SOME DIOPHANTINE EQUATIONS

APPROVED:

George Copp
Major Professor

H.C. Parrish
Minor Professor

H.C. Parrish
Director of the Department of Mathematics

Robert B. Toulouze
Dean of the Graduate School
SOME DIOPHANTINE EQUATIONS

THESIS

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

For the Degree of

MASTER OF ARTS

By

Kirby Smith Pressly, B. A.

Denton, Texas
January, 1960
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>FIRST DEGREE DIOPHANTINE EQUATIONS</td>
<td>1</td>
</tr>
<tr>
<td>II.</td>
<td>SYSTEMS OF FIRST DEGREE DIOPHANTINE EQUATIONS</td>
<td>19</td>
</tr>
<tr>
<td>III.</td>
<td>A QUADRATIC DIOPHANTINE EQUATION</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>BIBLIOGRAPHY</td>
<td>33</td>
</tr>
</tbody>
</table>
CHAPTER I

FIRST DEGREE DIOPHANTINE EQUATIONS

This paper will be devoted to an examination of several general and specific equations and systems of equations of the diophantine type. Only algebraic equations with integral coefficients, not all zero, will be considered. The elementary properties of the integers will be assumed.

1.1 Definition. -- An indeterminate equation is an equation in two or more unknowns without a limit on the choice of values for the unknowns.

1.2 Definition. -- An indeterminate system of equations is a system of equations in which the unknowns outnumber the equations.

1.3 Definition. -- A diophantine equation is an indeterminate, algebraic equation in which only integral solutions are considered.

1.4 Definition. -- A diophantine system of equations is an indeterminate system of algebraic equations in which only integral solutions are considered.

1.5 Definition. -- Solution will mean integral solution.

1.6 Definition. -- If $a, b, c, \ldots, n$ are integers, then $(a, b, c, \ldots, n)$ will mean the greatest common divisor of the integers $a, b, c, \ldots, n$. 
1.7 Theorem. -- A necessary and sufficient condition that \(x\) and \(y\) exist such that

\[ ax + by = c \]

is that \(c\) be divisible by \((a, b)\).

Proof: Case I. Assume that \(b = 0\), then \((a, b) = a\) and if \(a \mid c\) there is a solution

\[ x = c/a, \, y = 1. \]

Conversely, if there is a solution \(x_0, y_0\) then

\[ ax_0 + 0 \cdot y_0 = ax_0 = c \]

so that \(a \mid c\) and \(x_0 = c/a\).

Case II. Assume that \(a = 0\) and the theorem follows similarly to Case I.

Case III. Assume that \(a \neq 0\) and \(b \neq 0\). If \(|a| = |b|\), then \((a, b) = a\). If \((a, b)\) divides \(c\), then \(x = c/a, \, y = 0\) is a solution. Conversely, if \(ax + by = c\), then \(a(x + by/a) = c\) and \(a\) divides \(c\). If \(|a| \neq |b|\), then without loss of generality it can be assumed that \(|a| > |b|\). By Euclid's Algorithm (1, p52)

\[ |a| = |b| q_1 + b_1, \]
\[ |b| = b_1 q_2 + b_2, \]
\[ b_1 = b_2 q_3 + b_3, \]
\[ \ldots \]
\[ b_{n-2} = b_{n-1} q_n + b_n \]

where \(b_n\) is the greatest common divisor of \(a\) and \(b\), that is,

\[ b_n = (a, b). \]

The above equations can be arranged in the form
\[ b_1 = |a| - |b|q_1, \]
\[ b_2 = |b| - b_1 q_2, \]
\[ b_3 = b_1 - b_2 q_3, \]
\[ \ldots \ldots \ldots \ldots \]
\[ b_n = b_{n-2} - b_{n-1} q_n. \]

Let \( X_1 = 1 \) and \( Y_1 = q_1 \) so that the first equation becomes
\[ b_1 = |a|X_1 - |b|Y_1. \]

The second equation becomes
\[ b_2 = |b| - (|a|X_1 - |b|Y_1)q_2, \]
so that
\[ b_2 = - |a|X_1 q_2 - |b|X_2 q_2. \]

Let \( X_2 = X_1 q_2 \) and \( Y_2 = 1 + Y_1 q_2 \), then
\[ b_2 = - (|a|X_2 - |b|Y_2), \]
and
\[ b_3 = (|a|X_1 - |b|Y_1) + (|a|X_2 - |b|Y_2)q_3, \]
\[ b_3 = |a|(X_1 + X_2 q_3) - |b|(Y_1 + Y_2 q_3). \]

