THE SOLUTION OF EQUATIONS IN INTEGERS

APPROVED:

Major Professor

Minor Professor

Director of the Department of Mathematics

Dean of the Graduate School
THE SOLUTION OF EQUATIONS IN INTEGERS

THESIS

Presented to the Graduate Council of the
North Texas State University in Partial
Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

By

Billy D. Read, B. S.
Denton, Texas
January, 1964
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. FIRST DEGREE EQUATIONS</td>
<td>5</td>
</tr>
<tr>
<td>III. SECOND DEGREE EQUATIONS</td>
<td>19</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>35</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

This paper is devoted to finding integral solutions of algebraic equations. Only algebraic equations with integral coefficients are considered. The elementary properties of integers are assumed.

A number of definitions and fundamental theorems, without proof, are stated in this chapter to simplify the solving of algebraic equations in integers.

**Definition 1.1** -- An integer \( a \), not zero, divides an integer \( b \) if there is an integer \( k \) such that \( b = ka \). \( a \mid b \) means \( a \) divides \( b \).

**Definition 1.2** -- The integer \( a \) is a common divisor of \( b \) and \( c \) means \( a \mid b \) and \( a \mid c \). Since there is only a finite number of divisors of any non-zero integer, there is only a finite number of common divisors of \( b \) and \( c \), except where \( b = c = 0 \). If at least one of \( b \) and \( c \) is not zero, the greatest among their common divisors is called the greatest common divisor of \( b \) and \( c \), and is denoted by \( (b,c) \). Similarly the greatest common divisor of the integers \( a,b,c,...,n \), not all zero, is denoted by \( (a,b,c,...,n) \).

**Definition 1.3** -- \( a/b \) is an irreducible fraction means \( b \neq 0 \) and \( (a,b) = 1 \).
Theorem 1.4 -- If \( g = (a, b) \) and \( a = ga' \) and \( b = gb' \) then \( (a', b') = 1 \).

Theorem 1.5 -- If \( (x, y) = 1 \) and \( x|yz \) then \( x|z \).

Theorem 1.6 -- If \( g^2 | z^2 \) then \( g | z \).

Theorem 1.7 -- If \( a \) and \( b \) are positive integers then there exist an integer \( q \geq 0 \) and an integer \( r \) such that \( a = qb + r \), where \( 0 \leq r < b \). If \( b \nmid a \), then \( r \) satisfies the stronger inequalities \( 0 < r < b \).

Theorem 1.8 -- If \( a \) and \( b \) are positive integers then, by repeated application of theorem 1.7, one obtains a series of equations

\[
\begin{align*}
a &= q_1 b + r_1, \\
b &= q_2 r_1 + r_2, \\
r_1 &= q_3 r_2 + r_3, \\
&\quad\quad \cdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \\
r_{n-1} &= q_{n+1} r_n,
\end{align*}
\]

where \( 0 \leq r_1 < b \) and \( 0 \leq r_i < r_{i-1} \) for \( 1 < i \leq n \). The greatest common divisor \((a, b)\) of \( a \) and \( b \) is \( r_n \), the last non-zero remainder in the division process.

Definition 1.9 -- A regular continued fraction is an expression of the form

\[
q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\cdots}}}
\]
where the $q_n$, $n = 1, 2, 3, \ldots$, are positive integers. The $q_n$ are called the elements of the regular continued fraction.

**Definition 1.10** -- The $k$-th convergent, $\Delta_k$, is obtained from a regular continued fraction and

$$
\Delta_k = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_k}}}.
$$
CHAPTER BIBLIOGRAPHY

CHAPTER II

FIRST DEGREE EQUATIONS

**Definition 2.1** -- ax = c has a solution means there is an integer k such that ak = c.

**Definition 2.2** -- $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$, for $n > 1$, has a solution means there are integers $x_1', x_2', \ldots, x_n'$ such that $a_1x_1' + a_2x_2' + \ldots + a_nx_n' = c$. A solution is denoted by $[x_1', x_2', \ldots, x_n']$.

**Theorem 2.3** -- ax = c has a solution if and only if a | c.

Proof: If a | c then there exists an x such that ax = c. If ax = c has a solution $x = x_o$, then $ax_o = c$ so that a | c.

Consider the first degree equations in two unknowns

ax + by = c.

**Theorem 2.4** -- If ax + by = c has a solution then $(a, b) | c$.

Proof: Let $[x_o, y_o]$ be a solution and let $d = (a, b)$, then $a = dm$ and $b = dn$ where $(m, n) = 1$. Consequently

$$d(mx_o + ny_o) = dmx_o + dny_o = ax_o + by_o = c,$$

and d | c.

Only equations of the form ax + by = c where $(a, b) = 1$ will be considered now.

**Theorem 2.5** -- Let $[x_o, y_o]$ be a solution of

$$ax + by = c$$

(1)
then \( x = x_0 - bt, \ y = y_0 + at, \) for \( t = 0, 1, 2, \ldots \), give all the solutions of (1).

Proof: Let \([x, y]\) be an arbitrary solution of (1).

Then from the equalities

\[
ax + by = c \quad \text{and} \quad ax_0 + by_0 = c
\]

one obtains

\[
ax - ax_0 + by - by_0 = 0,
\]

\[
b(y - y_0) = a(x_0 - x).
\]

By theorem 1.5 \( b \mid (x_0 - x) \) and \( x_0 - x = bt \) for some integer \( t \).

Then \( b(y - y_0) = abt \) and \( y - y_0 = at \). hence the arbitrary solution \([x, y]\) is of the form

\[
x = x_0 - bt, \ y = y_0 + at.
\]

It is necessary to prove \( x = x_0 - bt \) and \( y = y_0 + at \) is a solution of (1) for any choice of \( t \).

\[
ax + by = a(x_0 - bt) + b(y_0 + at)
\]

\[
= ax_0 - abt + by_0 + abt
\]

\[
= ax_0 + by_0
\]

\[
= c.
\]

Therefore \([x, y]\) is a solution of (1) and the theorem is proved.

