71-27,621

JAINCHELL, Richard Anthony, 1944-
ON THE REPRESENTATION OF INTEGERS BY INTEGRAL BINARY QUARTIC FORMS.

The University of Oklahoma, Ph.D., 1971
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED

Downloaded from SHAREOK. Persistent Handle URL: https://hdl.handle.net/11244/3057

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

ON THE REPRESENTATION OF INTEGERS BY INTEGRAL BINARY QUARTIC FORMS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

RICHARD ANTHONY JAINCHELL

NORMAN, OKLAHOMA

1971

ON THE REPRESENTATION OF INTEGERS BY

INTEGRAL BINARY QUARTIC FORMS

APPROVED BY

John C. Driscoll

George M. Ewing

Leonard R. Rubin

Irene Loewy

DISSERTATION COMMITTEE

ACKNOWLEDGMENT

I gratefully acknowledge the advice, assistance, and encouragement given to me by Dr. John C. Brixey during the preparation of this paper.

TABLE OF CONTENTS

		Page
INTRODUCTION		v
Chapter		
I.	SOME SUFFICIENCY CONDITIONS FOR SPECIAL BINARY FORMS TO BE POSITIVE AND RELATED RESULTS	1
II.	NECESSARY AND SUFFICIENT CONDITIONS FOR INTEGRAL BINARY QUADRATIC AND QUARTIC FORMS TO BE POSITIVE.	8
III.	SOME RESULTS ON THE INVARIANTS OF INTEGRAL BINARY QUARTIC FORMS.	13
IV.	THE INTEGRAL SOLUTIONS OF THE INTEGRAL BINARY QUARTIC EQUATION $f(x,y) = m$	18
V.	ON THE NUMBER OF REPRESENTATIONS OF INTEGERS BY BINARY FORMS	45
REFERENCES		56

ON THE REPRESENTATION OF INTEGERS BY INTEGRAL BINARY QUARTIC FORMS

INTRODUCTION

A binary form of degree n is an expression of the type

$$f(x,y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_o y^n.$$

If the coefficients a_i are integers (rational numbers), then f is said to be an integral (rational) form. If f is an integral (rational) form and $f(x,y) > 0$ for every pair of integers (rational numbers) $(x,y) \neq (0,0)$, then f is said to be a positive form (over the rationals).

In the first, second, and third chapters necessary and sufficient conditions are given for an integral binary quartic form to be positive.

Thue (1909) proved that the equation $g(x,y) = m$ has at most a finite number of integral solutions, where $g(x,y)$ denotes an integral binary form of degree at least three which is irreducible over the rationals and m is an integer. Recently, Baker [1] has improved Thue's result by showing that a bound can be found for the magnitude of the integral solutions of the equation $g(x,y) = m$.

In Chapter IV the complete solution in integers of the equation $f(x,y) = m$ is discussed, where $f(x,y)$ denotes an integral binary quartic form and m is an integer. Emphasis is placed on giving methods of solution which can be completed in a finite number of steps. Although the

author wanted to avoid using Baker's result in the discussion of the solution in integers of the equation $f(x,y) = m$, it was necessary to use the result when f is irreducible over the rationals and the zeros of f are four irrational numbers or two irrational numbers and two imaginary numbers.

In Chapter V Baker's result, mentioned above, is used to give a bound for the number of integral representations of an integer by an integral binary form of degree at least three which is irreducible over the rationals.

CHAPTER I

SOME SUFFICIENCY CONDITIONS FOR SPECIAL BINARY FORMS TO BE POSITIVE AND RELATED RESULTS

Theorem 1.1 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form. Suppose $4ae - bd = 0$. Then f is a positive form if and only if $a > 0$, $e > 0$, and $4cae - b^2e - d^2a > 0$.

Proof. Suppose f is a positive form. Then $0 < f(1,0) = a$ and $0 < f(0,1) = e$. Therefore $a \neq 0$ and $e \neq 0$, and consequently

$$f(x,y) = \frac{x^2}{4a}(2ax + by)^2 + \frac{y^2}{4e}(2ey + dx)^2 + \frac{x^2y^2}{4ae}(4cae - b^2e - d^2a). \tag{1.1}$$

Since $e \neq 0$ and $4ae - bd = 0$,

$$0 < f(2e,-d) = \frac{ed^2}{a}(4cae - b^2e - d^2a). \tag{1.2}$$

Since $\frac{ed^2}{a} > 0$, by inequality (1.2) $4cae - b^2e - d^2a > 0$.

Conversely, suppose $a > 0$, $e > 0$, and $4cae - b^2e - d^2a > 0$. Since $ae \neq 0$, equation (1.1) holds. Therefore for integers x and y, $f(x,y) \geq 0$ and $f(x,y) = 0$ implies $x = 0$ and $y = 0$. Hence f is a positive form. ||

Corollary 1.2 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form. If $a > 0$, $e > 0$, and $4cae - b^2e - d^2e > 0$, then f is a positive form.

Proof. This is an immediate consequence of the second part of the

proof of Theorem 1.1. ||

Lemma 1.3 Let $f(x,y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_o y^n$ with $n = 2^k$, $k \geq 3$. Define $a_n = a_n^{(2)}$ and $a_o = a_o^{(1)}$. Let $a_{n-4i}^{(1)}$, $a_{n-4i}^{(2)}$, $i = 1,\cdots,2^{k-2}-1$, be constants such that

$$a_{n-4i}^{(1)} + a_{n-4i}^{(2)} = a_{n-4i}. \tag{1.3}$$

Define $x^o = y^o = 1$ and $h_i^k = x^{n-4i}y^{4i-4}$, $i = 1,2,\cdots,2^{k-2}$. Then

$$f(x,y) = \sum_{i=1}^{2^{k-2}} h_i^k (a_{n-4(i-1)}^{(2)} x^4 + a_{n-4(i-1)-1}x^3y + \cdots + a_{n-4(i-1)-4}^{(1)} y^4). \tag{1.4}$$

Proof (by induction). For $k = 3$

$$f(x,y) = a_8^{(2)}x^8 + \cdots + a_5x^5y^3 + a_4^{(2)}x^4y^4 + a_4^{(1)}x^4y^4 + \cdots + a_o^{(1)}y^8$$

$$= x^4(a_8^{(2)}x^4 + \cdots + a_4^{(1)}y^4) + y^4(a_4^{(2)}x^4 + \cdots + a_o^{(1)}y^4).$$

Therefore equation (1.4) holds.

Assume the lemma holds for $n = 2^k$, $k \geq 3$. For $f(x,y) = a_{2k+1}x^{2^{k+1}} + \cdots + a_o y^{2^{k+1}}$ and constants $a_i^{(\ell)}$ satisfying equations (1.3) with $n = 2^{k+1}$, we have

$$f(x,y) = x^{2^k}(a_{2^{k+1}}^{(2)}x^{2^k} + \cdots + a_{2^k}^{(1)}y^{2^k}) + y^{2^k}(a_{2^k}^{(2)}x^{2^k} + \cdots + a_o^{(1)}y^{2^k}).$$

By the induction hypothesis

$$f(x,y) = x^{2^k}\sum_{i=1}^{2^{k-2}} h_i^k (a_{2^{k+1}-4(i-1)}^{(2)}x^4 + \cdots + a_{2^{k+1}-4(i-1)-4}^{(1)}y^4) \tag{1.5}$$

$$+ y^{2^k}\sum_{i=1}^{2^{k-2}} h_i^k (a_{2^k-4(i-1)}^{(2)}x^4 + \cdots + a_{2^k-4(i-1)-4}^{(1)}y^4).$$

Since $x^{2^k}h_i^k = h_i^{k+1}$ and $y^{2^k}h_j^k = h_{j+2^{k-2}}^{k+1}$ for $i,j = 1,2,\cdots,2^{k-2}$, by equation (1.5)

$$(1.6)\quad f(x,y) = \sum_{i=1}^{2^{k-2}} h_i^{k+1}\left(a^{(2)}_{2^{k+1}-4(i-1)}x^4 + \cdots + a^{(1)}_{2^{k+1}-4(i-1)-4}y^4\right)$$

$$+ \sum_{j=1}^{2^{k-2}} h_{j+2^{k-2}}^{k+1}\left(a^{(2)}_{2^k-4(j-1)}x^4 + \cdots + a^{(1)}_{2^k-4(j-1)-4}y^4\right).$$

For $i = j + 2^{k-2}$, $2^k - 4(j-1) = 2^{k+1} - 4(i-1)$. Then the second sum $\sum_{j=1}^{2^{k-2}}$ in equation (1.6) may be expressed as

$$(1.7)\quad \sum_{j=1}^{2^{k-2}} = \sum_{\substack{j=1\\ i=j+2^{k-2}}}^{2^{k-2}} h_i^{k+1}\left(a^{(2)}_{2^{k+1}-4(i-1)}x^4 + \cdots + a^{(1)}_{2^{k+1}-4(i-1)-4}y^4\right).$$

By equations (1.6) and (1.7)

$$f(x,y) = \sum_{i=1}^{2^{k-1}} h_i^{k+1}\left(a^{(2)}_{2^{k+1}-4(i-1)}x^4 + \cdots + a^{(1)}_{2^{k+1}-4(i-1)-4}y^4\right). \quad \|$$

Theorem 1.4 Let $f(x,y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_o y^n$ be an integral form with $n = 2^k$ and $k \geq 2$. Suppose $a_o = a_o^{(1)} > 0$ and $a_n = a_n^{(2)} > 0$. If there exist positive integers $a^{(1)}_{n-4i}$, $a^{(2)}_{n-4i}$, $i = \cdots, 2^{k-2}-1$, such that equations (1.3) hold, if

$$(1.8)\qquad A_i \equiv 4a_{n-4i-2} - \frac{a^2_{n-4i-1}}{a^{(2)}_{n-4i}} - \frac{a^2_{n-4i-3}}{a^{(1)}_{n-4i-4}} \geq 0$$

for $i = 0,1,\cdots,2^{k-2}-1$, and if for some i, say $i = j$, $A_j > 0$, then f is a positive form.

Proof. If $k = 2$, Theorem 1.4 reduces to Corollary 1.2. For $k \geq 3$ equation (1.4) holds by Lemma 1.3. If none of a_n, a_o, $a^{(2)}_{n-4i}$, $a^{(1)}_{n-4i}$, $i = 1,\cdots,2^{k-2}-1$, are zero, then

$$(1.9)\qquad f(x,y) = \sum_{i=1}^{2^{k-2}} h_i^k \left[\frac{x^2}{4a_{n-4i}^{(2)}} \left(2a_{n-4i}^{(2)}x + a_{n-4i-1}y\right)^2 + \frac{y^2}{4a_{n-4i-4}^{(1)}} \left(2a_{n-4i-4}^{(1)}y + a_{n-4i-3}x\right)^2 + \frac{x^2y^2}{4} A_i \right].$$

By hypothesis $A_i \geq 0$, $i = 0,1,\cdots,2^{k-2}-1$, and A_j, a_o, a_n, $a_{n-4i}^{(1)}$, $a_{n-4i}^{(2)}$, $i = 1,\cdots,2^{k-2}-1$, are positive. Then, by equation (1.9), $f(x,y) \geq 0$ for every pair of integers (x,y) and $f(x,y) = 0$ implies $x = y = 0$. Hence f is a positive form. ‖

Definition 1.5 An integral binary form f is said to properly represent 0 if there exist integers u and v not both zero such that $f(u,v) = 0$.

Theorem 1.6 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form with $a > 0$, $e > 0$, and $4cae - b^2e - d^2a = 0$. Then

(i) f properly represents 0 if and only if $4ae - bd = 0$,

and

(ii) f is a positive form if and only if $4ae - bd \neq 0$.

Proof. Since $a \neq 0$ and $e \neq 0$, equation (1.1) holds. Then

$$(1.10)\qquad f(x,y) = \frac{x^2}{4a}(2ax + by)^2 + \frac{y^2}{4e}(2ey + dx)^2$$

since $4cae - b^2e - d^2a = 0$.

If $4ae - bd = 0$, by equation (1.10) $f(2e,-d) = 0$. Since $(2e,-d) \neq (0,0)$, f properly represents zero.

Conversely, suppose $f(u,v) = 0$ where u and v are integers and $(u,v) \neq (0,0)$. Then by equation (1.10) $uv \neq 0$, and consequently $2au + bv = 2ev + du = 0$. Since $uv \neq 0$, $4ae - bd = 0$. This completes the proof of (i).

If f is a positive form, then f does not properly represent zero. Then by conclusion (i) $4ae - bd \neq 0$.

If $4ae - bd \neq 0$, by conclusion (i) f does not properly represent 0. By equation (1.10) $f(x,y) \geq 0$ for every pair of integers (x,y). Hence f is a positive form. ‖

Definition 1.7 Let f be an integral binary form. A pair (u,v) is said to be a solution of the equation $f(x,y) = m$, m an integer, if u and v are integers and $f(u,v) = m$.

Corollary 1.8 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral binary form with $a > 0$, $e > 0$, and $4cae - b^2e - d^2a = 0$. Then the equation $f(x,y) = 0$ has infinitely many solutions if $4ae - bd = 0$ and (0,0) is the only solution if $4ae - bd \neq 0$.

Proof. If $4ae - bd \neq 0$, then by conclusion (ii) of Theorem 1.6 f is a positive form. Therefore (0,0) is the only solution of the equation $f(x,y) = 0$.