Let \( X_3 = X_1 + X_2 q_3 \) and \( Y_3 = Y_1 + Y_2 q_3 \) so that
\[ b_3 = |a|X_3 - |b|Y_3. \]

Continuing this process leads to the general equations
\[ b_{k-1} = (-1)^{k-2} (|a|X_{k-1} - |b|Y_{k-1}), \]
\[ b_k = (-1)^{k-1} (|a|X_k - |b|Y_k), \]
and
\[ b_{k+1} = (-1)^k (|a|X_{k+1} - |b|Y_{k+1}), \]
where
\[ X_{k+1} = X_{k-1} + X_k q_{k+1}, \]
and
\[ Y_{k+1} = Y_{k-1} + Y_k q_{k+1} \quad (k = 2, 3, 4, \ldots, n-1) \]

Let \( X_0 = 0 \) and \( Y_0 = 1 \) so that the derived expressions will hold for \( k = 1, 2, 3, \ldots, n-1 \). Use of the new notation in the expression for \( b_n \) gives

\[ b_n = (-1)^{n-1}(|a|X_n - |b|Y_n) \]

and

\[ b_n = |a|(-1)^{n-1}X_o + |b|(-1)^n Y_n. \]

Now by the hypothesis \( c \) is divisible by \( b_n \), and there exists an integer \( m \) so that

\[ c = mb_n = |a|(-1)^{n-1}mX_n + |b|(-1)^nmY_n. \]

Hence, the equation \( |a|x + |b|y = c \) has a solution,

\[ x = (-1)^{n-1}mX_n, \]

\[ y = (-1)^n mY_n. \]

Now \( ax/|a| \) and \( by/|b| \) is a solution of \( ax + by = c \).

Conversely, if the equation \( ax + by = c \) has a solution, and if \( a = b_n r \) and \( b = b_n s \) for some integers \( r \) and \( s \), then

\[ ax + by = b_n (rx + sy) = c. \]

Hence \( c \) is divisible by \( b_n \).

1.8 Theorem. -- If \( x_0 \) and \( y_0 \) exist such that \( ax_0 + by_0 = c \), then there is an infinite number of solutions of the form \( x = x_0 + bt/b_n \) and \( y = y_0 - at/b_n \), where \( t \) is an arbitrary integer.

Proof: Since \( x_0 \) and \( y_0 \) exist, by theorem 1.7 \( c \) is divisible by \( b_n \). If for an arbitrary integer \( t \) the expression \( abt/b_n \) is added and subtracted from the equation, it becomes

\[ ax_0 + y_0 b + abt/b_n - abt/b_n = c. \]
\[ a(x_o + bt/b_n) + b(y_o - at/b_n) = c. \]

Hence the equation is satisfied for any integral value of \( t \), and there is an infinite number of solutions \( x = x_o + bt/b_n \) and \( y = y_o - at/b_n \).

1.9 Theorem. -- If \( x_o \) and \( y_o \) exist such that \( ax_o + by_o = c \) when \( c \) is zero and \( b_n = (a, b) \), then there exists a \( t_o \) such that \( x_o = bt_o/b_n \) and \( y_o = -at_o/b_n \).

Proof: \[ ax_o + by_o = 0 \]
\[ ax_o = -by_o \]
\[ ax_o/b_n = -by_o/b_n \]

Since \((a/b_n, b/b_n) = 1, a/b_n \mid y_o\) so that \( \frac{y_o}{a/b_n} \) is an integer and
\[ x_o = \left( -\frac{b}{b_n} \right) \frac{-y_o}{a/b_n} . \]

Let \( t_o = -y_o \), then \( x_o = bt_o/b_n \). By substitution, the equation becomes
\[ a(bt_o/b_n) = -by_o, \]
and
\[ y_o = -at_o/b_n. \]

1.10 Theorem. -- If \( x_o \) and \( y_o \) is a solution and \( u_o \) and \( v_o \) is a solution both of which satisfy \( ax + by = c \), then there exists an integer \( t_o \) such that
\[ u_o = x_o + bt_o/b_n, \]
and
\[ v_o = y_o - at_o/b_n. \]

Proof: By the hypothesis, \( ax_o + by_o = c \) and \( au_o + bv_o = c \) so that
\[ ax_0 + by_0 = au_0 + bv_0, \]

and

\[ a(u_o - x_0) + b(v_o - y_0) = 0. \]

Now by theorem 1.9 there exists a \( t_o \) such that

\[ u_0 - x_0 = bt_o/b_n, \]

and

\[ v_0 - y_0 = -at_o/b_n. \]