Consequently, if one solution \([x_0, y_0]\) of the equation \( ax + by = c \) is known, then all the remaining solutions can be found from the arithmetic progressions whose general terms are

\[
x = x_0 - bt, \ y = y_0 + at \quad (t = 0, 1, 2, \ldots).
\]
Consider the positive integers \(|a|\) and \(|b|\). By

theorem 1.8

\[ |a| = q_1 |b| + r_1, \quad 0 < r_1 < |b| \]
\[ |b| = q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \]
\[ r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \]

\[ \cdots \cdots \cdots \cdots \cdots \cdots \]

\[ r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \]

\[ r_{n-1} = q_{n+1} r_n, \]

where \( r_n = (a, b) \). Change the form of the above equations to

\[ \frac{|a|}{|b|} = q_1 + \frac{1}{\frac{|b|}{r_1}} \]
\[ \frac{|b|}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}} \]
\[ \frac{r_1}{r_2} = q_3 + \frac{1}{\frac{r_2}{r_3}} \]

\[ \cdots \cdots \cdots \cdots \cdots \cdots \]

\[ \frac{r_{n-2}}{r_{n-1}} = q_n + \frac{1}{\frac{r_{n-1}}{r_n}} \]

\[ \frac{r_{n-1}}{r_n} = q_{n+1} \]

Replace \( \frac{|b|}{r_1} \) in the first equation of (2), by its equal from the second equation of (2). Replace \( \frac{r_1}{r_2} \), in the second equation, by its equal in the third equation.

Continue in this manner and obtain \( |a| / |b| \) as a regular
continued fraction, that is

\[
\frac{|a|}{|b|} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_n + q_{n+1}}}}.
\]  

(3)

**Definition 2.6** -- \(P_0 = 1, Q_0 = 0, P_1 = q_1\) and \(Q_1 = 1\).

\(P_k = P_{k-1}q_k + P_{k-2}\) and \(Q_k = Q_{k-1}q_k + Q_{k-2}\) for \(k \geq 2\).

**Theorem 2.7** -- Any convergent obtained from the regular continued fraction in equation (3) satisfies

\[
\Delta_n = \frac{P_n}{Q_n}.
\]

**Proof:** The theorem is proved by mathematical induction. For \(n = 1\):

\[
\Delta_1 = q_1 + \frac{q_1}{1} = \frac{P_1}{Q_1}.
\]

For \(n = 2\):

\[
\Delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1q_2 + 1}{q_2} = \frac{P_1q_2 + P_0}{Q_1q_2 + Q_0} = \frac{P_2}{Q_2}.
\]

Assume that \(\Delta_k = \frac{P_k}{Q_k}\). From the definition of the convergent \(\Delta_k\), it follows that if \(q_k\) is replaced by \(q_k + 1/q_{k+1}\), then \(\Delta_k\) is changed to \(\Delta_{k+1}\). From the assumption one obtains

\[
\Delta_k = \frac{P_k}{Q_k} = \frac{P_{k-1}q_k + P_{k-2}}{Q_{k-1}q_k + Q_{k-2}}.
\]

Replace \(q_k\) by \(q_k + 1/q_{k+1}\), then

\[
\Delta_{k+1} = \frac{P_{k-1}q_k + P_{k-2}}{Q_{k-1}q_k + Q_{k-2}},
\]

\[
\Delta_{k+1} = \frac{P_{k-1}\left[q_k + \frac{1}{q_{k+1}}\right] + P_{k-2}}{Q_{k-1}\left[q_k + \frac{1}{q_{k+1}}\right] + Q_{k-2}}.
\]
\[ \Delta_{k+1} = \frac{P_{k-1}q_kq_{k+1} + P_{k-1} + P_{k-2}q_{k+1}}{q_{k-1}q_kq_{k+1} + q_{k-1} + q_{k-2}q_{k+1}} \]

\[ = \frac{(P_{k-1}q_k + P_{k-2})q_{k+1} + P_{k-1}}{(q_{k-1}q_k + q_{k-2})q_{k+1} + q_{k-1}} \]

\[ = \frac{P_kq_{k+1} + P_{k-1}}{q_kq_{k+1} + q_{k-1}} \]

\[ = \frac{P_{k+1}}{Q_{k+1}}. \]

Therefore, \( \Delta_n = \frac{P_n}{Q_n} \).

**Theorem 2.8** -- The difference in the two convergents \( \Delta_k \) and \( \Delta_{k-1} \) is

\[ \Delta_k - \Delta_{k-1} = \frac{(-1)^k}{Q_kQ_{k-1}}. \]

**Proof:** Write \( \Delta_k \) and \( \Delta_{k-1} \) as \( \frac{P_k}{Q_k} \) and \( \frac{P_{k-1}}{Q_{k-1}} \). Then

\[ \Delta_k - \Delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_kQ_{k-1} - P_{k-1}Q_k}{Q_kQ_{k-1}}. \]

From definition 2.6, it follows that

\[ P_kQ_{k-1} - P_{k-1}Q_k = (P_{k-1}q_k + P_{k-2})Q_{k-1} - P_{k-1}(q_{k-1}q_k + q_{k-2}) \]

\[ = (-1)(P_{k-1}q_{k-2} - P_{k-2}q_{k-1}) \]

\[ = (-1)^2(P_{k-2}q_{k-3} - P_{k-3}q_{k-2}) \]

\[ \ldots \ldots \ldots \ldots \ldots \ldots \]

\[ = (-1)^{k-2}(q_1q_2 + 1 - q_1q_2) \]

\[ = (-1)^k. \]

Therefore,

\[ \Delta_k - \Delta_{k-1} = \frac{P_kQ_{k-1} - P_{k-1}Q_k}{Q_kQ_{k-1}} = \frac{(-1)^k}{Q_kQ_{k-1}}. \]
Theorem 2.9 -- \((P_n, Q_n) = 1\), where \(\Delta_n = \frac{P_n}{Q_n}\).

Proof: Let \(g = (P_n, Q_n)\), then \(P_n = gp_n^1\) and \(Q_n = gq_n^1\).

It was found in proving theorem 2.8 that

\[ P_nq_{n-1} - P_{n-1}q_n = (-1)^n. \]

Consequently,

\[ g(P_nq_{n-1} - P_{n-1}q_n) = \frac{P_nq_{n-1} - P_{n-1}q_n}{q_n} = (-1)^n. \]

Therefore \(g|1\) and hence \(g = 1\).

Theorem 2.10 -- The difference in the two convergents \(\Delta_k\) and \(\Delta_{k-2}\) is

\[ \Delta_k - \Delta_{k-2} = \frac{(-1)^k - 1}{q_kq_{k-2}}. \]

Proof: From theorem 2.8 one obtains

\[ \Delta_k - \Delta_{k-1} = \frac{(-1)^k}{q_kq_{k-1}} \quad \text{and} \quad \Delta_{k-1} - \Delta_{k-2} = \frac{(-1)^{k-1}}{q_{k-1}q_{k-2}}. \]

The addition of these two equations gives

\[ \Delta_k - \Delta_{k-2} = \frac{(-1)^k}{q_kq_{k-1}} + \frac{(-1)^{k-1}}{q_{k-1}q_{k-2}} \]

\[ = \frac{(-1)^{k-1}q_k - q_{k-2}}{q_kq_{k-1}q_{k-2}} \]

\[ = \frac{(-1)^{k-1}q_{k-1}q_k}{q_kq_{k-1}q_{k-2}} \]

\[ = \frac{(-1)^{k-1}q_k}{q_kq_{k-2}}. \]

Therefore,

\[ \Delta_k - \Delta_{k-2} = \frac{(-1)^k}{q_kq_{k-2}}. \]
Theorem 2.11 -- \(|a| \frac{|a|}{|b|} = \frac{P_{n-1} r_n + P_n r_{n-1}}{Q_n-1 r_n + Q_n r_{n-1}}\) for \(n > 1\), where the \(r_n\) are the \(r_n\) in equations (2).