If $4ae - bd = 0$, then by the proof of Theorem 1.6 $f(2e,-d) = 0$. Clearly $f(2et,-dt) = 0$ for every integer t. Since $e \neq 0$, the equation $f(x,y) = 0$ has infinitely many solutions. ‖

Theorem 1.9 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form with $a > 0$, $e > 0$, and $4cae - b^2e - d^2a \geq 0$. Then the equation

$$f(x,y) = m, \tag{1.11}$$

where m is a nonzero integer, has at most a finite number of solutions and the solutions (if any) can be found in a finite number of steps.

Proof. Equation (1.1) holds and has no solution when m is negative. For $m > 0$ let (u,v) be a solution of equation (1.11).

Suppose $4cae - b^2e - d^2a > 0$. Then from equation (1.1) it follows that

$$0 \leq u^2v^2(4cae - b^2e - d^2a) \leq 4am.$$

If $u = 0$, $ev^4 = m$. If $v = 0$, $au^4 = m$. For this case the desired conclusions now follow.

Suppose $4cae - b^2e - d^2a = 0$. Then equation (1.10) holds. If $u = 0$, $ev^4 = m$. If $v = 0$, $au^4 = m$. If $2au + bv = 0$, then $u = -\frac{b}{2a}v$ and

$$v^4(4ae - bd)^2 = 16a^2em.$$

If $2ev + du = 0$, $v = -\frac{d}{2e}u$ and

$$u^4(4ae - bd)^2 = 16ae^2m.$$

If $u \neq 0$, $v \neq 0$, $2au + bv \neq 0$, and $2ev + du \neq 0$, then

$$0 < u^2(2au + bv)^2 < 4am$$

and

$$0 < v^2(2ev + du)^2 < 4em.$$

Thus $0 < u^2 < 4am$ and $0 < v^2 < 4em$. The desired conclusions are now immediate. ||

Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form with $a \neq 0$. The transformation $x = u - \frac{b}{4a}v$, $y = v$ carries $f(x,y)$ into the form

$$g(u,v) = au^4 + v^2(Au^2 + Buv + Cv^2),$$

where

$$A = c - \frac{3b^2}{8a},$$

$$B = d - \frac{bc}{2a} + \frac{b^3}{8a^2},$$

$$C = e - \frac{bd}{4a} + \frac{b^2c}{16a^2} - \frac{3b^4}{256a^3}.$$

Since $\begin{vmatrix} 1 & -\frac{b}{4a} \\ 0 & 1 \end{vmatrix} \neq 0$, the forms f and g are equivalent over the field of rational numbers. Then f is a positive form if g is a positive form over the rationals. If $a > 0$, $C > 0$, and $4AC - B^2 \geq 0$, then g is a positive form over the rationals since

$$g(u,v) = au^4 + \frac{v^2}{4C}\left[(2Cv + Bu)^2 + (4AC - B^2)u^2\right].$$

Therefore we have the following result.

Theorem 1.10 If $a > 0$, $C > 0$, $4AC - B^2 \geq 0$, then f is a positive form. ‖

Theorem 1.11 Let $h(x,y) = Dx^{2k} + Ex^2y^2 + Fxy^3 + Gy^4$ be a rational form with $k > 2$. Suppose $F \neq 0$. Then h is a positive form over the rationals if and only if $D > 0$, $G > 0$, and $4EG - F^2 \geq 0$.

Proof. If $D > 0$, $G > 0$, and $4EG - F^2 \geq 0$, then h is a positive form over the rationals since

$$h(x,y) = Dx^{2k} + \frac{y^2}{4G}\left[(2Gy + Fx)^2 + (4EG - F^2)x^2\right].$$

Therefore suppose h is a positive form over the rationals. Then $D = h(1,0) > 0$ and $G = h(0,1) > 0$. If x is a nonzero rational number,

$$h\left(x, \frac{-Fx}{2G}\right) = x^4\left[Dx^{2k-4} + \frac{F^2}{16G^3}(4EG - F^2)\right] > 0.$$

Thus $4EG - F^2 \geq 0$ since $\frac{F^2}{16G^3} > 0$. ‖

CHAPTER II

NECESSARY AND SUFFICIENT CONDITIONS FOR INTEGRAL BINARY QUADRATIC AND QUARTIC FORMS TO BE POSITIVE

Theorem 2.1 Let $f(x,y) = a_{2n}x^{2n} + a_{2n-1}x^{2n-1}y + \cdots + a_0y^{2n}$ be an integral form. Define $g(z) = a_{2n}z^{2n} + a_{2n-1}z^{2n-1} + \cdots + a_0$. Then f is a positive form if and only if $a_{2n} > 0$ and $g(z) > 0$ for every rational value of z.

Proof. Suppose f is a positive form. Then for $y \neq 0$

$$0 < \frac{f(x,y)}{y^{2n}} = g(\frac{x}{y}).$$

Thus $g(z) > 0$ for every rational value of z. Since $f(1,0) = a_{2n}$, $a_{2n} > 0$.

Conversely, suppose $a_{2n} > 0$ and $g(z) > 0$ whenever z is a rational number. For integers x and $y(\neq 0)$

$$0 < y^{2n}g(\frac{x}{y}) = f(x,y). \tag{2.1}$$

Now $f(x,0) = a_{2n}x^{2n}$. Therefore $f(x,y) \geq 0$ for every pair of integers (x,y). By inequality (2.1) it is impossible for $f(x,y) = 0$ and $y \neq 0$. Thus $f(x,y) = 0$ implies $y = 0$, and consequently $a_{2n}x^{2n} = 0$. Since $a_{2n} > 0$, $x = 0$. Hence f is a positive form. ‖

Theorem 2.2 Let $f(x,y) = ax^2 + bxy + cy^2$ be an integral form.

Define $g(z) = az^2 + bz + c$. Then f is a positive form if and only if there exist a rational number α and a real number $\beta(\neq 0)$ such that $b = -2a\alpha$ and $c = a(\alpha^2 + \beta^2)$.

Proof. Suppose $a > 0$, $b = -2a\alpha$, and $c = a(\alpha^2 + \beta^2)$, where α is a rational number and $\beta(\neq 0)$ is a real number. Then

$$g(z) = a[z - (\alpha+\beta i)][z - (\alpha - \beta i)].$$

Since $\beta \neq 0$, g has no real zeros. Then $g(z) > 0$ for all real values of z since $a > 0$. Hence f is a positive form by Theorem 2.1.

Conversely, suppose f is a positive form. Then $0 < f(1,0) = a$. There exist complex numbers α_1 and α_2 such that

$$g(z) = a(z-\alpha_1)(z-\alpha_2).$$

If α_1 and α_2 are real numbers and not equal, there exists a rational number α_3 between α_1 and α_2. Then $g(\alpha_3) < 0$. This is impossible by Theorem 2.1. Therefore, suppose α_1 and α_2 are equal real numbers. By Theorem 2.1 α_1 is not a rational number. Now α_1 is not an irrational number since $\frac{b}{a} = -2\alpha_1$. Thus g has no real zeros. Therefore, let $\alpha_1 = \alpha + \beta i$ and $\alpha_2 = \alpha - \beta i$ where α and $\beta(\neq 0)$ are real numbers. Then $c = a(\alpha^2 + \beta^2)$ and $b = -2a\alpha$ which implies α is a rational number. ‖

As a corollary to Theorems 2.1 and 2.2 we have the familiar

Theorem 2.3 Let $f(x,y) = ax^2 + bxy + cy^2$ be an integral form. Then f is a positive form if and only if $a > 0$ and $b^2 - 4ac < 0$.

Proof. Suppose f is a positive form. By Theorem 2.2 $a > 0$, $b = -2a\alpha$, and $c = a(\alpha^2 + \beta^2)$, where α is a rational number and $\beta(\neq 0)$ is a real number. Then $b^2 - 4ac = -4a^2\beta^2$. Since $a\beta \neq 0$, $b^2 - 4ac < 0$.

Conversely, suppose $a > 0$ and $b^2 - 4ac < 0$. Define $g(z) = az^2 + bz + c$.

Since $a \neq 0$ and $b^2 - 4ac < 0$, g has no real zeros. Then $g(z) > 0$ for every real value of z since $a > 0$. Hence f is a positive form by Theorem 2.1. ‖

Lemma 2.4 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form. Define $g(z) = az^4 + bz^3 + cz^2 + dz + e$. If f is a positive form, then g cannot have two real and two imaginary zeros.

Proof (by contradiction). Suppose g has two real zeros γ, δ and two imaginary zeros $\alpha \pm \beta i$, where α and $\beta (\neq 0)$ are real numbers. Since f is a positive form, by Theorem 2.1 γ and δ are irrational numbers. Now

$$g(z) = a[z-\gamma][z-\delta][z-(\alpha+\beta i)][z-(\alpha-\beta i)].$$

Since $f(1,0) = a$, $a > 0$. Then $a[z-(\alpha+\beta i)][z-(\alpha-\beta i)] > 0$ for every real value of z since $a > 0$ and $\alpha + \beta i$ and $\alpha - \beta i$ are imaginary numbers. If $\gamma \neq \delta$, then there exists a real number r between γ and δ. Then $g(r) < 0$. But this is impossible by Theorem 2.1.

Suppose $\gamma = \delta$. Since $\beta \neq 0$ and γ is an irrational number, g is reducible over the rationals if and only if $(z-\gamma)^2$ and $[z-(\alpha+\beta i)][z-(\alpha-\beta i)]$ are rational polynomials. Then g is irreducible over the rationals since $(z-\gamma)^2 = z^2 - 2\gamma z + \gamma^2$ is not a rational polynomial. Therefore $g(z)/a$ is a monic irreducible polynomial over the rationals, and it has been shown [3], page 192, that g(z) has no multiple zeros. Thus it is impossible that $\gamma = \delta$. ‖

Theorem 2.5 Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form. Define $g(z) = az^4 + bz^3 + cz^2 + dz + e$. Then f is positive form if and only if $a > 0$ and the zeros of g are either

Case I four imaginary numbers, or

Case II four irrational numbers α_1, α_2, α_3, α_4 with $\alpha_1 = \alpha_2$, $\alpha_3 = \alpha_4$,

and $\alpha_1 \neq \alpha_3$.

Proof. The necessity part of the theorem is a consequence of Theorem 2.1. For Case I $g(z) > 0$ for every real value of z since all the zeros of g are imaginary and $a > 0$. For Case II g may be expressed in the form

$$g(z) = a(z-\alpha_1)^2(z-\alpha_3)^2.$$

Since $a > 0$ and α_1 and α_3 are irrational numbers, $g(z) > 0$ for every rational value of z. Hence in each case f is a positive form by Theorem 2.1.

Conversely, suppose f is a positive form. Then $a = f(1,0) > 0$. If g has four imaginary zeros, then Case I holds. If g does not have four imaginary zeros, then the zeros of g are four irrational numbers by Theorem 2.1 and Lemma 2.4.

Suppose g has four irrational zeros α_1, α_2, α_3, α_4. Then

$$g(z) = a(z-\alpha_1)(z-\alpha_2)(z-\alpha_3)(z-\alpha_4).$$

If no two of the α_i's are equal, there exists a rational number r such that $g(r) < 0$. (If $\alpha_1 < \alpha_2 < \alpha_3 < \alpha_4$, let r be a rational number between α_3 and α_4. The other cases follow in a similar manner.) However this is impossible by Theorem 2.1. Therefore at least two of the α_i's are equal, say $\alpha_1 = \alpha_2$. If $\alpha_3 \neq \alpha_4$, $\alpha_3 \neq \alpha_1$, and $\alpha_4 \neq \alpha_1$, then again there exists a rational number r such that $g(r) < 0$. But this is impossible. Therefore $\alpha_3 = \alpha_1$, $\alpha_3 = \alpha_4$, or $\alpha_4 = \alpha_1$. If $\alpha_3 = \alpha_4$ and $\alpha_3 \neq \alpha_1$, then Case II holds. If $\alpha_3 = \alpha_4 = \alpha_1$, then $g(z) = a(z-\alpha_1)^4$ which implies $b = -4a\alpha_1$. This is impossible since b and $a(\neq 0)$ are integers. Thus $\alpha_3 = \alpha_4 = \alpha_1$ is impossible. Therefore, if $\alpha_3 = \alpha_1$ or $\alpha_4 = \alpha_1$, then $\alpha_3 \neq \alpha_4$. If $\alpha_3 = \alpha_1$

and $\alpha_3 \neq \alpha_4$, $g(z) = a(z-\alpha_1)^3(z-\alpha_4)$. Then there exists a rational number r such that $g(r) < 0$. Again this is impossible. Similarly $\alpha_4 = \alpha_1$ and $\alpha_3 \neq \alpha_4$ cannot hold. Hence Case II holds if g has four irrational zeros. ‖

Since the zeros of a fourth degree polynomial can be found in a finite number of steps and the nature of the zeros can easily be determined, by Theorem 2.5 only a finite number of steps is required to determine if an integral binary quartic form is positive.

CHAPTER III

SOME RESULTS ON THE INVARIANTS OF INTEGRAL BINARY QUARTIC FORMS

Let $f(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$, where a, 4b, 6c, 4d, e are integers. It has been shown [8], page 139, that two invariants of f are

$$I = ae - 4bd + 3c^2$$

and

$$J = \begin{vmatrix} a & b & c \\ b & c & d \\ c & d & e \end{vmatrix} .$$

Theorem 3.1 If $f(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$ is a positive integral form, then $I > 0$.