Hence

\[ u_0 = x_0 + bt_o/b_n, \]

and

\[ v_0 = y_0 - at_o/b_n. \]

1.11 Theorem. -- If \( x_o \) and \( y_o \) is a solution of \( ax + by = c, \)
\( b_n = (a,b), \) and \( t \) is an integer then \( x = x_o + bt/b_n \) and
\( y = y_o - at/b_n \) is a solution of \( ax + by = c. \)

Proof: \[ a(x_o + bt/b_n) + b(y_o - at/b_n) = \]
\[ ax_o + by_o + abt/b_n - abt/b_n = c. \]

1.12 Theorem. -- A necessary and sufficient condition
that \( x, y, \) and \( z \) exist such that
\[ ax + by + cz = k \]
is that \( (a,b,c)|k. \)

Proof: Case I. For \( c = 0, a \neq 0, \) and \( b \neq 0, ax + by + 0 \cdot z = k \)
becomes
\[ ax + by = k. \]

By theorem 1.7 a solution exists if and only if \( (a,b)|k. \)

Now since \( (a,b,0) = (a,b), \) a necessary and sufficient condition
for a solution to exist is that \((a, b, 0) \mid k\).

Case II. For \(a = 0\) and \(b \neq 0\) and \(c \neq 0\), or for \(b = 0\) and \(a \neq 0\) and \(c \neq 0\), the theorem follows by the same reasoning as Case I.

Case III. For any two of the coefficients equal to zero the theorem follows from theorem 1.7 (Case I).

Case IV. For \(a \neq 0\), \(b \neq 0\), \(c \neq 0\), and \(k \neq 0\), certainly \((a, b, c) \mid 0\). Now if \((a, b) \mid c\) then \((a, b) \mid -cs\) for any \(s\). By theorem 1.7, the equation

\[ ax + by = -cs \]

has integers \(x_0\) and \(y_0\) for any \(s_0\) such that

\[ ax_0 + by_0 = -cs_0. \]

On the other hand if \((a, b) \nmid c\), then \(s_0\) can be chosen a multiple of \((a, b)\); where again by theorem 1.7 \(x_0\) and \(y_0\) exist such that

\[ ax_0 + by_0 = -cs_0. \]

Case V. For \(a \neq 0\), \(b \neq 0\), \(c \neq 0\), and \(k \neq 0\), let \(a = m(a, b)\) and \(b = n(a, b)\) so that the equation becomes

\[ (a, b)(mx + ny) + cs = k. \]

Since \((m, n) = 1\), then by theorem 1.7 the equation

\[ mx + ny = v \]

has a solution for any integer \(v\). Hence if it is possible to find a \(v\) and a \(s\) so that

\[ (a, b)v + cs = k, \]

then there is an \(x, y, \) and \(s\) such that

\[ (a, b)(mx + ny) + cs = k. \]
Conversely, if there is an \( x, y, \) and \( z \) so that
\[
(a, b)(mx + ny) + cs = k,
\]
then there is a \( v \) so that
\[
(a, b)v + cs = k.
\]

By theorem 1.7 a necessary and sufficient condition for the last equation to have a solution is that \( (a, b, c) \mid k. \) Now \( (a, b, c) = (a, b, c); \) hence \( (a, b, c) \) must divide \( k. \)

1.13 Theorem. -- If \( ax + by + cs = k \) has a solution, then there exists a solution \( x_0, y_0, \) and \( z_0, \) and two integers \( h_0 \) and \( n_0 \) satisfying the equation \( bh_0 + cn_0 = (b, c) \) such that if \( r \) is an integer and \( s \) is an integer, then
\[
x = x_0 + (b, c)r/(a, b, c),
\]
\[
(1) \quad y = y_0 - ah_0r/(a, b, c) - cs/(b, c)
\]
and
\[
s = z_0 - an_0r/(a, b, c) + bs/(b, c)
\]
is a solution of \( ax + by + cs = k. \)