Proof: The theorem is proved by mathematical induction.

For \(n = 2\):

\[ |a| = q_1 + \frac{1}{r_2} = q_1 + \frac{r_1}{q_2 r_1 + r_2} \]

\[ = \frac{q_1 q_2 r_1 + q_1 r_2 + r_1}{q_2 r_1 + r_2} = \frac{q_1 r_2 + (q_1 q_2 + 1)r_1}{r_2 + q_2 r_1} \]

\[ = \frac{p_1 r_2 + p_2 r_1}{q_1 r_2 + q_2 r_1}. \]

Hence the theorem is true for \(n = 2\). Assume that

\[ |a| = \frac{P_k-1 r_k + P_k r_{k-1}}{Q_k-1 r_k + Q_k r_{k-1}}. \]

Consequently,

\[ |a| = \frac{P_k-1 r_k + P_k r_{k-1}}{Q_k-1 r_k + Q_k r_{k-1}} = \frac{(P_k+1 - P_k q_{k-1}) r_k + P_k r_{k-1}}{(Q_k+1 - Q_k q_{k-1}) r_k + Q_k r_{k-1}} \]

\[ = \frac{P_k r_{k-1} - P_k q_{k+1} r_k + P_k+1 r_k}{Q_k r_{k-1} - Q_k q_{k+1} r_k + Q_k+1 r_k} \]

\[ = \frac{p_k (r_{k-1} - q_{k+1} r_k) + p_{k+1} r_k}{q_k (r_{k-1} - q_{k+1} r_k) + q_{k+1} r_k} \]

\[ = \frac{p_k r_{k+1} + p_{k+1} r_k}{q_k r_{k+1} + q_{k+1} r_k}. \]

Therefore,

\[ |a| = \frac{p_n-1 r_n + p_n r_{n-1}}{q_n-1 r_n + q_n r_{n-1}}. \]
**Theorem 2.12** -- The convergents obtained from the expansion of the irreducible fraction \( \frac{a}{b} \) into a regular continued fraction satisfy the inequalities

\[
\Delta_1 < \Delta_3 < \ldots < \Delta_{2k-1} < \ldots < \frac{|a|}{|b|} < \Delta_{2k} < \ldots < \Delta_4 < \Delta_2.
\]

**Proof:** One obtains from theorem 2.10 that

\[
\Delta_{2k+1} - \Delta_{2k-1} = \frac{(-1)^{2k} q_{2k+1}}{Q_{2k+1} Q_{2k-1}} > 0,
\]

since \( q_{2k+1} \), \( Q_{2k+1} \) and \( Q_{2k-1} \) are all positive. Therefore,

\[
\Delta_{2k-1} < \Delta_{2k+1}.
\]

The proof that \( \Delta_{2k+2} < \Delta_{2k} \) is similar.

It is necessary to prove that \( \frac{|a|}{|b|} > \Delta_{2k-1} \). The \( r_n \) and \( Q_n \) are all positive, consequently

\[
\frac{r_{2k-1} (-1)^{2k}}{Q_{2k-1} (Q_{2k-1} r_{2k} + Q_{2k} r_{2k-1})} > 0,
\]

\[
\frac{r_{2k-1} (P_{2k} q_{2k-1} - P_{2k-1} q_{2k})}{Q_{2k-1} (Q_{2k-1} r_{2k} + Q_{2k} r_{2k-1})} > 0,
\]

\[
\frac{P_{2k} q_{2k-1} r_{2k} - P_{2k-1} q_{2k} r_{2k-1}}{Q_{2k-1} (Q_{2k-1} r_{2k} + Q_{2k} r_{2k-1})} > 0,
\]

\[
\frac{P_{2k-1} r_{2k} + P_{2k} r_{2k-1}}{Q_{2k-1} r_{2k} + Q_{2k} r_{2k-1}} - \frac{P_{2k-1}}{Q_{2k-1}} > 0,
\]

and by theorem 2.11

\[
\frac{|a|}{|b|} - \Delta_{2k-1} > 0
\]

and

\[
\frac{|a|}{|b|} > \Delta_{2k-1}.
\]

The proof that \( \frac{|a|}{|b|} < \Delta_{2k} \) is similar.
Theorem 2.13 -- A solution to the equation \(ax + by = c\) is 
\(x_0 = \frac{la}{a}(-1)^nc_{n-1}, \ y_0 = \frac{lb}{b}(-1)^{n+1}c_{n-1}\), where \(n\) is the number of elements in the expansion of the irreducible fraction \(\frac{la}{b}\) into a regular continued fraction (1, p. 13).

Proof: Let \(n\) be the number of elements in the expansion of \(\frac{la}{b}\) into a regular continued fraction. It is evident that the convergent \(\Delta_n\) is equal to \(\frac{la}{b}\). By theorem 2.8,
\[
\Delta_n - \Delta_{n-1} = \frac{(-1)^n}{Q_nQ_{n-1}}
\]
and
\[
\frac{la}{b} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{|b|Q_{n-1}}.
\]
Consequently,
\[
|a|Q_{n-1} - |b|P_{n-1} = (-1)^n,
\]
\[
|a|Q_{n-1} + |b|(-1)P_{n-1} = (-1)^n,
\]
\[
|a|(-1)^nc_{n-1} + |b|(-1)^{n+1}c_{n-1} = c,
\]
and finally,
\[
a\left[\frac{la}{a}(-1)^nc_{n-1}\right] + b\left[\frac{lb}{b}(-1)^{n+1}c_{n-1}\right] = c.
\]

Definition 2.14 -- Let \(x\) be any real number. The symbol \([x]\) will denote the largest integer less than or equal to \(x\).

Theorem 2.15 -- Let \(x\) and \(y\) each denote a real number, then \([x] + [y] \leq [x + y] \leq [x] + [y] + 1\).