Proof. Suppose f is a positive integral form. By Theorem 2.5 let the zeros of $f(z,1)$ be $\alpha_1 + \beta_1 i$, $\alpha_1 - \beta_1 i$, $\alpha_2 + \beta_2 i$, $\alpha_2 - \beta_2 i$, where

(i) α_1, α_2, β_1, β_2 are real numbers and $\beta_1\beta_2 \neq 0$, or

(ii) $\beta_1 = \beta_2 = 0$ and α_1 and α_2 are unequal irrational numbers.

In each case we have

$$4b = -2a(\alpha_1 + \alpha_2),$$

$$6c = a(\alpha_1^2 + \alpha_2^2 + 4\alpha_1\alpha_2 + \beta_1^2 + \beta_2^2),$$

$$4d = -2a(\alpha_1^2\alpha_2 + \alpha_1\alpha_2^2 + \alpha_1\beta_2^2 + \alpha_2\beta_1^2),$$

$$e = a(\alpha_1^2\alpha_2^2 + \alpha_1^2\beta_2^2 + \alpha_2^2\beta_1^2 + \beta_1^2\beta_2^2).$$

Then

$$I = \frac{a^2}{12}\,[(\alpha_1-\alpha_2)^4 + \beta_1^4 + 14\beta_1^2\beta_2^2 + \beta_2^4 + 2\beta_1^2(\alpha_1-\alpha_2)^2 + 2\beta_2^2(\alpha_1-\alpha_2)^2].$$

It is clear that in each case $I > 0$. ‖

Theorem 3.2 If $f(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$ is a positive integral form and Case II of Theorem 2.5 holds, then $J < 0$.

Proof. Suppose f is a positive integral form. As in the proof of Theorem 3.1 let the zeros of $f(z,1)$ be $\alpha_1 + \beta_1 i$, $\alpha_1 - \beta_1 i$, $\alpha_2 + \beta_2 i$, $\alpha_2 - \beta_2 i$. Then

$$(3.1)\qquad J = -\frac{a^3}{216}\,[(\alpha_1-\alpha_2)^6 + 3\beta_1^2(\alpha_1-\alpha_2)^4 + 3\beta_2^2(\alpha_1-\alpha_2)^4 + 3\beta_1^4(\alpha_1-\alpha_2)^4 + 3\beta_2^4(\alpha_1-\alpha_2)^2 + \beta_1^6 + \beta_2^6 - 30\,\beta_1^2\beta_2^2(\alpha_1-\alpha_2)^2 - 33\,\beta_1^2\beta_2^2(\beta_1^2 + \beta_2^2)].$$

If Case II of Theorem 2.5 holds, $\alpha_1 \neq \alpha_2$ and $\beta_1 = \beta_2 = 0$. In this case the quantity inside the brackets in equation (3.1) is positive, and consequently $J < 0$. ‖

Theorem 3.3 If $f(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$ is a positive integral form, then $I^3 - 27J^2 \geq 0$.

Proof. Let α, β, γ, δ denote the zeros of the polynomial $f(z,1)$. It has been shown [2], page 142, that

$$256(I^3-27J^2) = a^6(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2(\alpha-\delta)^2(\beta-\delta)^2(\gamma-\delta)^2.$$

If f is a positive integral form, then with the aid of Theorem 2.5 one can easily verify that $I^3 - 27J^2 \geq 0$. ‖

Theorem 3.4 Let $f(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$ be an

integral form with $a > 0$, $H \equiv ac - b^2 > 0$, and $J > 0$. Then

(i) f is a positive form,

(ii) the equation $f(x,y) = m$, m an integer, has at most a finite number of solutions,

(iii) the solutions (if any) of the equation $f(x,y) = m$ can be found in a finite number of steps, and

(iv) only a finite number of steps is required to find the smallest positive integer represented by f.

Proof. By hypothesis a, H, and J are positive. Under these conditions it has been shown [2], page 126, that all zeros of $f(z,1)$ are imaginary. Then f is a positive form.

Define the polynomial g_y by

$$(3.2) \qquad \begin{aligned} g_y(x) &\equiv f(x,y) - m \\ &= ax^4 + 4(by)x^3 + 6(cy^2)x^2 + 4(dy^3)x + ey^4 - m \\ &\equiv ax^4 + 4b'x^3 + 6c'x^2 + 4d'x + e'. \end{aligned}$$

Now

$$(3.3) \qquad H_y \equiv ac' - (b')^2 = Hy^2$$

and

$$(3.4) \qquad J_y \equiv \begin{vmatrix} a & b' & c' \\ b' & c' & d' \\ c' & d' & e' \end{vmatrix} = y^2(y^4J - Hm).$$

Suppose s and t are integers such that $f(s,t) = m$. If $t = 0$, $as^4 = m$, and consequently there are at most two integral values of x such that $f(x,0) = m$. Therefore suppose $t \neq 0$. Then by equation (3.3) $H_t > 0$ since $H > 0$. It may be shown [2], page 126, that if $J_t > 0$, $H_t > 0$, and $a > 0$, then g_t has no real zeros. But $g_t(s) = 0$ and s is an integer.

Therefore $J_t \leq 0$, and by equation (3.4) $t^4 J - Hm \leq 0$. Then

$$0 < t^4 \leq \frac{Hm}{J} \tag{3.5}$$

since $J > 0$. Now s is zero or a divisor of the first of the terms $et^4 - m$, $4dt^3$, $6ct^2$, $4bt$ which is not zero. (Note that $d = c = b = 0$ cannot hold since in this case $J = 0$ which is contrary to hypothesis. Therefore at least one of the terms $et^4 - m$, $4dt^3$, $6ct^2$, $4bt$ is not zero.) Thus

$$0 \leq |s| \leq \max\{|et^4 - m|, |4dt^3|, |6ct^2|, |4bt|\}. \tag{3.6}$$

Conclusions (ii) and (iii) follow from inequalities (3.5) and (3.6).

Since $f(1,0) = a > 0$, an integral pair (s,t) which furnishes a positive integral minimum for f satisfies either

$$t = 0 \quad \text{and} \quad s = 1$$

or

$$0 < t^4 \leq \frac{H}{J} f(s,t) \leq \frac{H}{J} a$$

and s = 0 or s is a divisor of the first of the terms $et^4 - f(s,t)$, $4dt^3$, $6ct^2$, $4bt$ which is not zero. Thus

$$0 \leq t^4 \leq \frac{H}{J} a$$

and

$$0 \leq |s| \leq \max\{|ae\tfrac{H}{J}| + a, |4ad\tfrac{H}{J}|, |6ac\tfrac{H}{J}|, |4ab\tfrac{H}{J}|\}.$$

Conclusion (iv) is now immediate. ‖

Corollary 3.5 Let $f(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$ be an integral form with $e > 0$, $ec - d^2 > 0$, and $J > 0$. Then the conclusions of Theorem 3.4 hold.

Proof. Define the form h by $h(x,y) = f(y,x)$. Then h is equivalent to f. Therefore the conclusions of Theorem 3.4 hold for f if and only if they hold for h. Now

$$0 < J = \begin{vmatrix} e & d & c \\ d & c & b \\ c & b & a \end{vmatrix} \equiv L.$$

Since e, $ec - d^2$, and L are positive, the conclusions of Theorem 3.4 hold for h. Therefore they hold for f. ‖

CHAPTER IV

THE INTEGRAL SOLUTIONS OF THE INTEGRAL BINARY QUARTIC EQUATION $f(x,y) = m$

Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral form. Any reference to the form f in this chapter will mean the form f defined above. The complete integral solution of the equation

$$f(x,y) = m, \tag{4.1}$$

where m is an integer, will be discussed. By a solution of equation (4.1) we mean an integral solution.

Definition 4.1 If g is an integral binary form, then g is reducible over the rationals if and only if there exist rational binary forms h and ℓ of positive degree such that $g(x,y) = h(x,y)\ell(x,y)$.

Definition 4.2 If $g(x,1)$ denotes the polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_o$, then

$$g(x,y) \equiv a_nx^n + a_{n-1}x^{n-1}y + \cdots + a_oy^n.$$

Theorem 4.3 If $g(x,1)$ is an integral polynomial, then $g(x,1)$ is reducible over the rationals if and only if $g(x,y)$ is reducible over the rationals.

Proof. If $g(x,1)$, $h(x,1)$, $\ell(x,1)$ are polynomials of positive degree in one indeterminate, then it is clear that $g(x,1) = h(x,1)\ell(x,1)$ if and only if $g(x,y) = h(x,y)\ell(x,y)$. ‖

Theorem 4.4 Let the zeros of $f(x,1)$ be α_1, α_2, α_3, α_4. Then $f(x,y)$ is reducible over the rationals if and only if for some permutation (i,j,k,ℓ) of the integers 1,2,3,4 $(x-\alpha_i)(x-\alpha_j)$ and $(x-\alpha_k)(x-\alpha_\ell)$ are rational polynomials or $(x-\alpha_i)$ and $(x-\alpha_j)(x-\alpha_k)(x-\alpha_\ell)$ are rational polynomials.

Proof. This follows from Theorem 4.3 and from the fact that every complex fourth degree polynomial has exactly four zeros. ‖

Theorem 4.5 Let $g(x,1)$ be an integral third degree polynomial with zeros α_1, α_2, and α_3. Then $g(x,y)$ is reducible over the rationals if and only if for some permutation (i,j,k) of the integers 1,2,3 $x-\alpha_i$ and $(x-\alpha_j)(x-\alpha_k)$ are rational polynomials.

Proof. This is immediate by Theorem 4.3 and from the fact that every third degree polynomial has exactly three zeros. ‖

A theorem of Baker [1], page 174, which we will need is

Theorem 4.6 Let $g(x,y)$ denote a homogeneous polynomial in x, y of degree $n \geq 3$ with integral coefficients, irreducible over the rationals. Suppose that $k > n+1$ and let m be any positive integer. Then all solutions of the equation $g(x,y) = m$ in integers x, y satisfy

$$\max(|x|,|y|) < c\, e^{(\log m)^k},$$

where c is an effectively computable number depending only on n, k, and the coefficients of g. ‖

The phrase "c is an effectively computable number" means that c can be found in a finite number of steps.

If $m = 0$ and $g(x,y)$ is irreducible over the rationals, then $x = 0$, $y = 0$ is the only solution of the equation $g(x,y) = 0$.

An immediate consequence of Theorem 4.6 is

Corollary 4.7 Let $g(x,y)$ denote a homogeneous polynomial in x, y of degree $n \geq 3$ with integral coefficients, irreducible over the rationals. Suppose $k > n+1$ and let m be any negative integer. Then all solutions of the equation $g(x,y) = m$ in integers x, y satisfy

$$\max(|x|,|y|) < c\, e^{[\log(-m)]^k},$$

where c is an effectively computable number depending only on n, k, and the coefficients of $-g$. ‖

The zeros of polynomials of degree at most four can be found in a finite number of steps. This fact will be used implicitly throughout the remainder of this chapter. For rational polynomials of degree at most four it is easy to determine if the zeros are imaginary, rational, or irrational numbers.

The solution of equation (4.1) with $m = 0$ will now be given. Without loss of generality we may assume that at least one of the coefficients of f is not zero. Suppose a or e is not zero, say $a \neq 0$. Then let α_1, α_2, α_3, α_4 be the zeros of $f(x,1)$. Therefore

$$f(x,y) = a(x-\alpha_1 y)(x-\alpha_2 y)(x-\alpha_3 y)(x-\alpha_4 y). \tag{4.2}$$

The trivial solution of

$$f(x,y) = 0 \tag{4.3}$$

is $(x,y) = (0,0)$. By equation (4.2) equation (4.3) has a nontrivial solution if and only if at least one of the zeros is a rational number. Suppose this is the case and let $\alpha_1,\cdots,\alpha_j$ be rational numbers. Thus $\alpha_i = p_i/q_i$, $1 \leq i \leq j$, where p_i (possibly zero) and q_i are relatively prime integers. Therefore $(x,y) = (p_i t, q_i t)$ is a solution of equation (4.3) for each integer t. These values for x and y are the only

solutions of equation (4.3).

Suppose $a = e = 0$ and b or d is not zero, say $b \neq 0$. Then there exist complex numbers β_1 and β_2 such that

$$f(x,y) = bxy(x - \beta_1 y)(x - \beta_2 y).$$

Clearly $(x,y) = (0,t)$ and $(x,y) = (t,0)$, t an integer, are solutions of equation (4.3). Now the form $(x - \beta_1 y)(x - \beta_2 y)$ properly represents zero if and only if β_1 and β_2 are rational numbers.

Suppose this is the case. Then $\beta_i = p_i/q_i$, $1 \leq i \leq 2$, where p_i (possibly zero) and q_i are relatively prime integers. Therefore $(x,y) = (p_i t, q_i t)$, $i = 1,2$, are solutions of the equation $(x-\beta_1 y)(x-\beta_2 y) = 0$ for each integer t. These solutions are the only solutions of this equation.

If $a = b = d = e = 0$, then $c \neq 0$ by hypothesis and $f(x,y) = cx^2y^2$. Then $(x,y) = (0,t)$ and $(x,y) = (t,0)$, t any integer, are the solutions of equation (4.3).

We now discuss the solution of equation (4.1) with $m \neq 0$. Suppose $a = e = 0$. Then for a solution (u,v) of the equation

$$f(x,y) = m(\neq 0), \tag{4.4}$$

$uv|m$. Therefore u and v are divisors of m. Equation (4.4) has at most a finite number of solutions and the solutions (if any) can be found in a finite number of steps.

Suppose a or e is not zero. Without loss of generality we may assume $a \neq 0$. Also we may assume $a > 0$ since $f(u,v) = m$ if and only if $-f(u,v) = -m$.