Proof: In order to prove the theorem, two linear substitutions of the form \( y = hv + js \) and \( s = nw + ms \) will be determined so that \( ax + by + cs \) becomes \( ax + (b, c)v. \) This can be accomplished if \( j = -c/(b, c), \) \( m = b/(b, c) \) and \( bh + cn = (b, c). \) The last equation has a solution \( h_0 \) and \( n_0 \) by theorem 1.7. Now if \( y = h_0v - cs/(b, c) \) and \( s = n_0v + bs/(b, c), \) then
\[
ax + by + cs = ax + (b, c)v.
\]
Since \( ax + by + cs = k \) has a solution, \( (a, b, c) \mid k, \) and \( (a, (b, c)) \mid k. \) Hence there is an \( x_0 \) and a \( v_0 \) so that \( ax_0 + (b, c)v_0 = k. \) To define \( y_0 \) and \( z_0, \) let \( s = 0 \) so that \( y_0 = h_0v_0 \) and \( z_0 = n_0v_0. \) By theorem 1.8,
\[
x = x_0 + (b, c)r/(a, b, c) \text{ and } v = v_0 = ar/(a, b, c) \text{ is a solution}.
\]
of \( ax + (b, c)w = k \) for each integer \( r \). Hence

\[ x = x_0 + (b, c)r/(a, b, c), \]
\[ y = y_0 + js \]
\[ = h_0 w_0 - ah_0 r/(a, b, c) - cs/(b, c) \]
\[ = y_0 - ah_0 r/(a, b, c) - cs/(b, c) \]

and

\[ z = n_0 w + ms \]
\[ = n_0 w_0 - an_0 r/(a, b, c) + bs/(b, c) \]
\[ = z_0 - an_0 r/(a, b, c) + bs/(b, c) \]

is a solution for each integer \( s \).

1.14 \textbf{Corollary.} -- If \( ax + by + cs = k \) has a solution, then there exist solutions \( x_0^*, y_0^*, z_0^* \) and \( x_0^{**}, y_0^{**}, z_0^{**} \) and integers \( h_0^*, n_0^* \) and \( h_0^{**}, n_0^{**} \) satisfying the equations

\[ ah_0^* + cn_0^* = (a, c), \]
\[ ah_0^{**} + bn_0^{**} = (a, b) \]

such that if \( r^*, r^{**}, s^* \) and \( s^{**} \) are integers, then

\[ x = x_0^* + bh_0^* r/(a, b, c) - cs/(a, c), \]
\[ y = y_0^* - (a, c)r/(a, b, c), \]
\[ z = z_0^* + bn_0^* r/(a, b, c) + as/(a, c) \]

and

\[ x = x_0^{**} + ch_0^{**} r/(a, b, c) - bs/(a, b), \]
\[ y = y_0^{**} + cn_0^{**} r/(a, b, c) + as/(a, b), \]
\[ z = z_0^{**} - (a, b)r/(a, b, c) \]

are solutions of \( ax + by + cs = k \).

\textbf{Proof:} The proofs follow similarly to the proof of theorem 1.13.
1.15 Theorem. --- If \( x_0, y_0 \) and \( z_0 \) is a solution of
\[ ax + by + cz = k, \]
and \( bh_0 + cn_0 = (b, c) \), then
\[ x = x_0 + (b, c)r/(a, b, c), \]
\[ y = y_0 - ah_0r/(a, b, c) - cs/(b, c), \]
\[ z = z_0 - an_0r/(a, b, c) + bs/(b, c) \]
is a solution of \( ax + by + cz = k \).

Proof: By substitution, \( ax + by + cz = \)
\[ ax_0 + by_0 + cz_0 = a(b, c)r/(a, b, c) - abh_0r/(a, b, c) - acn_0r/(a, b, c), \]
then
\[ ax + by + cz = k + a(b, c)r/(a, b, c) - (bh_0 + cn_0)ar/(a, b, c), \]
and
\[ 0 = a(b, c)r/(a, b, c) - a(b, c)r/(a, b, c). \]

1.16 Corollary. --- If \( x_0, y_0 \) and \( z_0 \) is a solution of
\[ ax + by + cz = k, \]
and \( ah_0' + cn_0' = (a, c) \) and \( ah_0'' + bn_0''' = (a, b) \),
then
\[ x = x_0 + bh_0'r/(a, b, c) - cs/(a, c), \]
\[ y = y_0 - (a, c)r/(a, b, c), \]
\[ z = z_0 + bn_0'r/(a, b, c) + as/(a, c) \]
and
\[ x = x_0 + ch_0''r/(a, b, c) - bs/(a, b), \]
\[ y = y_0 + cn_0''r/(a, b, c) + as/(a, b), \]
\[ z = z_0 - (a, b)r/(a, b, c) \]
are solutions of \( ax + by + cz = k \).