Proof: Let \(x = n + \nu\) and \(y = m + \mu\) where \(n\) and \(m\) are integers and \(0 \leq \nu < 1, \ 0 \leq \mu < 1\). Then
\[
[x] + [y] = n + m \leq n + m + [\nu + \mu],
\]
\[ [x] + [y] \leq [n + v + m + \mu] \]
\[ = [x + y]. \]
Since \( v + \mu < 1 + 1 = 2 \), it follows that \([v + \mu] \leq 1\). Then
\[ [x + y] = [n + v + m + \mu] \]
\[ = n + m + [v + \mu] \]
\[ \leq [x] + [y] + 1. \]

**Theorem 2.16** -- The largest integer less than \( x \) is \(-[-x + 1]\).

**Proof:** Let \( x = n + v \), where \( n \) is an integer and \( 0 \leq v < 1 \).

Case I. If \( v > 0 \) then the largest integer less than \( x \) is \( n \) and
\[ n = -(-n) = -[-n - v + 1] = -[-(n + v) + 1] = -[-x + 1]. \]

Case II. If \( v = 0 \) then the largest integer less than \( x \) is \( n - 1 \) and
\[ n - 1 = -(-n + 1) = -[-n + 1] = -[-x + 1]. \]

**Definition 2.17** -- A positive solution of \( ax + by = c \) is a solution \([x', y']\) such that \( x' > 0 \) and \( y' > 0 \).

**Theorem 2.18** -- Let \( a, b \) and \( c \) denote positive integers such that \((a, b) | c\). Let \( g = (a, b) \). Then
\[ \left\lfloor \frac{ge}{ab} \right\rfloor - 1 \leq N \leq \left\lceil \frac{ge}{ab} \right\rceil, \]
where \( N \) is the number of positive solutions of \( ax + by = c \) (2, p. 96).

**Proof:** Since \( g = (a, b) \), then \( a = ga' \) and \( b = gb' \), where \((a', b') = 1\). There exists a solution \([x_0, y_0]\) of
\[ a'x + b'y = c/g \]
by theorem 2.13, that is

\[ a'x_o + b'y_o = c/g, \]
\[ ga'x_o + gb'y_o = c, \]
\[ ax_o + by_o = c. \]

All solutions of \( a'x + b'y = c/g \) are given by

\[ x = x_o - b't, \quad y = y_o + a't \]

from theorem 2.5, so that

\[ a'(x_o - b't) + b'(y_o + a't) = c/g, \]
\[ ga'(x_o - b't) + gb'(y_o + a't) = c, \]
\[ a(x_o - b't) + b(y_o + a't) = c. \]

Since the solutions are to be positive then \( t \) has to be chosen so as to make \( x_o - \frac{b}{g}t > 0 \) and \( y_o + \frac{a}{g}t > 0 \). Combining these two inequalities gives

\[ -\frac{g}{a}y_o < t < \frac{g}{b}x_o. \]

The smallest integer larger than \( -\frac{g}{a}y_o \) is

\[ \left[ -\frac{g}{a}y_o \right] + 1 = \left[ -\frac{g}{a}y_o + 1 \right]. \]

by theorem 2.16, the largest integer less than \( \frac{g}{b}x_o \) is

\[ \left[ -\frac{g}{b}x_o + 1 \right]. \]

Hence the number of positive solutions is

\[ n = \left[ -\frac{g}{b}x_o + 1 \right] - \left[ -\frac{g}{a}y_o + 1 \right] + 1 \]
\[ = -\left[ -\frac{g}{b}x_o \right] - \left[ -\frac{g}{a}y_o \right] - 1 \]
\[ = -\left( \left[ -\frac{g}{b}x_o \right] + \left[ -\frac{g}{a}y_o \right] + 1 \right). \]

Therefore, by theorem 2.15,

\[ -\left( \left[ \frac{g}{b}x_o - \frac{g}{a}y_o \right] + 1 \right) \leq n \leq -\left[ \frac{g}{b}x_o - \frac{g}{a}y_o \right]. \]
Since \(-\frac{g}{b} x_0 - \frac{g}{a} y_0 = -\frac{g}{ab} (ax_0 + by_0) = -\frac{gc}{ab}\), then
\[-\left[\frac{gc}{ab}\right] - 1 \leq N \leq -\left[\frac{gc}{ab}\right].
\]

**Theorem 2.19** -- If \((a, b) = 1\) and \(a\) and \(b\) are of different sign, then \(ax + by = c\) has an infinite number of positive solutions for any value of \(c\).

**Proof:** Case I. Assume that \(a > 0\) and \(b < 0\). By theorem 2.13, the equation \(ax + by = c\) has a solution \([x_0, y_0]\).

By theorem 2.5, all of the solutions are given by

\[x = x_0 - bt, \ y = y_0 + at \ \text{for} \ t = 0, 1, 2, \ldots \]

Since the solutions are to be positive then
\[x_0 - bt > 0 \ \text{and} \ y_0 + at > 0,\]
\[-bt > -x_0 \ \text{and} \ at > -y_0,\]
\[t > \frac{x_0}{b} \ \text{and} \ t > -\frac{y_0}{a}.\]

Let \(M\) be the maximum of \(\frac{x_0}{b}\) and \(-\frac{y_0}{a}\). If \(t > M\), then the solutions will be positive and there is certainly an infinite number of values of \(t > M\), hence there is an infinite number of positive solutions.

Case II. Assume that \(a < 0\) and \(b > 0\). The proof follows similarly to that in case I.

Consider the general linear equation
\[a_1 x_1 + a_2 x_2 + \ldots + a_{n-1} x_{n-1} + a_n x_n = c.\]
Suppose the coefficients are not zero and \((a_1, a_2, \ldots, a_n) \text{c,}\) since, as in theorem 2.4, if there is a solution, then \((a_1, a_2, \ldots, a_n) \text{c.}\)
Theorem 2.20 -- The general linear equation
\[ a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} + a_nx_n = c \]  \hspace{1cm} (4)
can be reduced to an equation with two variables which can be solved by theorem 2.13 (2, pp. 97-98).