Theorem 4.8 If f is a positive form and Case I of Theorem 2.5

holds, then equation (4.4) has at most a finite number of solutions, and the solutions (if any) can be found in a finite number of steps.

Proof. Suppose f is a positive form and Case I of Theorem 2.5 holds. Therefore let $\alpha_1 + \beta_1 i$, $\alpha_1 - \beta_1 i$, $\alpha_2 + \beta_2 i$, $\alpha_2 - \beta_2 i$ be the zeros of $f(z,1)$, where α_j and β_j are real numbers and $\beta_1\beta_2 \neq 0$. Then

$$(4.5) \quad f(x,y) = a[(x-\alpha_1 y)^2(x-\alpha_2 y)^2 + \beta_1^2 y^2(x-\alpha_2 y)^2 + \beta_2^2 y^2(x-\alpha_1 y)^2 + \beta_1^2\beta_2^2 y^4],$$

and

$$(4.6) \quad f(x,y) = \frac{a}{(\alpha_1^2+\beta_1^2)(\alpha_2^2+\beta_2^2)}\left\{\left[(\alpha_1^2+\beta_1^2)y - \alpha_1 x\right]^2\left[(\alpha_2^2+\beta_2^2)y - \alpha_2 x\right]^2\right.$$

$$\left. + \beta_1^2 x^2\left[(\alpha_2^2+\beta_2^2)y - \alpha_2 x\right]^2 + \beta_2^2 x^2\left[(\alpha_1^2+\beta_1^2)y - \alpha_1 x\right]^2 + \beta_1^2\beta_2^2 x^4\right\}.$$

If $f(u,v) = m$, then by equations (4.5) and (4.6)

$$(4.7) \quad 0 \leq v^4 \leq \frac{m}{a\beta_1^2\beta_2^2}$$

and

$$(4.8) \quad 0 \leq u^4 \leq \frac{(\alpha_1^2+\beta_1^2)(\alpha_2^2+\beta_2^2)m}{a\beta_1^2\beta_2^2}.$$

Since inequalities (4.7) and (4.8) restrict u and v to a finite number of integral values, the desired conclusions follow. |

Conclusion (i) of Theorem 3.4 was proved first in the proof of Theorem 3.4. In the proof of conclusion (i) of Theorem 3.4 it was pointed out that all the zeros of $f(z,1)$ are imaginary. Therefore the proof of Theorem 4.8 could have been used to prove the remaining conclusions of Theorem 3.4.

Theorem 4.9 If f is a positive form and Case II of Theorem 2.5

holds, then equation (4.4) has infinitely many solutions if it has a solution.

Proof. Suppose f is a positive form and Case II of Theorem 2.5 holds. Then there exist unequal irrational numbers α_1 and α_2 such that

$$\begin{aligned} b &= -2a(\alpha_1 + \alpha_2), \\ c &= a(\alpha_1^2 + \alpha_2^2 + 4\alpha_1\alpha_2) = a(\frac{b^2}{4a^2} + 2\alpha_1\alpha_2), \\ d &= -2a(\alpha_1 + \alpha_2)\alpha_1\alpha_2 = b\alpha_1\alpha_2, \\ e &= a\alpha_1^2\alpha_2^2. \end{aligned} \tag{4.9}$$

Suppose b = 0. Then $c = -2a\alpha_1^2$ and $e = a\alpha_1^4$. Therefore

$$f(x,y) = ax^4 - 2a\alpha_1^2x^2y^2 + a\alpha_1^4y^4, \tag{4.10}$$

and

$$4af(x,y) = (2ax^2 - 2a\alpha_1^2y^2)^2. \tag{4.11}$$

Define $D_1 = 2a\alpha_1^2$ and $D_2 = 4a^2\alpha_1^2$. Since $c = -2a\alpha_1^2$ and α_1 is an irrational number, D_2 is a positive integer. D_2 is not a perfect square since $4a^2\alpha_1^2 = k^2$, k an integer, implies $\alpha_1 = \pm k/2a$ which implies α_1 is a rational number.

If (x,y) is a solution of equation (4.4), then there exists an integer n such that $n^2 = 4am$ and

$$2ax^2 - D_1y^2 = n. \tag{4.12}$$

Clearly equation (4.4) has infinitely many solutions if equation (4.12) has infinitely many solutions.

Assume (x_o,y_o) is a solution of equation (4.4). Then equation (4.12) holds with $(x,y) = (x_o,y_o)$ and some integer n such that $n^2 = 4am$. Now

D_2 is a positive integer which is not a perfect square. It may be shown [6] that there exist infinitely many distinct integers p_i and infinitely many distinct integers q_i, $i = 1,2,\cdots$, such that

$$p_i^2 - D_2 q_i^2 = 1.$$

Define for $i = 1,2,\cdots$

$$x_i = x_o p_i + y_o q_i D_1$$

and

$$y_i = 2ax_o q_i + y_o p_i.$$

Then

$$2ax_i^2 - D_1 y_i^2 = (2ax_o^2 - D_1 y_o^2)(p_i^2 - D_2 q_i^2) = n,$$

and consequently (x_i,y_i) is a solution of equation (4.12).

Suppose $(x_i,y_i) = (x_j,y_j)$ with $i \neq j$. Then $p_i \neq p_j$ and $q_i \neq q_j$. Since $x_i = x_j$ and $y_i = y_j$,

$$x_o(p_i - p_j) = y_o D_1 (q_j - q_i) \tag{4.13}$$

and

$$2ax_o(q_i - q_j) = y_o(p_j - p_i). \tag{4.14}$$

Then $x_o \neq 0$ since $x_o = 0$ implies $y_o(p_j - p_i) = 0$ which implies $y_o = 0$. This implies $n = 0$ which is impossible. Therefore by equations (4.13) and (4.14)

$$x_o(p_i - p_j) = \frac{y_o^2}{2ax_o} D_1 (p_i - p_j)$$

which implies $2ax_o^2 - D_1 y_o^2 = 0$. This is impossible since $n \neq 0$. Thus $(x_i,y_i) \neq (x_j,y_j)$ if $i \neq j$. Hence there are infinitely many pairs of integers (x_i,y_i) such that $f(x_i,y_i) = m$ if $b = 0$ and equation (4.4) has

a solution.

We now consider the case $b \neq 0$. By equations (4.9)

$$c = \frac{b^3 + 8a^2d}{4ab} \quad \text{and} \quad e = \frac{ad^2}{b^2}.$$

Therefore

$$4ab^2 f(x,y) = (2abx^2 + b^2xy + 2ady^2)^2 \tag{4.15}$$
$$= \left\{\frac{1}{8ab}\left[(4abx + b^2y)^2 - (b^4 - 16a^2bd)y^2\right]\right\}^2.$$

Define $D_3 = b^4 - 16a^2bd$. Since $b = -2a(\alpha_1 + \alpha_2)$ and $d = b\alpha_1\alpha_2$,

$$D_3 = 4a^2b^2(\alpha_1 - \alpha_2)^2 \tag{4.16}$$

and

$$\alpha_i^2 + \frac{b}{2a}\alpha_i + \frac{d}{b} = 0, \quad i = 1,2. \tag{4.17}$$

Since $\alpha_1 \neq \alpha_2$, by equation (4.16) D_3 is a positive integer. By equations (4.17), let

$$\alpha_i = \frac{-b}{4a} + \frac{(-1)^i}{2}\sqrt{\frac{b^3 - 16a^2d}{4a^2b}}, \quad i = 1,2.$$

Then $\sqrt{\frac{b^3 - 16a^2d}{4a^2b}}$ is a positive irrational number since α_1 is an irrational number. Now

$$D_3 = 4a^2b^2\left(\frac{b^3 - 16a^2d}{4a^2b}\right).$$

Therefore D_3 is not a perfect square. Thus D_3 is a positive integer which is not a perfect square.

If (x,y) is a solution of equation (4.4), then there exists an integer n such that $n^2 = 4ab^2m$ and

$$(4abx + b^2y)^2 - D_3y^2 = 8abn. \tag{4.18}$$

Clearly equation (4.4) has infinitely many solutions if equation (4.18) has infinitely many solutions.

Assume (x_o,y_o) is a solution of equation (4.4). Then equation (4.18) holds with $(x,y) = (x_o,y_o)$ and some integer n such that $n^2 = 4ab^2m$. Now D_3 is a positive integer which is not a perfect square. It is shown in [6] that there exist infinitely many distinct integers r_i and infinitely many distinct integers s_i, $i = 1,2,\cdots$, such that

$$r_i^2 - D_3 s_i^2 = 1.$$

Define for $i = 1,2,\cdots$

$$x_i = (4abx_o + b^2y_o)r_i + y_o s_i D_3 \tag{4.19}$$

and

$$y_i = (4abx_o + b^2y_o)s_i + y_o r_i. \tag{4.20}$$

Then

$$x_i^2 - D_3 y_i^2 = [(4abx_o + b^2y_o)^2 - D_3 y_o^2][r_i^2 - D_3 s_i^2] = 8abn. \tag{4.21}$$

Define $w_i = y_i$ and v_i by the equation $4abv_i + b^2w_i = x_i$, $i = 1,2,\cdots$. By equations (4.19) and (4.20)

$$4abv_i = 4ab(-b^2x_o s_i + x_o r_i - 4y_o s_i ad),$$

and consequently v_i is an integer since $4ab \neq 0$. By the equation $n^2 = 4ab^2m$ and equations (4.15) and (4.21)

$$\begin{aligned} 4ab^2 f(v_i,w_i) &= \left\{\frac{1}{8ab}\,[(4abv_i + b^2w_i)^2 - D_3 w_i^2]\right\}^2 \\ &= \left\{\frac{1}{8ab}\,[x_i^2 - D_3 y_i^2]\right\}^2 \\ &= n^2 \\ &= 4ab^2m. \end{aligned}$$

Therefore $f(v_i,w_i) = m$ for each pair of integers (v_i,w_i).

Suppose $(v_i,w_i) = (v_j,w_j)$ with $i \neq j$. Then $(x_i,y_i) = (x_j,y_j)$, and consequently by equations (4.19) and (4.20)

$$(4.22) \qquad (4abx_o + b^2y_o)(r_i - r_j) = y_oD_3(s_j - s_i)$$

and

$$(4.23) \qquad (4abx_o + b^2y_o)(s_i - s_j) = y_o(r_j - r_i).$$

If $4abx_o + b^2y_o = 0$, $y_o = 0$ by equation (4.23). Then $x_o = 0$. This is impossible since $f(0,0) = 0 \neq m$. Therefore $4abx_o + b^2y_o \neq 0$. Then by equations (4.22) and (4.23)

$$(4abx_o + b^2y_o)^2 - D_3y_o^2 = 0.$$

This is impossible since

$$(4abx_o + b^2y_o)^2 - D_3y_o^2 = 8abn$$

and $8abn \neq 0$. Thus $(v_i,w_i) \neq (v_j,w_j)$ if $i \neq j$. Hence equation (4.4) has infinitely many solutions if $b \neq 0$ and equation (4.4) has a solution. ‖

Corollary 4.10 If f is a positive form and Case II of Theorem 2.5 holds, then a necessary condition for f to represent m is am and em are perfect squares.

Proof. Suppose f represents m. If $b = 0$, by equation (4.11) $4am$ is a perfect square. If $b \neq 0$, by equation (4.15) $4ab^2m$ is a perfect square. Therefore in each case am is a perfect square. By symmetry em is a perfect square. ‖

If f is a positive form and Case II of Theorem 2.5 holds, then by equations (4.11) and (4.15) f represents m if and only if a certain quadratic form $Ax^2 + Bxy + Cy^2$, where $B^2 - 4AC$ is a positive integer

which is not a perfect square, represents n where $n^2 = 4am$ if $b = 0$ or $n^2 = 4ab^2m$ if $b \neq 0$. A method will be given to determine if the equation

$$Ax^2 + Bxy + Cy^2 = n$$

has a solution. By equations (4.11) and (4.15) we may assume without loss of generality that $A > 0$.

We first consider the equation

$$x^2 - Dy^2 = 1, \tag{4.24}$$

where D is a positive integer which is not a perfect square. The following material may be found in [6]. Equation (4.24) has an infinite number of solutions. There is a positive solution (x_1,y_1) of equation (4.24) with $x_1 > 0$ and $y_1 > 0$ such that $x_1 < x_2$ and $y_1 < y_2$ if (x_2,y_2) is another positive solution of equation (4.24). Since D is a positive integer and not a perfect square, $\sqrt{D}$ is a quadratic irrational. Then $\sqrt{D}$ has a simple periodic continued fraction expansion. Let $\sqrt{D} = \langle a_o,a_1,\cdots\rangle$, where $\langle a_o,a_1,\cdots\rangle$ denotes the continued fraction of $\sqrt{D}$. Define $r_\ell = \langle a_o,a_1,\cdots,a_\ell\rangle$ for $\ell \geq 0$. Then r_ℓ may be expressed as $r_\ell = h_\ell/k_\ell$, where h_ℓ and k_ℓ are relatively prime positive integers for $\ell \geq 0$. Let r denote the period of the expansion by $\sqrt{D}$. If r is even, $(x_1,y_1) = (h_{r-1},k_{r-1})$. If r is odd, $(x_1,y_1) = (h_{2r-1},k_{2r-1})$. If r is even, all positive solutions (x,y) of equation (4.24) are given by the formula $(x,y) = (h_{\ell r-1},k_{\ell r-1})$ where $\ell = 1,2,\cdots$. If r is odd, all positive solutions (x,y) of equation (4.24) are given by the formula $(x,y) = (h_{\ell r-1},k_{\ell r-1})$ where $\ell = 2,4,6,\cdots$. The positive solutions (x_i,y_i) of equation (4.24) can also be found by the formula $(x_i + y_i\sqrt{D})^i$ where $i = 1,2,\cdots$. Here x_i is equal to the rational part of $(x_1 + y_1\sqrt{D})^i$, and

y_i is equal to the purely irrational part of $(x_1 + y_1\sqrt{D})^i$. If r is even, all solutions of equation (4.24) are given by the formulas $(x,y) = (\pm 1,0)$ and $(x,y) = (\pm h_{\ell r-1}, \pm k_{\ell r-1})$, $\ell = 1,2,\cdots$, and in the second formula we take the four combinations of plus and minus. Similarly if r is odd, all solutions (x,y) of equation (4.24) are given by the formulas $(x,y) = (\pm 1,0)$ and $(x,y) = (\pm h_{\ell r-1}, \pm k_{\ell r-1})$ where $\ell = 2,4,6,\cdots$. Clearly the formulas $(x,y) = (\pm 1,0)$ and $(x,y) = (\pm x_i, \pm y_i)$, $i = 1,2,\cdots$, also give all the solutions of equation (4.24).

