

(b) The quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are equivalent, and we write $f \sim g$, if there is an $M = [m_{ij}] \in \Gamma$ such that $g(x, y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. In this case we say that M takes f to g.

(c) Let $f = ax^2 + bxy + cy^2$. Let $F = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$. If $X = \begin{bmatrix} x \\ y \end{bmatrix}$, then $X^t F X = f(x, y)$. F is called the matrix associated with f.

Remark 3.2.14 Let f, g be binary quadratic forms and F, G be the matrices associated with F and G, respectively.

(a) If M takes f to g, then $M^t F M = G$. Moreover, if $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$, then $A = f(m_{11}, m_{12}), C = f(m_{21}, m_{22}), B = 2am_{11}m_{12} + 2cm_{21}m_{22} + b(m_{12}m_{21} + m_{11}m_{22})$.

(b) $f \sim g$ if and only if there exists $M \in \Gamma$ such that $M^t F M = G$.

(c) The relation $\sim$ is an equivalence relation.

Theorem 3.2.15 Let f and g be equivalent quadratic forms.

(a) For any given integers n, the representation of n by f are in one -to-one correspondence with the representation of n by g.

(b) Also, the proper representation of n by f are in one-to-one correspondence with the proper representation of n by g.

(c) The discriminant of f and g are equal.

Definition 3.2.16 Let f be a binary quadratic form whose discriminant d is not a perfect square.

(a) If d is not a square, we call f reduced if $-|a| < b \leq |a| < |c|$ or if $0 \leq b \leq |a| = |c|$.

(b) If d is a square, we call f reduced if $c = 0$ and $0 \leq a < |b|$.

Theorem 3.2.17 Let d be a given integer which is not a perfect square. Each equivalent class of binary quadratic forms of discriminant d contains at least one reduced form.

Example 3.2.18 Find a reduced form equivalent to the form $133x^2 + 108xy + 22y^2$.

Theorem 3.2.19 Let f be a reduced binary quadratic form whose discriminant d is not a perfect square.

(a) If f is indefinite, then $0 < |a| \leq \frac{1}{2}\sqrt{d}$

(b) If f is positive definite then $0 < a \leq \sqrt{\frac{-d}{3}}$.

(c) In either case, the number of reduce forms of a given nonsquare discriminant d is finite.

Definition 3.2.20 If d is not a perfect square then the number of equivalence classes of binary quadratic forms of discriminant d is called the class number of d, denoted $H(d)$.

Example 3.2.21 An odd prime p can be written in the form $p = ax^2 - 2y^2$ if and only if $p \equiv \pm 1 (\text{mod } 8)$.

Lemma 3.2.22 Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced positive definite form. If for some pair of integers x and y we have $(x, y) = 1$ and $f(x, y) \leq c$, then $f(x, y) = a$ or c, and the point (x, y) is one of the six points $\pm(1, 0), \pm(0, 1), \pm(1, -1)$. Moreover, the number of proper representation of a by f is

$$\begin{cases} 2 & \text{if } a \leq c, \\ 4 & \text{if } 0 \leq b < a = c, \\ 6 & \text{if } a = b = c. \end{cases}$$

Theorem 3.2.23 Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ be two equivalent reduced positive definite forms. Then $f = g$.

Definition 3.2.24 Let $f(x, y)$ be a positive definite binary quadratic form. A matrix $M \in \Gamma$ is called an automorph of f if M takes f into itself. The number of automorphs of f is denoted by $w(f)$.

Theorem 3.2.25 (a) Let f and g be equivalent positive definite binary quadratic forms. Then $w(f) = w(g)$, there are exactly $w(f)$ matrices that takes f to g, and there are exactly $w(g)$ matrices that takes g to f.

(b) The only values of $w(f)$ are 2,4,and 6. If f is reduced then

$$\begin{cases} w(f) = 4 & \text{if } a = c \text{ and } b = 0, \\ w(f) = 6 & \text{if } a = b = c, \\ w(f) = 2 & \text{otherwise.} \end{cases}$$