Proof: Write the last two variables, \( x_{n-1} \) and \( x_n \), in terms of two other variables \( u \) and \( v \), that is
\[ x_{n-1} = au + \beta v, \quad x_n = \gamma u + \mu v \]  \hspace{1cm} (5)
where
\[ \beta = \frac{a_n}{(a_{n-1}, a_n)}, \quad \mu = \frac{a_{n-1}}{(a_{n-1}, a_n)}, \]
and \( a \) and \( \gamma \) are such that \( a\mu - \beta\gamma = 1 \), which has a solution \([a, \gamma]\) by theorem 2.13, since \((\beta, \mu) = 1\) by theorem 1.4.
Substitute (5) into (4) and obtain
\[ a_1x_1 + a_2x_2 + \ldots + a_{n-1}(au + \beta v) + a_n(\gamma u + \mu v) = c, \]
\[ a_1x_1 + a_2x_2 + \ldots + (a_{n-1}a + a_n\gamma)u + (a_{n-1}\beta + a_n\mu)v = c. \]  \hspace{1cm} (6)
\[ a_{n-1}\beta + a_n\mu = \frac{a_{n-1}a_n}{(a_{n-1}, a_n)} - \frac{a_{n-1}a_n}{(a_{n-1}, a_n)} = 0. \]
Therefore equation (6) takes the form
\[ a_1x_1 + a_2x_2 + \ldots + (a_{n-1}a + a_n\gamma)u = c, \]  \hspace{1cm} (7)
which has only \( n-1 \) variables. Since
\[ a_{n-1}a + a_n\gamma = -c\mu(a_{n-1}, a_n) + \gamma\beta(a_{n-1}, a_n) = -(a_{n-1}, a_n), \]
one has
\[ (a_1, a_2, \ldots, a_{n-2}, a_{n-1}a + a_n\gamma) | c. \]
If \( n > 3 \) this process can be applied to equation (7) to obtain an equation with \( n - 2 \) variables, and continuation finally leads to an equation with two variables.
CHAPTER BIBLIOGRAPHY


CHAPTER III

SECOND DEGREE EQUATIONS

Consider the solution of
\[ x^2 + y^2 = z^2 \]  
\[ (1) \]
in positive integers. Geometrically one interprets the solving of this equation as finding all right triangles such that the sides \( x, y \) and \( z \) will be integers.

**Lemma 3.1** -- If \( a \) and \( b \) are positive integers such that \((a, b) = 1\) and \(ab = x^2\), then \( a \) and \( b \) are exact squares (2, p. 33).

**Proof:** Let \( g = (a, x) \). Then \( a = gm \) and \( x = gn \) where \((m, n) = 1\). Then \( ab = x^2 \) becomes
\[ gmb = g^2 n^2, \]
\[ mb = gn^2. \]

Since \((m, n) = 1\), then \( n^2 \mid b \) and \( b = pn^2 \) so that
\[ mpn^2 = gn^2, \]
\[ mp = g. \]

Now \((g, p) = 1\), since \((g, p) \mid a, (g, p) \mid b\) and \((a, b) = 1\). Hence \( g \mid m \) and \( m = gq \). Therefore,
\[ gqp = g, \]
\[ qp = 1. \]

Hence \( q = p = 1 \) and \( m = g \). Consequently, \( a = g^2 \) and \( b = n^2 \).
**Definition 3.2** — \( x^2 + y^2 = z^2 \) has a solution means there are integers \( x', y' \) and \( z' \) such that \( x'^2 + y'^2 = z'^2 \). A solution is denoted by \([x', y', z']\).

Consider a solution \([x, y, z]\) and let \( g = (x, y) \). Now \( x = gx' \) and \( y = gy' \) where \((x', y') = 1\). Equation (1) takes the form \( g^2(x'^2 + y'^2) = z^2 \). Therefore \( g^2 \mid z^2 \). By theorem 1.6, \( g \mid z \) and \( z = gz' \). Equation (1) can now be written \( x'^2g^2 + y'^2g^2 = z'^2g^2 \), which reduces to \( x'^2 + y'^2 = z'^2 \).

Consequently, if \([x, y, z]\) is a solution and \( g = (x, y) \) then \([x/g, y/g, z/g]\) is a solution and \((x/g, y/g) = 1\).

**Lemma 3.3** — If \([x, y, z]\) is a solution of (1) and \((x, y) = 1\), then \((x, z) = 1 \) and \((y, z) = 1\).

**Proof:** Let \((x, z) = g\), then \( x = gx' \) and \( z = gz' \). Equation (1) becomes

\[
y^2 = g^2(z'^2 - x'^2).
\]

Therefore \( g^2 \mid y^2 \) and hence \( g \mid y \). Since \((x, y) = 1\), \( g \mid x \), and \( g \mid y \), it follows that \( g = 1 \) and \((x, z) = 1\). The proof that \((y, z) = 1\) is similar.

**Lemma 3.4** — If \([x, y, z]\) is a solution of (1), then \([kx, ky, kz]\), for any integer \( k \), is a solution of (1).

**Proof:** \([x, y, z]\) is a solution of (1) means

\[
x^2 + y^2 = z^2,
\]

\[
k^2x^2 + k^2y^2 = k^2z^2,
\]

\[
(kx)^2 + (ky)^2 = (kz)^2.
\]

Hence, \([kx, ky, kz]\) is a solution of (1).
**Definition 3.5** -- A primitive solution of (1) is a solution \([x,y,z]\) where \((x,y) = 1\).

Only primitive solutions will be considered now. Since \((x,y) = 1\), both \(x\) and \(y\) can not be even.

**Lemma 3.6** -- If \([x,y,z]\) is a solution of (1), then \(x\) and \(y\) can not both be odd.

**Proof:** Suppose \(x\) and \(y\) are both odd then they can be written in the form \(x = 2n + 1\) and \(y = 2m + 1\). Then
\[
x^2 + y^2 = 4n^2 + 4n + 1 + 4m^2 + 4m + 1, \\
x^2 + y^2 = 2 \left( 2(n^2 + n + m^2 + m) + 1 \right) = z^2.
\] (2)

Since \(x\) and \(y\) are both odd, it follows that \(x^2\) and \(y^2\) are odd and \(x^2 + y^2\) is even. Hence \(z^2\) is even and \(z\) is even.

\(z\) is even implies \(4z^2\) but from (2) it is clear that \(4z^2\).

Consequently, \(x\) and \(y\) can not both be odd.

Of the two numbers \(x\) and \(y\), one is odd and the other is even. Without any loss in generality, suppose \(x\) is odd and \(y\) is even.

**Theorem 3.7** -- All primitive solutions \([x,y,z]\) of
\[
x^2 + y^2 = z^2
\] (3)
are given by
\[
x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2},
\]
where \(u\) and \(v\) are odd, \((u,v) = 1\) and \(u > v > 0\).