The solution of the equation

$$x^2 - Dy^2 = G, \tag{4.25}$$

where G is a nonzero integer and D is a positive integer which is not a perfect square, is discussed by Nagell [5], pp. 204-208. We give some of the results concerning the solution of equation (4.25). First $u + v\sqrt{D}$ is called a solution of equation (4.25) if (u,v) is a solution of equation (4.25). $x_1 + y_1\sqrt{D}$ is called the fundamental solution of equation (4.24). If $x + y\sqrt{D}$ is a solution of equation (4.24) and $u + v\sqrt{D}$ is a solution of equation (4.25), then

$$(u + v\sqrt{D})(x + y\sqrt{D}) = ux + vyD + (uy + vx)\sqrt{D}$$

is a solution of equation(4.25), and it is said to be associated with $u + v\sqrt{D}$. If two solutions of equation (4.25) are associated in this way, they are said to belong to the same class. Each class contains infinitely many members since equation (4.24) has an infinitude of solutions. Two solutions $u + v\sqrt{D}$ and $u' + v'\sqrt{D}$ are associated if and only if $(uu' - vv'D)/G$ and $(vu' - uv')/G$ are integers. If class $K = \{u_i + v_i\sqrt{D} \mid i = 1,2,\cdots\}$, then the conjugate class $\bar{K}$ is defined by

$\bar{K} = \{u_i - v_i\sqrt{D} \mid i = 1,2,\cdots\}$. If $K = \bar{K}$, then K and $\bar{K}$ are said to be ambiguous classes. For a given class K, there exists a member $u^* + v^*\sqrt{D}$ such that v^* is the smallest nonnegative value of the v_i's. If K is not ambiguous, u^* is unique. If K is ambiguous, u^* is unique if $u^* \geq 0$. The solution $u^* + v^*\sqrt{D}$ determined in this manner is called the fundamental solution of the class K.

Let N be a positive integer. In addition to the above material the next three theorems are discussed by Nagell [5], pp. 205-208.

Theorem 4.11 If $u + v\sqrt{D}$ is the fundamental solution of the class K of the equation

$$u^2 - Dv^2 = N, \tag{4.26}$$

and if $x_1 + y_1\sqrt{D}$ is the fundamental solution of equation (4.24), we have the inequalities

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1+1)}}\sqrt{N}\ , \tag{4.27}$$

$$0 < |u| \leq \sqrt{\tfrac{1}{2}(x_1+1)N}\ . \quad \| \tag{4.28}$$

Theorem 4.12 If $u + v\sqrt{D}$ is the fundamental solution of the class K of the equation

$$u^2 - Dv^2 = -N, \tag{4.29}$$

and if $x_1 + y_1\sqrt{D}$ is the fundamental solution of equation (4.24), we have the inequalities

$$0 < v \leq \frac{y_1}{\sqrt{2(x_1-1)}}\sqrt{N}\ , \tag{4.30}$$

$$0 \leq |u| \leq \sqrt{\tfrac{1}{2}(x_1-1)N}\ . \quad \| \tag{4.31}$$

Theorem 4.13 If D and N are natural numbers, and if D is not a perfect square, the Diophantine equations (4.26) and (4.29) have a finite number of classes of solutions. The fundamental solutions of all the classes can be found after a finite number of trials by means of the inequalities in Theorems 4.11 and 4.12. If $u^* + v^*\sqrt{D}$ is the fundamental solution of the class K, we obtain all the solutions $u + v\sqrt{D}$ of K by the formula

$$u + v\sqrt{D} = (u^* + v^*\sqrt{D})(x + y\sqrt{D}),$$

where $x + y\sqrt{D}$ runs through all the solutions of equation (4.24), including ± 1. The Diophantine equation (4.26), or (4.29), has no solution at all when it has no solution satisfying the inequalities (4.27) and (4.28), or (4.30) and (4.31), respectively. ‖

Again let $Ax^2 + Bxy + Cy^2$ be an integral form, where A and $B^2 - 4AC$ are positive integers and $B^2 - 4AC$ is not a perfect square. Consider the Diophantine equations

$$Ax^2 + Bxy + Cy^2 = N, \tag{4.32}$$

$$Ax^2 + Bxy + Cy^2 = -N, \tag{4.33}$$

$$(2Ax + By)^2 - (B^2 - 4AC)y^2 = 4AN, \tag{4.34}$$

$$(2Ax + By)^2 - (B^2 - 4AC)y^2 = -4AN, \tag{4.35}$$

where N is a positive integer. Integers $x = u$ and $y = v$ satisfy equation (4.32), or (4.33), if and only if they satisfy equation (4.34), or (4.35), respectively. We prove

Theorem 4.14 Equation (4.34) has a solution if and only if there exist integers x^* and y^* such that

$$y^* = v^*, \quad 2Ax^* + By^* = u^*, \tag{4.36}$$

where $u^* + v^*\sqrt{B^2 - 4AC}$ is a fundamental solution of the equation

$$u^2 - (B^2 - 4AC)v^2 = 4AN. \tag{4.37}$$

In this case (x^*,y^*) is a solution of equation (4.34). Only a finite number of steps is required to determine if equation (4.34) has a solution. If equation (4.34) has a solution, all solutions (x,y) are given by the equations

$$y = v^*t + u^*s, \quad 2Ax + By = u^*t + v^*s(B^2 - 4AC), \tag{4.38}$$

where $t + s\sqrt{B^2 - 4AC}$ runs through the solutions of equation (4.24) and $u^* + v^*\sqrt{B^2 - 4AC}$ is restricted to the fundamental solutions of equation (4.37) such that equations (4.36) hold.

Proof. If there exist integers x^* and y^* such that equations (4.36) hold, then equation (4.34) has a solution, namely (x^*,y^*). Therefore suppose equation (4.34) has a solution, say (x,y). By Theorem 4.13 there exist integers u and v such that $y = v$, $2Ax + By = u$, and

$$u + v\sqrt{B^2 - 4AC} = (u^* + v^*\sqrt{B^2 - 4AC})(t + s\sqrt{B^2 - 4AC}),$$

where $u^* + v^*\sqrt{B^2 - 4AC}$ is a fundamental solution of equation (4.37) and $t + s\sqrt{B^2 - 4AC}$ is a solution of equation (4.24). Then

$$y = v^*t + u^*s \quad \text{and} \quad 2Ax + By = u^*t + v^*s(B^2 - 4AC)$$

which implies

$$2Ax = (u^* - Bv^*)(t - Bs) - 4ACv^*s. \tag{4.39}$$

Since

$$t^2 - (B^2 - 4AC)s^2 = 1,$$

$$(t + Bs)(t + Bs) \equiv 1 \pmod{2A},$$

and consequently $t - Bs$ and $2A$ are relatively prime. Thus $2A \mid (u^* - Bv^*)$ by

equation (4.39). Therefore there exists an integer x^* such that $2Ax^* = u^* - Bv^*$. Define y^* by $y^* = v^*$. Then equations (4.36) hold, and (x^*,y^*) is a solution of equation (4.34). This completes the oof of the first part of the theorem.

Since the fundamental solutions of equation (4.37) can be found in a finite number of steps by use of the inequalities in Theorem 4.11 with $D = B^2 - 4AC$ and $4AN$ in place of N, then by the first part of this theorem only a finite number of steps is required to determine if equation (4.34) has a solution.

By Theorem 4.13 equations (4.38), where $t + s\sqrt{B^2 - 4AC}$ runs through the solutions of equation (4.24) and $u^* + v^*\sqrt{B^2 - 4AC}$ runs through the fundamental solutions of equation (4.37), give all possible values of x and y such that (x,y) is a solution of equation (4.34). Now by the proof of the first part of this theorem equations (4.38) give all possible values of x and y such that equation (4.34) holds with $u^* + v^*\sqrt{B^2 - 4AC}$ restricted to the fundamental solutions of equation (4.37) such that equations (4.36) hold. Therefore let x and y be given by equations (4.38) with $u^* + v^*\sqrt{B^2 - 4AC}$ restricted to a fundamental solution of equation (4.37) such that equations (4.36) hold. By equations (4.38) equation (4.39) holds. Since equations (4.36) hold, $2A|(u^* - Bv^*)$. Therefore by equation (4.39) x is indeed an integer. Now

$$
\begin{aligned}
&(2Ax + By)^2 - (B^2 - 4AC)y^2 \\
&\quad = [u^*t + v^*s(B^2 - 4AC)]^2 - [B^2 - 4AC][v^*t + u^*s]^2 \\
&\quad = [(u^*)^2 - (B^2 - 4AC)(v^*)^2][t^2 - (B^2 - 4AC)s^2] \\
&\quad = 4AN. \quad \|
\end{aligned}
$$

Corollary 4.15 Equation (4.34) has a solution if and only if there exist integers x and y such that $y = v$ and $2Ax + By = u$, where

$$u^2 - (B^2 - 4AC)v^2 = 4AN$$

and u and v are integers which satisfy the inequalities in Theorem 4.11.

Proof. The sufficiency part of the corollary is obvious. The necessity part of the corollary is immediate by the first part of Theorem 4.14 since u^* and v^* satisfy the inequalities in Theorem 4.11 if $u^* + v^*\sqrt{B^2 - 4AC}$ is a fundamental solution of equation (4.37). ‖

The proofs of the following theorem and corollary are very similar to the proofs of Theorem 4.14 and Corollary 4.15, respectively. Therefore the proofs will be omitted.

Theorem 4.16 Equation (4.35) has a solution if and only if there exist integers x^* and y^* such that

(4.40) $$y^* = v^*, \quad 2Ax^* + By^* = u^*,$$

where $u^* + v^*\sqrt{B^2 - 4AC}$ is a fundamental solution of the equation

(4.41) $$u^2 - (B^2 - 4AC)v^2 = -4AN.$$

In this case (x^*,y^*) is a solution of equation (4.35). Only a finite number of steps is required to determine if equation (4.35) has a solution. If equation (4.35) has a solution, all solutions (x,y) are given by the equations

$$y = v^*t + u^*s, \quad 2Ax + By = u^*t + v^*s(B^2 - 4AC),$$

where $t + s\sqrt{B^2 - 4AC}$ runs through the solutions of equation (4.24) and $u^* + v^*\sqrt{B^2 - 4AC}$ is restricted to the fundamental solutions of equation (4.41) such that equations (4.40) hold. ‖

Corollary 4.17 Equation (4.35) has a solution if and only if there exist integers x and y such that $y = v$ and $2Ax + By = u$, where

$$u^2 - (B^2 - 4AC)v^2 = -4AN$$

and u and v are integers which satisfy the inequalities in Theorem 4.12. ‖

Theorem 4.18 If $f(x,1)$ has at least one imaginary zero, then there are at most a finite number of solutions of equation (4.4), and the solutions (if any) can be found in a finite number of steps.

Proof. Suppose $f(x,1)$ has at least one imaginary zero. Then $f(x,1)$ has two or four imaginary zeros. Recall that $a > 0$ by hypothesis. Suppose $f(x,1)$ has four imaginary zeros. Then by Theorem 2.5 f is a positive form and Case I of that theorem holds. By Theorem 4.8 the desired conclusions are immediate.

Suppose $f(x,1)$ has exactly two imaginary zeros. Then let α_1 and α_2 denote the real zeros and $\alpha + \beta i$ and $\alpha - \beta i$ denote the imaginary zeros. Assume α_1 and α_2 are irrational numbers. By Theorem 4.4 $f(x,y)$ is reducible over the rationals if and only if

$$g(x,1) \equiv (x - \alpha_1)(x - \alpha_2)$$

and

$$h(x,1) \equiv [x - (\alpha + \beta i)][x - (\alpha - \beta i)]$$

are rational polynomials. If this is not the case, $f(x,y)$ is irreducible over the rationals. Then by Theorem 4.6 and Corollary 4.7 the desired conclusions follow. Therefore suppose $g(x,1)$ and $h(x,1)$ are rational polynomials (if $g(x,1)$ or $h(x,1)$ is a rational polynomial, the other polynomial is rational since $f(x,1)$ is an integral polynomial). Then there exist integers $K_1 \neq 0$ and $K_2 > 0$ such that $K_1 g(x,y)$ and $aK_2 h(x,y)$ are integral forms. Now for integers x and y $f(x,y) = m$ if and only if $K_1 K_2 f(x,y) = K_1 K_2 m$. Therefore, suppose x and y are integers such that $K_1 K_2 f(x,y) = K_1 K_2 m$. Then $aK_2 h(x,y) = D$, where D is a divisor of $K_1 K_2 m$. Therefore

$$aK_2 h(x,y) = aK_2[(x-\alpha y)^2 + \beta^2 y^2] = D \leq |K_1 m| K_2.$$

Thus

$$0 \leq y^2 \leq \frac{|K_1 m|}{a\beta^2} \tag{4.42}$$

since $aK_2 > 0$ and $\beta^2 > 0$.

Also

$$aK_2 h(x,y) = \frac{aK_2}{(\alpha^2+\beta^2)} \left\{[(\alpha^2+\beta^2)y - \alpha x]^2 + \beta^2 x^2\right\} = D < |K_1 m| K_2.$$

Thus

$$0 \leq x^2 \leq |K_1 m| \frac{(\alpha^2+\beta^2)}{a\beta^2} \quad . \tag{4.43}$$

Since inequalities (4.42) and (4.43) restrict x and y to a finite number of integral values, the conclusions of the theorem follow.

Assume α_1 and α_2 are rational numbers. Then $g(x,1)$ and $h(x,1)$ are rational polynomials. Therefore there exist integers $K_1 \neq 0$ and $K_2 > 0$ such that $K_1 g$ and $aK_2 h$ are integral forms. As in the case with α_1 and α_2 irrational numbers, $f(x,y) = m$ implies inequalities (4.42) and (4.43) hold, and the desired conclusions follows.

Suppose α_1 is a rational number and α_2 is an irrational number. Then

$$s(x,1) \equiv [x-\alpha_2][x - (\alpha-\beta i)][x - (\alpha-\beta i)]$$

is a rational polynomial. Therefore there exist nonzero integers K_1 and K_2 such that $K_1(x-\alpha_1 y)$ and $aK_2 s(x,y)$ are integral forms. Suppose $f(x,y) = m$. Then $K_1 K_2 f(x,y) = K_1 K_2 m$, and consequently

$$x = \alpha_1 y + \frac{D}{K_1} ,$$

where D is a divisor of $K_1 K_2 m$. Solving for y, we have

$$(4.44)\quad [\alpha_1-\alpha_2][\alpha_1-(\alpha-\beta i)][\alpha_1-(\alpha-\beta i)]y^3 + \frac{D}{K_1}[(\alpha_1-\alpha)(3\alpha_1-2\alpha_2-\alpha)+\beta^2]y^2$$
$$+\left(\frac{D}{K_1}\right)^2(3\alpha_1-\alpha_2-2\alpha)y+\left(\frac{D}{K_1}\right)^3-\frac{K_1 m}{aD}$$
$$=0.$$

Since α_1 is a rational number and α_2, $\alpha+\beta i$, and $\alpha-\beta i$ are not rational numbers, the coefficient of y^3 in equation (4.44) is not zero. Then there are at most a finite number of solutions of equation (4.4) since there are a finite number of divisors of K_1K_2m and equation (4.44) restricts y to a finite number of values for each divisor of K_1K_2m. Clearly the solutions (if any) can be found in a finite number of steps. ‖

Assume the zeros α_1, α_2, α_3, α_4 of $f(x,1)$ are real numbers. The zeros cannot be four equal irrational numbers or three rational numbers and one irrational number since $f(x,1)$ is an integral polynomial. In order to complete the discussion of the solution of equation (4.4) we consider six cases.

I. $\alpha_1=\alpha_2$, $\alpha_3=\alpha_4$, $\alpha_1\neq\alpha_3$, and α_1 and α_3 are irrational numbers.

Then f is a positive form and Case II of Theorem 2.5 holds. The solution of equation (4.4) has already been discussed. See Theorems 4.9, 4.14, and 4.16 and the material between Theorems 4.9 and 4.14.

II. $\alpha_1=\alpha_2=\alpha_3=\alpha_4$, and α_1 is a rational number.

Then $f(x,y)=a(x-\alpha_1 y)^4$. Since α_1 is a rational number, there exists a nonzero integer K such that $Kx-K\alpha_1 y$ is an integral form. For integers u and v, $f(u,v)=m$ if and only if $Ku-K\alpha_1 v=D$, where D is a divisor of K^4m and $aD^4=K^4m$. If there is no integer D such that $aD^4=K^4m$, then equation (4.4) does not have a solution. Let $(K,K\alpha_1)$ denote the greatest

common divisor of K and $K\alpha_1$. If there exists an integer D such that $aD^4 = K^4m$ but $(K,K\alpha_1) \nmid D$, then equation (4.4) does not have a solution. Therefore, suppose there exists an integer D such that $aD^4 = K^4m$ and $(K,K\alpha_1) \mid D$. Then -D is the only other integral solution of the equation $aw^4 = K^4m$. By the Euclidean algorithm there exist integers s and t such that $Ks - K\alpha_1 t = (K,K\alpha_1)$. Then all integral solutions (x,y) of equation (4.4) are given by the formulas

$$(x,y) = \left(s\frac{D}{(K,K\alpha_1)} + eK\alpha_1,\ t\frac{D}{(K,K\alpha_1)} + eK\right),$$

$$(x,y) = \left(-s\frac{D}{(K,K\alpha_1)} + eK\alpha_1,\ -t\frac{D}{(K,K\alpha_1)} + eK\right),$$

where e is any integer.

III. $\alpha_1 = \alpha_2$, $\alpha_3 = \alpha_4$, $\alpha_1 \neq \alpha_3$, and α_1 and α_3 are rational numbers. Then

$$f(x,y) = a[x^2 - (\alpha_1+\alpha_3)xy + \alpha_1\alpha_3 y^2]^2,$$

and there exists a nonzero integer K such that

$$g(x,y) \equiv Kx^2 - K(\alpha_1+\alpha_3)xy + K\alpha_1\alpha_3 y^2$$

is an integral form. For integers x_1 and y_1 $f(x_1,y_1) = m$ if and only if $g(x_1,y_1) = D$ where D is a divisor of K^2m and $aD^2 = K^2m$. If no such integer D exists, then equation (4.4) does not have a solution. If there exists an integer D such that $aD^2 = K^2m$, then -D is the only other solution of the equation $aw^2 = K^2m$. Therefore, suppose x_1, x_2, y_1, y_2, and D are integers such that $g(x_1,y_1) = D$, $g(x_2,y_2) = -D$, and $aD^2 = K^2m$. Then

$$[2Kx_1 - K(\alpha_1+\alpha_3)y_1]^2 - [K(\alpha_1-\alpha_3)y_1]^2 = 4KD, \tag{4.45}$$

$$[2Kx_2 - K(\alpha_1+\alpha_3)y_2]^2 - [K(\alpha_1-\alpha_3)y_2]^2 = -4KD. \tag{4.46}$$

By equation (4.45)

$$(4.47) \qquad x_1 = \left[\frac{4KD}{L_1} + L_1 + \frac{(\alpha_1+\alpha_3)}{(\alpha_1-\alpha_3)}\left(L_1 - \frac{4KD}{L_1}\right)\right] \Big/ 4K,$$

$$(4.48) \qquad y_1 = \left[L_1 - \frac{4KD}{L_1}\right] \Big/ [2K(\alpha_1-\alpha_3)],$$

where L_1 is a divisor of 4KD. By equation (4.46)

$$(4.49) \qquad x_2 = \left[L_2 - \frac{4KD}{L_2} + \frac{(\alpha_1+\alpha_3)}{(\alpha_1-\alpha_3)}\left(L_2 + \frac{4KD}{L_2}\right)\right] \Big/ 4K,$$

$$(4.50) \qquad y_2 = \left[L_2 + \frac{4KD}{L_2}\right] \Big/ [2K(\alpha_1-\alpha_3)],$$

where L_2 is a divisor of 4KD.

Since there are a finite number of divisors of 4KD, equation (4.4) has at most a finite number of solutions. For rational numbers x_1 and y_1 defined by equations (4.47) and (4.48), respectively, $g(x_1,y_1) = D$. Similarly, for x_2 and y_2 defined by equations (4.49) and (4.50), respectively, $g(x_2,y_2) = -D$. Therefore equation (4.4) has a solution if and only if there exists an integer D such that $aD^2 = K^2m$ and x_1 and y_1 are integers for some divisor L_1 of 4KD or x_2 and y_2 are integers for some divisor L_2 of 4KD. Clearly the solutions (if any) of equation (4.4) can be found in a finite number of steps.

IV. α_1, α_2, α_3, α_4 are irrational numbers, and $(x-\alpha_i)(x-\alpha_j)$ and $(x-\alpha_k)(x-\alpha_\ell)$ are not both rational polynomials for each permutation (i,j,k,ℓ) of the integers 1,2,3,4.

Then by Theorem 4.4 f(x,y) is irreducible over the rationals. By

Theorem 4.6 and Corollary 4.7 equation (4.4) has at most a finite number of solutions, and the solutions (if any) can be found in a finite number of steps.

V. Either V_1, all the zeros are rational numbers, and neither case II nor case III holds,

or V_2, α_1 and α_2 are rational numbers and α_3 and α_4 are irrational numbers,

or V_3, all the zeros are irrational numbers, $(x-\alpha_1)(x-\alpha_2)$ and $(x-\alpha_3)(x-\alpha_4)$ are rational polynomials, and Case I does not hold.

If case V_2 holds, then $(x-\alpha_3)(x-\alpha_4)$ is a rational polynomial since α_1 and α_2 are rational numbers and $f(x,1)$ is an integral polynomial. Therefore in all cases there exist nonzero integers K_1 and K_2 such that

$$g(x,y) \equiv aK_1(x-\alpha_1 y)(x-\alpha_2 y) \equiv A_1x^2 + B_1xy + C_1y^2 \tag{4.51}$$

and

$$h(x,y) \equiv K_2(x-\alpha_3 y)(x-\alpha_4 y) \equiv A_2x^2 + B_2xy + C_2y^2 \tag{4.52}$$

are integral forms. Also

$$K_1K_2f(x,y) = g(x,y)h(x,y). \tag{4.53}$$

For integers u and v, $f(u,v) = m$ if and only if there exist divisors D_1 and D_2 of K_1K_2m such that

$$\frac{K_1K_2m}{D_1} \cdot \frac{K_1K_2m}{D_2} = K_1K_2m,$$

$$g(u,v) = \frac{K_1K_2m}{D_1}, \tag{4.54}$$

$$h(u,v) = \frac{K_1K_2m}{D_2}. \tag{4.55}$$

Suppose this is the case. Define the form Q by

$$(4.56) \quad Q(x,y) = (D_1A_1 - D_2A_2)x^2 + (D_1B_1 - D_2B_2)xy + (D_1C_1 - D_2C_2)y^2.$$

By equations (4.51), (4.52), (4.54), and (4.55)

$$(4.57) \quad Q(u,v) = 0.$$

If the coefficients of Q are all zero, by equations (4.51), (4.52), and (4.53)

$$f(x,y) = \frac{D_1}{D_2K_1K_2}[g(x,y)]^2.$$

This implies case I, II, or III holds. But this is impossible by hypothesis. Therefore at least one of the coefficients of Q is not zero.

Suppose $D_1A_1 - D_2A_2 = D_1C_1 - D_2C_2 = 0$. Then $D_1B_1 - D_2B_2 \neq 0$. By equations (4.56) and (4.57) u or v is zero. If u = 0, by equations (4.51) and (4.54)

$$D_1aK_1\alpha_1\alpha_2v^2 = K_1K_2m.$$

If v = 0, by equations (4.51) and (4.54)

$$D_1aK_1u^2 = K_1K_2m.$$

Assume $D_1A_1 - D_2A_2 \neq 0$. Then Q may be expressed in the form

$$Q(x,y) = (D_1A_1 - D_2A_2)(x - R_1y)(x - R_2y),$$

where R_1 and R_2 are the zeros of Q(x,1). Therefore by equations (4.57) $u = R_1v$ or $u = R_2v$. If $u = R_1v$, by equations (4.54) and (4.57)

$$D_1aK_1(R_1 - \alpha_1)(R_1 - \alpha_2)v^2 = K_1K_2m.$$

If $u = R_2v$, by equations (4.54) and (4.57)

$$D_1aK_1(R_2 - \alpha_1)(R_2 - \alpha_2)v^2 = K_1K_2m.$$

Similarly, if $D_1C_1 - D_2C_2 = 0$, then

$$v = S_1u \quad \text{and} \quad D_1aK_1(1-\alpha_1S_1)(1-\alpha_2S_1)u^2 = K_1K_2m,$$

or

$$v = S_2u \quad \text{and} \quad D_1aK_1(1-\alpha_1S_2)(1-\alpha_2S_2)u^2 = K_1K_2m,$$

where S_1 and S_2 are the zeros of $Q(1,y)$.

Since there are a finite number of divisors of K_1K_2m and in each case the equations for u and v have a finite number of solutions, equation (4.4) has at most a finite number of solutions. To determine the solutions of equation (4.4) one has only to solve the respective equations for u and v and see if these values for u and v (if any, since the coefficients in some of the equations may be zero) are integers and solutions. Thus the solutions of equation (4.4) can be found in a finite number of steps.