**Proof:** Write equation (3) in the form
\[
x^2 = z^2 - y^2, \\
x^2 = (z + y)(z - y).
\] (4)
Let \( g = (x + y, z - y) \). Then
\[
z + y = ag \quad \text{and} \quad z - y = bg
\]
where \((a, b) = 1\). Substitute these values into (4) and obtain
\[
x^2 = abg^2.
\]
Since \( x \) is odd, \( x^2 \) is odd and \( a, b \) and \( g \) are odd. By adding and subtracting the equations in (5) one obtains
\[
2z = g(a + b) \quad \text{and} \quad 2y = g(a - b).
\]
Hence \( g | 2z \) and \( g | 2y \). Now \( g \) being odd implies \( g | z \) and \( g | y \), but \((z, y) = 1\), hence \( g = 1 \). Equation (6) may now be written
\[
x^2 = ab,
\]
where \((a, b) = 1\). By lemma 3.1, \( a = u^2 \) and \( b = v^2 \). Then
\[
x^2 = u^2v^2,
x = uv,
\]
where \( u \) and \( v \) are odd since \( a \) and \( b \) are odd. Equation (7) may now be written
\[
z = \frac{u^2 + v^2}{2}, \quad \text{and} \quad y = \frac{u^2 - v^2}{2}.
\]
Therefore all solutions of (3) are given by
\[
x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2},
\]
where \( u \) and \( v \) are odd, \((u, v) = 1\), and \( u > v > 0 \). Now
\[
x^2 + y^2 = (uv)^2 + \left(\frac{u^2 - v^2}{2}\right)^2
= \frac{4u^2v^2}{4} + \frac{u^4 - 2u^2v^2 + v^4}{4},
\]
\[ x^2 + y^2 = \frac{u^4 + 2u^2v^2 + v^4}{4} = \left(\frac{u^2 + v^2}{2}\right)^2 = z^2. \]

Consequently \(x, y\) and \(z\) obtained from (8) for any \(u\) and \(v\), will be a solution of (3).

Consider the solution of \(x^2 - 2y^2 = 1\) in positive integers. To solve this equation it will be useful to have the regular continued fraction for \(\sqrt{2}\), which is irrational. The regular continued fraction will have an infinite number of elements, since if it has only \(n\) elements then \(\sqrt{2} = \frac{p_n}{q_n}\), which is rational. From the identity

\[(\sqrt{2} - 1)(\sqrt{2} + 1) = 1,
\]

it follows that

\[\sqrt{2} - 1 = \frac{1}{\sqrt{2} + 1}, \tag{9}\]

\[\sqrt{2} - 1 = \frac{1}{2 + (\sqrt{2} - 1)}. \tag{10}\]

Replace \(2 - 1\) in the denominator of (10) by its equal from (9) and obtain

\[\sqrt{2} - 1 = \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} - 1}}}}.\]

Continuing this process, one obtains the following expansion of \(\sqrt{2}\) into an infinite regular continued fraction:

\[\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ldots}}}. \tag{11}\]
The convergent $\Delta_k$, obtained from (11), satisfies $\Delta_k = \frac{p_k}{q_k}$, since in the proof of theorem 2.7 the fact that there was only a finite number of elements was nowhere used. Also the difference in the two convergents $\Delta_k$ and $\Delta_{k-1}$, obtained from (11), is

$$\Delta_k - \Delta_{k-1} = \frac{(-1)^k}{q_k q_{k+1}}.$$ Therefore,

$$\Delta_{2k} - \Delta_{2k+1} = -\left(\Delta_{2k+1} - \Delta_{2k}\right) = -\frac{(-1)^{2k+1}}{q_{2k} q_{2k+1}} = \frac{1}{q_{2k} q_{2k+1}}.$$ (12)

**Theorem 3.8** -- The convergents obtained from (11) satisfy

$$\Delta_1 < \Delta_3 < \ldots < \Delta_{2k-1} < \ldots < \sqrt{2} < \ldots < \Delta_{2k} < \ldots < \Delta_4 < \Delta_2.$$ (13)

The proof is similar to the proof of theorem 2.12.

**Lemma 3.9** -- The numerator $p_{2k}$ and the denominator $q_{2k}$ of the convergent $\Delta_{2k}$ satisfy the inequalities

$$0 < p_{2k} - \sqrt{2} q_{2k} < \frac{1}{q_{2k+1}}.$$ (14)

for $k \geq 1$.

Proof: From (13), one finds that

$$\sqrt{2} < \Delta_{2k} = \frac{p_{2k}}{q_{2k}},$$
hence

$$\sqrt{2} q_{2k} < p_{2k},$$

$$0 < p_{2k} - \sqrt{2} q_{2k},$$

and the left side of (14) is proved. From (13), one also
finds that
\[
\Delta_{2k+1} < \sqrt{2},
\]
\[-\sqrt{2} < -\Delta_{2k+1}.
\]

Hence, by (12), it follows that
\[
\Delta_{2k} - \sqrt{2} < \Delta_{2k} - \Delta_{2k+1} = \frac{1}{q_{2k}q_{2k+1}}.
\]

Replace \( \Delta_{2k} \) by \( \frac{P_{2k}}{Q_{2k}} \) and obtain
\[
\frac{P_{2k}}{Q_{2k}} - \sqrt{2} < \frac{1}{q_{2k}q_{2k+1}},
\]
\[
P_{2k} - \sqrt{2}q_{2k} < \frac{1}{q_{2k+1}},
\]
which is the right side of the inequalities in (14).

**Definition 3.10** -- \( x^2 - 2y^2 = 1 \) has a solution means there are integers \( x' \) and \( y' \) such that \( x'^2 - 2y'^2 = 1 \). A solution is denoted by \([x',y']\).

**Theorem 3.11** -- For \( k \geq 1 \), \( x = P_{2k} \) and \( y = q_{2k} \) is a solution of
\[
x^2 - 2y^2 = 1,
\]
where \( P_{2k} \) is the numerator and \( q_{2k} \) is the denominator of the convergent \( \Delta_{2k} \) obtained from (11) (1, pp. 24-25).

**Proof:** Write the left side of (15) in the form
\[
x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y).
\]
Replace \( x \) by \( P_{2k} \) and \( y \) by \( q_{2k} \) and obtain
\[
P_{2k}^2 - 2q_{2k}^2 = (P_{2k} - \sqrt{2}q_{2k})(P_{2k} + \sqrt{2}q_{2k}).
\]
Since \( \Delta_{2k} > \sqrt{2} \) from (13), then \( P_{2k}^2 > 2q_{2k}^2 \) and
\( P_{2k}^2 - 2Q_{2k}^2 > 0. \) Therefore \( P_{2k}^2 - 2Q_{2k}^2 \) is a positive integer.