VI. α_1 is a rational number and α_2, α_3, and α_4 are irrational numbers.

Since α_1 is a rational number and $f(x,1)$ is an integral polynomial, there exist nonzero integers K_1 and K_2 such that $K_1(x-\alpha_1y)$ and $aK_2(x-\alpha_2y)(x-\alpha_3y)(x-\alpha_4y)$ are integral forms. Suppose $f(x,y) = m$. Then $K_1K_2f(x,y) = K_1K_2m$, and consequently

$$x = \alpha_1y + \frac{D}{K_1},$$

where D is a divisor of K_1K_2m. Solving for y, we have

(4.58)

$$(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)y^3 + \frac{D}{K_1}[(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)+(\alpha_1-\alpha_2)(\alpha_1-\alpha_4)+(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)]y^2$$

$$+ \left(\frac{D}{K_1}\right)^2(3\alpha_1-\alpha_2-\alpha_3-\alpha_4)y + \left(\frac{D}{K_1}\right)^3 - \frac{K_1m}{aD}$$

$$= 0.$$

Since α_1 is a rational number and α_2, α_3, and α_4 are irrational numbers, the coefficient of y^3 in equation (4.58) is not zero. Then there are at most a finite number of solutions of equations (4.4) since there are a finite number of divisors of K_1K_2m and equation (4.58) restricts y to a finite number of values for each divisor of K_1K_2m. Clearly the solutions (if any) can be found in a finite number of steps.

The above results are summarized in the following two theorems.

Theorem 4.19 If the zeros of f(x,1) are four equal rational numbers or two distinct pairs of equal irrational numbers, then equation (4.4) has an infinite number of solutions if it has a solution. In each case only a finite number of steps is required to determine if equation (4.4) has a solution. Also, in each case there are formulas for x and y which give all the solutions of equation (4.4). ‖

Theorem 4.20 If the zeros of f(x,1) are real and neither four equal rational numbers nor two distinct pairs of equal irrational numbers, then equation (4.4) has at most a finite number of solutions and the solutions (if any) can be found in a finite number of steps. ‖

Theorem 4.21 If the zeros of f(x,1) are neither four equal rational numbers nor two distinct pairs of equal irrational numbers, then equation (4.4) has at most a finite number of solutions and the solutions (if any) can be found in a finite number of steps.

Proof. This follows immediately from Theorems 4.18 and 4.20. ‖

Note that Theorems 4.19, 4.20, and 4.21 remain valid if $a < 0$.

Theorem 4.22 Equation (4.4) has infinitely many solutions for some nonzero integer m if and only if f(x,y) can be expressed in the form

$$f(x,y) = A(Bx^2 + Cxy + Dy^2)^2, \tag{4.59}$$

where $A \neq 0$, $B \neq 0$, C, D are integers and $C^2 - 4BD = 0$ or $C^2 - 4BD$ is a positive integer which is not a perfect square.

Proof. Suppose equation (4.59) holds where $A \neq 0$, $B \neq 0$, C, D are integers, $C^2 - 4BD = 0$, or $C^2 - 4BD$ is a positive integer which is not a perfect square. Then

$$f(x,1) = A\{\frac{1}{4B}[(2Bx + C)^2 - (C^2 - 4BD)]\}^2 \tag{4.60}$$

Since $AB \neq 0$ and $C^2 - 4BD = 0$ or $C^2 - 4BD$ is a positive integer which is not a perfect square, by equation (4.60) the zeros of $f(x,1)$ are four equal rational numbers or two distinct pairs of equal irrational numbers. By Theorem 4.19 equation (4.4) has infinitely many solutions with $m = f(1,0) = AB^2 \neq 0$.

Conversely, suppose equation (4.4) has infinitely many solutions for some nonzero integer m. By Theorems 4.19 and 4.21, $f(x,1)$ has four equal rational zeros or two distinct pairs of equal irrational zeros. Then by the proof of Theorem 4.9 and the discussion of case II ($f(x,1)$ has four equal rational zeros) $f(x,1)$ may be expressed in the form

$$f(x,y) = a(Ex^2 + Gxy + Hy^2)^2,$$

where E, G, and H are rational numbers. Then there exist integers A, B, C, D such that

$$f(x,y) = A(Bx^2 + Cxy + Dy^2)^2.$$

Now $AB \neq 0$ since $a \neq 0$. Since the zeros of $f(x,1)$ are four equal rational numbers or two distinct pairs of equal irrational numbers, $C^2 - 4BD = 0$ or $C^2 - 4BD$ is a positive integer which is not a perfect square. ‖

CHAPTER V

ON THE NUMBER OF REPRESENTATIONS OF INTEGERS BY BINARY FORMS

Let $g(x,y)$ be an integral binary form with degree $n \geq 3$, irreducible over the rationals. If (u,v) is an integral solution of the equation

$$g(x,y) = m, \tag{5.1}$$

where m is an integer, then there are at most n integral solutions with v the second component of the solutions. If $v = 0$, there are at most two integral solutions. If $m > 0$, let B denote the bound in Theorem 4.6 for the integral solutions (x,y) of equation (5.1). Then $2nB + 2$ is an upper bound for the number of integral solutions of equation (5.1). If $m < 0$, let D denote the bound in Corollary 4.7 for the integral solutions (x,y) of equation (5.1). Then $2nD + 2$ is an upper bound for the number of integral solutions of equation (5.1). If $m = 0$, there is only one integral solution of equation (5.1), namely $(0,0)$, since $g(x,y)$ is irreducible over the rationals. The remainder of the chapter will be devoted to improving the above upper bounds.

Theorem 5.1 Let $g(z,1)$ be a real n-th degree polynomial with only imaginary zeros, say $\alpha_1,\cdots,\alpha_n$. Then there exists a positive constant δ such that there are no real numbers z which satisfy any of the inequalities

$$|z - \alpha_K| < \delta,$$

where $K = 1,\cdots,n$.

Proof. Since α_K is an imaginary number for each K, there exist real numbers a_K and nonzero real numbers b_K, $K = 1,\cdots,n$, such that $\alpha_K = a_K + b_K i$. Then there exist positive constants ε_K such that $|b_K| - \varepsilon_K > 0$. Define $\delta = \min(|b_1| - \varepsilon_1,\cdots,|b_n| - \varepsilon_n)$. For each K there are no real numbers z such that $|z - \alpha_K| < |b_K| - \varepsilon_K$. Thus for each K there is no real number z such that $|z - \alpha_K| < \delta$. ‖

Theorem 5.2 Let g(z,1) be a real n-th degree polynomial with distinct zeros, say $\alpha_1,\cdots,\alpha_n$, and at least one real zero. Then there exist positive constants δ and M such that

$$|g^{(1)}(z,1)| > M$$

whenever $|z - \alpha_i| < \delta$, z real, for some i. †

Proof. If $\alpha_K = a_K + b_K i$, where a_K and $b_K \neq 0$ are real numbers, then there exists a positive constant ε_K such that $|b_K| - \varepsilon_K > 0$. Then there are no real numbers z such that $|z - \alpha_K| < |b_K| - \varepsilon_K$. For imaginary zeros α_K define $\delta_K = |b_K| - \varepsilon_K$ and $M_K = 1$. By hypothesis g(z,1) has no multiple zeros. It may be shown [3] that $g^{(1)}(\alpha_i,1) \neq 0$ for $i = 1,\cdots,n$. Then for each real zero α_i there exist positive constants M_i and δ_i such that

$$|g^{(1)}(z,1)| > M_i \quad \text{whenever} \quad |z - \alpha_i| < \delta_i, \ z \text{ real},$$

since $g^{(1)}(z,1)$ is a continuous function. Define $\delta = \min \delta_i$ and $M = \min M_i$, $i = 1,\cdots,n$. Suppose $|z - \alpha_i| < \delta$ for some i and z real. Then $|z - \alpha_i| < \delta_i$ since $\delta \leq \delta_i$. Therefore $|g^{(1)}(z,1)| > M_i \geq M$. ‖

In the following theorem the method of proof is suggested by Mordell [4], 188

Theorem 5.3 Let $g(z,1) = a_n z^n + \cdots + a_o$ be a real polynomial with

† $g^{(r)}(z,1)$ denotes the r-th derivative of g(z,1) with respect to z.

distinct zeros $\alpha_1, \alpha_2, \cdots, \alpha_n$, $n \geq 2$. Define $B_1 = \left|\frac{m}{a_n}\right|^{1/n}$, where m is a nonzero integer, and $B_2 = \min|\alpha_i - \alpha_j|$, $i,j = 1,\cdots,n$, $i \neq j$. Suppose $g(x,y) = m$ with $|y| > \frac{2B_1}{B_2}$ and x and y real numbers. Then for some i

$$\left|\frac{x}{y} - \alpha_i\right| < \left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1} \frac{1}{|y|^n}.$$

Proof. Since $g(x,y) = m$,

$$|x-\alpha_1 y||x-\alpha_2 y|\cdots|x-\alpha_n y| = \left|\frac{m}{a_n}\right|.$$

Then for at least one zero of g, say α_1, $0 < |x-\alpha_1 y| < B_1$. Since $|y| > \frac{2B_1}{B_2}$, for $i = 2,\cdots,n$

$$|\alpha_1-\alpha_i||y| - |x-\alpha_1 y| \geq |\alpha_1-\alpha_i||y| - B_1 \geq B_2|y| - B_1 > \frac{B_2}{2}|y| > 0.$$

Therefore for $i = 2,\cdots,n$

$$|x-\alpha_i y| = |(\alpha_1-\alpha_i)y + x-\alpha_1 y| > ||(\alpha_1-\alpha_i)y| - |x-\alpha_1 y|| > \frac{B_2}{2}|y|.$$

Thus

$$\left|a_n(x-\alpha_1 y)\left(\frac{B_2}{2}\right)^{n-1} y^{n-1}\right| < |m|,$$

and consequently

$$\left|\frac{x}{y} - \alpha_1\right| < \left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1} \frac{1}{y^n}. \quad \|$$

Theorem 5.4 Let $g(z) = a_n z^n + \cdots + a_o$ be a real polynomial with distinct zeros $\alpha_1,\cdots,\alpha_n$, $n \geq 2$, and at least one real zero. Suppose $g(x,y) = m$, where m is a nonzero integer and x and y are real numbers. Let δ be defined as in the proof of Theorem 5.2. Define

$B_1 = \left|\frac{m}{a_n}\right|^{1/n}$ and $B_2 = \min|\alpha_i - \alpha_j|$, $i,j = 1,\cdots,n$, $i \neq j$. Suppose

$$|y| > \max\left\{\sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}},\ \frac{2B_1}{B_2}\right\}.$$

Then for some i

$$\left|\frac{x}{y} - \alpha_i\right| < \delta.$$

Proof. Since $|y| > \frac{2B_1}{B_2}$, by Theorem 5.3 for some i

$$\left|\frac{x}{y} - \alpha_i\right| < \left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{|y|^n}.$$

Also

$$|y| > \sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}},$$

or equivalently

$$\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{|y|^n} < \delta.$$

Thus for some i

$$\left|\frac{x}{y} - \alpha_i\right| < \delta. \ \|$$

Theorem 5.5 Let $g(z,1) = a_n z^n + \cdots + a_o$ be a real polynomial with distinct zeros $\alpha_1,\cdots,\alpha_n$, $n \geq 2$, and no real zeros. Let δ be defined as in the proof of Theorem 5.1. Define $B_1 = \left|\frac{m}{a_n}\right|^{1/n}$, where m is a nonzero integer, and $B_2 = \min|\alpha_i - \alpha_j|$, $i,j = 1,\cdots,n$, $i \neq j$. Then there is no real solution (x,y) of the equation $g(x,y) = m$ such that

$$|y| > \max\left\{\sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}},\ \frac{2B_1}{B_2}\right\}.$$

Proof (by contradiction). Suppose there is a real solution (x,y) with

$$|y| > \max\left\{\sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}},\ \frac{2B_1}{B_2}\right\}.$$

Since $|y| > \frac{2B_1}{B_2}$, by Theorem 5.3 for some i

$$\left|\frac{x}{y} - \alpha_i\right| < \left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1} \frac{1}{|y|^n}.$$

Now

$$|y| > \sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1} \frac{1}{\delta}},$$

or equivalently

$$\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1} \frac{1}{|y|^n} < \delta.$$

Then for some i

$$\left|\frac{x}{y} - \alpha_i\right| < \delta.$$

This is impossible by Theorem 5.1. ‖

Theorem 5.6 Let $g(z,1)$ be a real polynomial with distinct zeros $\alpha_1, \alpha_2, \cdots, \alpha_n$, $n \geq 2$, and at least one real zero. Define $\beta = 1 - \varepsilon$, where $0 < \varepsilon < 1$. Suppose (x,y) and (p,q) are integral solutions of the equation $g(x,y) = m$, m a nonzero integer, $\frac{x}{y} \neq \frac{p}{q}$, $|y| \neq |q|$, $yq > 0$, $|y| > \sqrt[\beta]{\frac{|m|}{M}}$, $|q| > \sqrt[\beta]{\frac{|m|}{M}}$, where M is defined as in the proof of Theorem 5.2. Assume

$$\left|\frac{x}{y} - \alpha_i\right| < \delta \text{ and } \left|\frac{p}{q} - \alpha_i\right| < \delta$$

for some i, where δ is defined as in the proof of Theorem 5.2. Then

$$|y|^{n-2+\varepsilon} \leq |q| \quad \text{or} \quad |q|^{n-2+\varepsilon} \leq |y|.$$

Proof. Suppose neither $|y|^{n-2+\varepsilon} \leq |q|$ nor $|q|^{n-2+\varepsilon} \leq |y|$ holds. Without loss of generality we may assume $|y| < |q|$. Since neither inequality holds, $|q| < |y|^{n-2+\varepsilon}$. If ξ is between $\frac{x}{y}$ and $\frac{p}{q}$, then

$|\xi - \alpha_i| < \delta$ since $\left|\frac{x}{y} - \alpha_i\right| < \delta$ and $\left|\frac{p}{q} - \alpha_i\right| < \delta$. Then by Theorem 5.2 we have $|g^{(1)}(\xi,1)| > M$. By hypothesis $g(x,y) = m$. Therefore $g(\frac{x}{y},1) = \frac{m}{y^n}$. Similarly $g(\frac{p}{q},1) = \frac{m}{q^n}$. Then by the mean value theorem there exists ξ_o between $\frac{x}{y}$ and $\frac{p}{q}$ such that

$$\left|\frac{m}{q^n} - \frac{m}{y^n}\right| = |g^{(1)}(\xi_o,1)|\left|\frac{x}{y} - \frac{p}{q}\right|.$$

Therefore

$$|yq|\left|\frac{1}{q^n} - \frac{1}{y^n}\right| > \frac{M}{|m|}\,|xq - yp|.$$

Since $|xq - yp|$ is a positive integer,

$$|yq|\left|\frac{1}{q^n} - \frac{1}{y^n}\right| > \frac{M}{|m|}.$$

Now $|y| < |q|$ and $yq > 0$. Then

$$1 > \left|\left(\frac{y}{q}\right)^n - 1\right|.$$

Thus

$$|y|^{n-2+\epsilon} > |q| > \frac{M}{|m|}\,|y|^{n-1}$$

which yields

$$\frac{1}{|y|^{\beta}} > \frac{M}{|m|}.$$

Equivalently

$$\sqrt[\beta]{\frac{|m|}{M}} > |y|.$$

This is impossible by hypothesis. Hence at least one of the desired inequalities holds. ‖

Theorem 5.7 Let $g(z,1) = a_n z^n + \cdots + a_o$ be a real polynomial with distinct zeros $\alpha_1,\cdots,\alpha_n$, $n \geq 2$, and no real zeros. Let δ be defined as in the proof of Theorem 5.1. Define $B_1 = \left|\frac{m}{a_n}\right|^{1/n}$, where m is a

nonzero integer, and $B_2 = \min|\alpha_i - \alpha_j|$, $i,j = 1,\cdots,n$, $i \neq j$. Let H denote the number of integral solutions of the equation $g(x,y) = m$. Then

$$H \leq 2n \max\left\{\sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}}\ ,\ \frac{2B_1}{B_2}\right\} + 2.$$

Proof. If (u,v) is an integral solution of the equation $g(x,y) = m$, then by Theorem 5.5

$$|v| < \max\left\{\sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}}\ ,\ \frac{2B_1}{B_2}\right\}.$$

The desired conclusion now follows. ‖

Theorem 5.8 Let $g(z,1) = a_n z^n + \cdots + a_o$ be an integral polynomial of degree $n \geq 3$, irreducible over the rationals, with zeros $\alpha_1,\cdots,\alpha_n$ and $s \geq 1$ real zeros. Suppose m is a nonzero integer. Let B and D be defined as in the first paragraph of this chapter and δ and M be defined as in Theorem 5.2. Set $\beta = 1 - \varepsilon$, where $0 < \varepsilon < 1$. Define $B_1 = \left|\frac{m}{a_n}\right|^{1/n}$ and $B_2 = \min|\alpha_i - \alpha_j|$, $i,j = 1,\cdots,n$, $i \neq j$. Denote the number of integral solutions of the equation $g(x,y) = m$ by K. Define

$$R = \max\left\{\sqrt[\beta]{\frac{|m|}{M}}\ ,\ \sqrt[n]{\left|\frac{m}{a_n}\right|\left(\frac{2}{B_2}\right)^{n-1}\frac{1}{\delta}}\ ,\ \frac{2B_1}{B_2}\ ,\ \sqrt[n]{\left|\frac{m}{a_o}\right|}\right\}.$$

Suppose $R < B$ if $m > 0$ and $R < D$ if $m < 0$. Assume $R > 1$. Then

$$K < 2nR + 2 + 2ns\left[\frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n - 2 + \varepsilon)} + 1\right] \tag{5.2}$$

if $m > 0$, and if $m < 0$

$$K < 2nR + 2 + 2ns\left[\frac{\ell n\ \ell n\ D - \ell n\ \ell n\ R}{\ell n(n - 2 + \varepsilon)} + 1\right]. \tag{5.3}$$

Remark. The proofs that inequalities (5.2) and (5.3) hold are very similar. Therefore we will only prove that inequality (5.2) holds.

Proof. By hypothesis $g(z,1)$ is irreducible over the rationals. It has been shown [3] that the zeros of $g(z,1)$ are distinct. The number of integral solutions of equation (5.1) such that $0 \leq |y| \leq R$ is at most $2nR + 2$. Let L_1 denote the number of integral values of y with $R < y < B$ such that y is the second component of an integral solution (x,y) of equation (5.1). Then there are at most nL_1 integral solutions of equation (5.1) with $R < y < B$. Let L_2 denote the number of negative integral values of y with $R < |y| < B$ such that y is the second component of an integral solution (x,y) of equation (5.1). Then there are at most nL_2 integral solutions of equation (5.1) with $y < 0$ and $R < |y| < B$. Thus

$$K \leq 2nR + 2 + n(L_1 + L_2).$$

To complete the proof we show

$$\max\{L_1,L_2\} < s\left[\frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n-2+\varepsilon)} + 1\right].$$

Define

$$T = \{y \mid y \text{ is an integer, } R < y < B, \text{ and there exists an integer } x_y \text{ such that } g(x_y,y) = m\}.$$

If $y \in T$, by Theorem 5.4 for some i

$$\left|\frac{x_y}{y} - \alpha_i\right| < \delta.$$

By the proof of Theorem 5.2 α_i is a real zero. For $i = 1,\cdots,s$ define

$$T_i = \{y \mid y \in T \text{ and } \left|\frac{x_y}{y} - \alpha_i\right| < \delta\}.$$

For a set V let "order of V" denote the number of elements of V. Then

$$T = \bigcup_{i=1}^{s} T_i \quad \text{and} \quad L_1 = \text{order of } T \leq \sum_{i=1}^{s} \text{order of } T_i.$$

Suppose order $T_1 \geq 2$. Then let

$$T_1 = \{y_1, y_2, \cdots, y_h\}$$

with $y_1 < y_2 < \cdots < y_h$. Now $\frac{x_{y_i}}{y_i} \neq \frac{x_{y_j}}{y_j}$ if $i \neq j$. To prove this suppose $\frac{x_{y_i}}{y_i} = \frac{x_{y_j}}{y_j}$ with $i \neq j$. If $x_{y_i} = 0$, then $a_o y_i^n = m$ which implies $|y_i| = \sqrt[n]{\left|\frac{m}{a_o}\right|}$. This is impossible since $y_i > R$. Therefore there exist nonzero integers a, b, c, d such that $ac = x_{y_i}$, $ad = y_i$, $bc = x_{y_j}$, $bd = y_j$. Then $a^n g(c,d) = b^n g(c,d)$ which implies $a = b$ or $a = -b$. If $a = b$, $y_i = y_j$. This is impossible. Therefore $a = -b$, and consequently $y_i = -y_j$. Then y_i or y_j is a negative integer. This is impossible by the definition of T_1. Therefore by Theorem 5.6

$$y_1^{(n-2+\varepsilon)} < y_2,\ y_2^{(n-2+\varepsilon)} < y_3, \cdots, y_{h-1}^{(n-2+\varepsilon)} < y_h$$

since $n-2+\varepsilon > 1$ and $y_i < y_{i+1}$, $i = 1, \cdots, h-1$. Now $R < y_1$ and $y_h < B$. Thus

$$R^{[(n-2+\varepsilon)^{h-1}]} < y_1^{[(n-2+\varepsilon)^{h-1}]} < B,$$

and consequently

$$\text{order of } T_1 = h < \frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n-2+\varepsilon)} + 1 .$$

Clearly this inequality holds if order of $T_1 \leq 1$. Similarly for $i = 2, \cdots, s$

$$\text{order of } T_i < \frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n-2+\varepsilon)} + 1.$$

Therefore

$$L_1 = \text{order of } T < s\left[\frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n-2+\varepsilon)} + 1\right].$$

By a similar argument

$$L_2 < s\left[\frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n-2+\varepsilon)} + 1\right].$$

Hence

$$L_1 + L_2 \leq 2 \max\{L_1, L_2\} < 2s\left[\frac{\ell n\ \ell n\ B - \ell n\ \ell n\ R}{\ell n(n-2+\varepsilon)} + 1\right]. \quad \|$$

Theorem 5.9 Assume the hypotheses of Theorem 5.8 hold. Suppose the degree of g is three or four. Then the right-hand members of inequalities (5.2) and (5.3) can be found in a finite number of steps.

Proof. By Theorem 4.6 and Corollary 4.7 it remains to prove that M and δ can be found in a finite number of steps. To do this we show that for each real zero α_i of $g(z,1)$ there exist positive constants M_i and δ_i which can be found in a finite number of steps such that

$$|g^{(1)}(z,1)| > M_i \quad \text{whenever } |z - \alpha_i| < \delta_i,\ z \text{ real.}$$

Let α_i be a real zero of $g(z,1)$. By hypothesis $g(z,1)$ is irreducible over the rationals. It may be shown [3] that $g^{(1)}(\alpha_i,1) \neq 0$. Suppose $g^{(1)}(\alpha_i,1) > 0$. If there are no real numbers r_1 or r_2 such that $r_1 < \alpha_i$ and $g^{(1)}(r_1,1) = 0$ or $r_2 > \alpha_i$ and $g^{(1)}(r_2,1) = 0$, define $\delta_i = 1$. If there exists a real number $r < \alpha_i$ such that $g^{(1)}(r,1) = 0$ and if there does not exist a real number $r_2 > \alpha_i$ such that $g^{(1)}(r_2,1) = 0$, then let r_1 be the nearest real number to α_i such that $r_1 < \alpha_i$ and $g^{(1)}(r_1,1) = 0$ and define $\delta_i = \frac{\alpha_i - r_i}{2}$. If there exists a real number $r > \alpha_i$ such that $g^{(1)}(r,1) = 0$ and if there does not exist a real number $r_1 < \alpha_i$ such that $g^{(1)}(r_1,1) = 0$, then let r_2 be the nearest real number to α_i such that $r_2 > \alpha_i$ and $g^{(1)}(r_2,1) = 0$ and define $\delta_i = \frac{r_2 - \alpha_i}{2}$. If there exist real numbers r and S such that $r < \alpha_i < S$ and $g^{(1)}(r,1) = g^{(1)}(S,1) = 0$, then let r_1 and r_2 be the nearest real numbers to α_i such that $r_1 < \alpha_i < r_2$ and $g^{(1)}(r_1,1) = g^{(1)}(r_2,1) = 0$ and define $\delta_i = \min\left\{\frac{\alpha_i - r_1}{2}, \frac{r_2 - \alpha_i}{2}\right\}$.

Then for whichever of the above cases holds by the continuity of $g^{(1)}(z,1)$ we have $g^{(1)}(z,1) > 0$ for each element z of the closed interval $[\alpha_i - \delta_i, \alpha_i + \delta_i]$. Suppose there exists a real number $z_o \in [\alpha_i - \delta_i, \alpha_i + \delta_i]$ such that

$$(5.4) \qquad g^{(1)}(z_o,1) < \min\{g^{(1)}(\alpha_i - \delta_i,1), g^{(1)}(\alpha_i + \delta_i,1)\}.$$

Then $g^{(1)}(z,1)$ has a relative minimum on the open interval $(\alpha_i - \delta_i, \alpha_i + \delta_i)$, say at z_1. Therefore $g^{(1)}(z_1,1) > 0$ and $g^{(2)}(z_1,1) = 0$. Define $M_i = \frac{g^{(1)}(z_1,1)}{2}$. If there does not exist a real number z_o such that inequality (5.4) holds, then define $2M_i$ to be the right-hand member of inequality (5.4). Therefore for whichever case holds $g^{(1)}(z,1) > M_i$ whenever z is real and $|z - \alpha_i| < \delta_i$. Since the degree of g is three or four, only a finite number of steps is required to determine which definitions of δ_i and M_i apply. Clearly M_i and δ_i can be found in a finite number of steps.

Suppose $g^{(1)}(\alpha_i,1) < 0$. Then $-g^{(1)}(\alpha_i,1) > 0$. By the above argument positive constants δ_i and M_i can be found in a finite number of steps such that $-g^{(1)}(z,1) = |g^{(1)}(z,1)| > M_i$ whenever z is real and $|z - \alpha_i| < \delta_i$. ‖

References

1. A. Baker, "On the Representations of Integers by Binary Forms", Phil. Trans. R. Soc., 263(1968), 173-191.
2. W. S. Burnside and A. W. Panton, The Theory of Equations, 1, Dublin, Hodges, Figgis, and Co. (Ltd) (1904).
3. I. N. Herstein, Topics in Algebra, Waltham, Mass., Blaisdell Publishing Co. (1964), 192.
4. L. J. Mordell, Diophantine Equations, New York, Academic Press Inc. (1969), 188.
5. T. Nagell, Introduction to Number Theory, New York, John Wiley and Sons, Inc. (1951), 204-208.
6. I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, New York, John Wiley and Sons, Inc. (1966), 151-181.
7. A. Thue, "Über Annäherungswerte algebraischer Zahlen", discussed by L. J. Mordell in Diophantine Equations, New York, Academic Press Inc., (1969), 186-198.
8. H. W. Turnbull, The Theory of Determinants, Matrices, and Invariants, New York, Dover Publications, Inc. (1960), 139.