Furthermore, by lemma 3.9,

\[
P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}} = \frac{1}{Q_{2k}Q_{2k+1} + Q_{2k-1}} < \frac{1}{2Q_{2k}}. \tag{17}
\]

From (13), one finds that

\[
\sqrt{2} < \Delta_{2k} = \frac{P_{2k}}{Q_{2k}},
\]

\[
\sqrt{2}Q_{2k} < P_{2k},
\]

\[
P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k}. \tag{18}
\]

Multiply the inequalities from (17) and (18) and obtain

\[
(P_{2k} - \sqrt{2}Q_{2k})(P_{2k} + \sqrt{2}Q_{2k}) < \frac{2P_{2k}}{2Q_{2k}},
\]

\[
P_{2k}^2 - 2Q_{2k}^2 < \frac{P_{2k}}{Q_{2k}}.
\]

Applying lemma 3.9 yields

\[
\sqrt{2}Q_{2k} + \frac{1}{Q_{2k+1}} = \sqrt{2} + \frac{1}{Q_{2k+1}Q_{2k}}.
\]

and since

\[
\frac{1}{Q_{2k+1}Q_{2k}} \leq \frac{1}{Q_{3}Q_{2}} = \frac{1}{10},
\]

then

\[
P_{2k}^2 - 2Q_{2k}^2 < \sqrt{2} + \frac{1}{10} < 2.
\]

Therefore, \( P_{2k}^2 - 2Q_{2k}^2 \) for \( k \geq 1 \), is an integer satisfying

\[
0 < P_{2k}^2 - 2Q_{2k}^2 < 2,
\]

hence

\[
P_{2k}^2 - 2Q_{2k}^2 = 1.
\]

Furthermore, \([\pm P_{2k}, \pm Q_{2k}]\) are also solutions to (15).
Lemma 3.12 -- For \( k \geq 4 \), \( P_k = 6P_{k-2} - P_{k-4} \) and \( Q_k = 6Q_{k-2} - Q_{k-4} \) where \( P_1 \) is the numerator and \( Q_1 \) is the denominator of the convergent \( A_1 \) obtained from (11).

Proof: For \( k > 1 \), \( q_k = 2 \). From definition 2.6, one obtains

\[
P_k = 2P_{k-1} + P_{k-2},
\]

(19)

\[
P_{k-1} = 2P_{k-2} + P_{k-3},
\]

(20)

\[
P_{k-2} = 2P_{k-3} + P_{k-4}.
\]

The last equation may be written

\[
2P_{k-3} = P_{k-2} - P_{k-4}.
\]

(21)

Replace \( P_{k-1} \), in (19), by its equal from (20) and obtain

\[
P_k = 4P_{k-2} + 2P_{k-3} + P_{k-2}.
\]

Replace \( 2P_{k-3} \) by its equal from (21) and obtain

\[
P_k = 4P_{k-2} + P_{k-2} - P_{k-4} + P_{k-2},
\]

\[
P_k = 6P_{k-2} - P_{k-4},
\]

which is the desired result. The proof that

\[
Q_k = 6Q_{k-2} - Q_{k-4}
\]

is similar.

Lemma 3.13 -- Let \( [x', y'] \) be any positive solution of \( x^2 - 2y^2 = 1 \), other than \( [3, 2] \), then

\[
x' + y'\sqrt{2} > 3 + 2\sqrt{2}.
\]

Proof: Suppose \( x' + y'\sqrt{2} \leq 3 + 2\sqrt{2} \).

Case I. If \( x' + y'\sqrt{2} = 3 + 2\sqrt{2} \), then

\[
x' - 3 = (2 - y')\sqrt{2}.
\]
This is impossible since the left side is an integer and
the right side is an irrational number.

Case II. Suppose \( x' + y'\sqrt{2} < 3 + 2\sqrt{2} \). Since \( \sqrt{2} < 2 \),
then \( 3 + 2\sqrt{2} < 7 \) and \( x' + y'\sqrt{2} < 7 \), hence
\[ x' < 7 - y'\sqrt{2} \leq 7 - \sqrt{2} < 6. \]
Checking values of \( x' < 6 \), it is clear that \( x' = 3 \) is the
only value for \( x' \) such that \( y' \) will be an integer. Hence,
the lemma is true.

**Lemma 3.14** -- Let
\[ x_n = \frac{1}{2} [(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n], \]
\[ y_n = \frac{1}{2\sqrt{2}} [(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n], \]
then \( x_n \) and \( y_n \) are integers for every integer \( n \).

Proof: The theorem is proved by mathematical induction.

For \( n = 1 \):
\[ x_1 = \frac{1}{2} (3 + 2\sqrt{2} + 3 - 2\sqrt{2}) = 3, \]
\[ y_1 = \frac{1}{2\sqrt{2}} (3 + 2\sqrt{2} - 3 + 2\sqrt{2}) = 2. \]
Therefore, the lemma is true for \( n = 1 \). Assume that
\[ x_{k-1} = \frac{1}{2} [(3 + 2\sqrt{2})^{k-1} + (3 - 2\sqrt{2})^{k-1}] = M \]
and
\[ x_k = \frac{1}{2} [(3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k] = N \]
where \( M \) and \( N \) are integers.
\[ x_{k+1} = \frac{1}{2} [(3 + 2\sqrt{2})^{k+1} + (3 - 2\sqrt{2})^{k+1}], \]
\[ x_{k+1} = \frac{1}{2} \left[ (3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k \right] \left( (3 + 2\sqrt{2}) + (3 - 2\sqrt{2}) \right) \]
\[ - \frac{1}{2} \left[ (3 + 2\sqrt{2})^k (3 - 2\sqrt{2}) + (3 - 2\sqrt{2})^k (3 + 2\sqrt{2}) \right] \]
\[ = (\text{even}) 6 - \frac{1}{2} \left[ (3 + 2\sqrt{2})^{k-1} + (3 - 2\sqrt{2})^{k-1} \right] \]
\[ = 6M - N. \]

Therefore, \( x_{k+1} \) is an integer. The proof that \( y_n \) is an integer is similar.

**Theorem 3.15** -- Let \( n \) be a positive integer, then
\[ x_n = \frac{1}{2} \left[ (3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n \right], \]
\[ y_n = \frac{1}{2\sqrt{2}} \left[ (3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n \right] \]

is a solution of \( x^2 - 2y^2 = 1 \).

**Proof:**
\[ x_n^2 - 2y_n^2 = \left\{ \frac{1}{2} \left[ (3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n \right] \right\}^2 \]
\[ - 2 \left\{ \frac{1}{2\sqrt{2}} \left[ (3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n \right] \right\}^2 \]
\[ = \frac{1}{4} (3 + 2\sqrt{2})^{2n} + \frac{1}{2} + \frac{1}{4} (3 - 2\sqrt{2})^{2n} \]
\[ - \frac{1}{4} (3 + 2\sqrt{2})^{2n} + \frac{1}{2} - \frac{1}{4} (3 - 2\sqrt{2})^{2n} \]
\[ = \frac{1}{2} + \frac{1}{2} = 1. \]

Furthermore, \( \pm x_n, \pm y_n \) are also solutions of \( x^2 - 2y^2 = 1 \).

**Theorem 3.16** -- Each solution \( [x_n, y_n] \) obtained from (22) is equal to the solution \( [P_{2n}, Q_{2n}] \), where \( P_{2n} \) is the numerator and \( Q_{2n} \) is the denominator of the convergent \( \Delta_{2n} \) obtained from (11).
Proof: The theorem is proved by mathematical induction.

For \( n = 1 \):

\[ x_1 = \frac{1}{2} (3 + 2\sqrt{2} + 3 - 2\sqrt{2}) = 3 = p_2 \]

and

\[ y_1 = \frac{1}{2\sqrt{2}} (3 + 2\sqrt{2} - 3 + 2\sqrt{2}) = 2 = q_2. \]

Hence the theorem is true for \( n = 1 \). Assume that \( x_k = p_{2k} \),

that is

\[ x_k = \frac{1}{2} [(3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k] = p_{2k}. \]

Now

\[
x_{k+1} = \frac{1}{2} \bigg( (3 + 2\sqrt{2})^{k+1} + (3 - 2\sqrt{2})^{k+1} \bigg)
= \frac{1}{2} \bigg\{ [(3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k] [ (3 + 2\sqrt{2}) + (3 - 2\sqrt{2}) ]
- [(3 + 2\sqrt{2})^k (3 - 2\sqrt{2}) + (3 - 2\sqrt{2})^k (3 + 2\sqrt{2}) ] \bigg\}
= 6 \left( \frac{1}{2} [(3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k] \right)
- \frac{1}{2} \left((3 + 2\sqrt{2})^{k-1} + (3 - 2\sqrt{2})^{k-1}\right).\]

From the assumption, it follows that

\[ x_{k+1} = 6p_{2k} - p_{2k-2}. \]

Hence, by lemma 3.12,

\[ x_{k+1} = p_{2k+2} \]

and consequently, \( x_n = p_{2n} \) for every positive integer \( n \).

The proof that \( y_n = q_{2n} \) is similar.

Theorem 3.17 -- If \( n \) is a positive integer, then

\[ x_n = \frac{1}{2} [(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n], \]

\[ y_n = \frac{1}{2\sqrt{2}} [(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n] \]

give every solution of \( x^2 - 2y^2 = 1 \) (1, p. 28).
Proof: By adding the equations in (23), one obtains
\[ 2x_n + 2\sqrt{2}y_n = 2(3 + 2\sqrt{2})^n, \]
\[ (3 + 2\sqrt{2})^n = x_n + \sqrt{2}y_n. \]  \hspace{1cm} (24)

By subtracting the equations in (23), one obtains
\[ 2x_n - 2\sqrt{2}y_n = 2(3 - 2\sqrt{2})^n, \]
\[ (3 - 2\sqrt{2})^n = x_n - \sqrt{2}y_n. \]

A solution \([x_k, y_k]\) obtained from (23) can be obtained from (24) alone by expanding \((3 + 2\sqrt{2})^k\) by the binomial theorem and letting \(x_n\) be the sum of the rational terms and \(y_n\) be the sum of the coefficients of \(\sqrt{2}\).

Assume there is a solution \([x', y']\) not obtained from (23), that is
\[ x' + \sqrt{2}y' = (3 + 2\sqrt{2})^n \]
is not satisfied for any positive integer \(n\). Consider the increasing unbounded sequence
\[ (3 + 2\sqrt{2}), (3 + 2\sqrt{2})^2, (3 + 2\sqrt{2})^3, \ldots. \]  \hspace{1cm} (25)

By lemma 3.13, it follows that
\[ x' + \sqrt{2}y' > 3 + 2\sqrt{2}. \]

Since \(x' + \sqrt{2}y'\) is larger than the first term of the unbounded sequence (25), then there is a positive integer \(n\) such that
\[ (3 + 2\sqrt{2})^n < x' + \sqrt{2}y' < (3 + 2\sqrt{2})^{n+1}. \]  \hspace{1cm} (26)

Since \((3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1 > 0\), then \((3 - 2\sqrt{2}) > 0\).

Multiply (26) by \((3 - 2\sqrt{2})^n\) and obtain
\[(3 + 2\sqrt{2})^n (3 - 2\sqrt{2})^n < (x' + \sqrt{2}y') (3 - 2\sqrt{2})^n < (3 + 2\sqrt{2})^{n+1} (3 - 2\sqrt{2})^n,\]

\[1 < (x' + \sqrt{2}y') (x_n - \sqrt{2}y_n) < 3 + 2\sqrt{2}. \quad (27)\]

\[(x' + \sqrt{2}y') (x_n - \sqrt{2}y_n) = (x'x_n - 2y'y_n) + \sqrt{2} (x_ny' - x'y_n) = \overline{x} + \sqrt{2}\overline{y},\]

where

\[\overline{x} = x'x_n - 2y'y_n \text{ and } \overline{y} = x_ny' - x'y_n.\]

The inequalities in (27) may now be written

\[1 < \overline{x} + \sqrt{2}\overline{y} < 3 + 2\sqrt{2}. \quad (28)\]

Since

\[\overline{x} - \sqrt{2}\overline{y} = (x'x_n - 2y'y_n) - \sqrt{2} (x_ny' - x'y_n) = (x' - \sqrt{2}y') (x_n + \sqrt{2}y_n) = (x' - \sqrt{2}y') (3 + 2\sqrt{2})^n,\]

then

\[\overline{x}^2 - 2\overline{y}^2 = (\overline{x} + \sqrt{2}\overline{y}) (\overline{x} - \sqrt{2}\overline{y}) = (x' + \sqrt{2}y') (3 - 2\sqrt{2})^n (x' - \sqrt{2}y') (3 + 2\sqrt{2})^n = (x'^2 - 2y'^2)(1)^n = 1.\]

Therefore, \([\overline{x}, \overline{y}]\) is a solution. From (28)

\[1 < \overline{x} + \sqrt{2}\overline{y} < 3 + 2\sqrt{2},\]

but, by lemma 3.13, there is no solution \([\overline{x}, \overline{y}]\) such that

\[\overline{x} + \sqrt{2}\overline{y} < 3 + 2\sqrt{2}.\]

Consequently, the assumption that there is an \([x', y']\), not obtained from (23), is false.

By theorem 3.17, every solution of \(x^2 - 2y^2 = 1\) comes from (23) and, by theorem 3.16, every solution obtained
from (23) is equal to \([P_{2n}, Q_{2n}]\) for some \(n\). Hence, every solution of \(x^2 - 2y^2 = 1\) is of the form \([P_{2n}, Q_{2n}]\) and, by theorem 3.11, every \([P_{2n}, Q_{2n}]\) is a solution.
CHAPTER BIBLIOGRAPHY


BIBLIOGRAPHY

Books