Proof: The proof that the equations of (2a) and (3a)
determine solutions follows similarly to the proof of
theorem 1.15.
1.17 Remark. -- If \( a, b, c \) are relatively prime, the forms (1a), (2a), and (3a) are simplified as follows:
\[
x = x_0 + (b,c) r
\]
(1b) \[
y = y_0 - ah_0 r - cs/(b,c)
z = z_0 - an_0 r + bs/(b,c)
\]
(2b) \[
x = x_0 + bh_0 r - cs/(a,c)
y = y_0 - (a,c) r
z = z_0 + bn_0 r + as/(a,c)
\]
(3b) \[
x = x_0 + ch_0 r - bs/(a,b)
y = y_0 + cn_0 r + as/(a,b)
z = z_0 - (a,b) r.
\]

1.18 Lemma. -- If the integers \( a, b, \) and \( c \) are relatively prime, but not in pairs, then the greatest common divisor of one of the pairs will not divide the third integer.

Proof: If \( a, b, \) and \( c \) are not relatively prime in pairs, then at least one pair must have a greatest common divisor not equal to unity. Let \( (b,c) \neq 1 \) and assume that \( (b,c) \) divides \( a \). Then there is an integer \( m \) such that
\[
a = (b,c) m.
\]
Consequently
\[
(a,b,c) = ((b,c)m,b,c)
= ((b,c)m,(b,c))
= (b,c) \neq 1,
\]
and there is a contradiction. Hence \( a \) is not divisible by \( (b,c) \).
1.19 Theorem. -- If $x_0$, $y_0$, $z_0$ is a solution to the equation

$$ax + by + cz = 0,$$

then there exists integers $r_o$ and $s_o$ such that

$$x_0 = (b, c)r_o$$

(1c)  \[ y_0 = -ah_0r_o - cs_0/(b, c) \]

$$z_0 = -an_0r_o + bs_0/(b, c)$$

where $bh_o + cn_o = (b, c)$, and there exists integers $r_o'$ and $s_o'$ such that

$$x_0 = bh_o'r_o' - cs_0'/(a, c)$$

(2c)  \[ y_0 = -(a, c)r_o' \]

$$s_0 = bn_o'r_o' + as_0'/(a, c)$$

where $ah_o' + cn_o' = (a, c)$, and there exists integers $r_o''$ and $s_o''$ such that

$$x_0 = ch_o''r_o'' - bs_0''/(a, b)$$

(3c)  \[ y_0 = cn_o''r_o'' + as_0''/(a, b) \]

$$z_0 = -(a, b)r_o''$$

where $ah_o'' + cn_o'' = (a, b)$.

Proof: It can be assumed without loss of generality that $a$, $b$ and $c$ are relatively prime, for if they are not, an equivalent equation with relatively prime coefficients can be obtained by dividing through by $(a, b, c)$. Furthermore, one particular solution to the equation is $x_0 = 0$, $y_0 = 0$, $z_0 = 0$, which, if substituted in (1b), (2b), (3b) gives the same forms as (1c), (2c), (3c). Therefore it is
necessary only to exhibit integers \( r_0 \) and \( s_0 \) such that (1c), (2c), and (3c) are true.

Case I. Let \( a, b, c \) be relatively prime in pairs, then \( r_0 = x_0 \) and \( s_0 = h_0 z_0 - n_0 y_0 \) are integers such that (1c) is true. Proof of the last statement is as follows: with \( (b, c) = 1 \), (1c) becomes

(i) \( x_0 = r_0 \)
(ii) \( y_0 = -ah_0 r_0 - cs_0 \)
(iii) \( z_0 = -an_0 r_0 + bs_0 \),

where \( bh_0 + cn_0 = 1 \). The equation (i) is satisfied.

Now by substituting \( r_0 \) and \( s_0 \) in (ii), it follows that

\[-ah_0 x_0 - c(h_0 s_0 - n_0 y_0) = -h_0 (ax_0 + cs_0) + cn_0 y_0 =

-ah_0 x_0 - ch_0 s_0 - bh_0 y_0 + bh_0 y_0 + cn_0 y_0 = y_0 \cdot\]

Substitution in equation (iii) gives

\[-an_0 r_0 + bs_0 =

-an_0 x_0 + b(h_0 s_0 - n_0 y_0) =

-an_0 x_0 - bn_0 y_0 - cn_0 z_0 + cn_0 z_0 + bh_0 s_0 = z_0 \cdot\]

Thus for Case I integers \( r_0 \) and \( s_0 \) exist such that (1c) is true. Also (2c) and (3c) follow similarly for \( r_0' = -y_0', s_0' = h_0' z_0 - n_0' x_0 \) and \( r_0'' = -s_0, s_0'' = h_0'' y_0 - n_0'' x_0 \) respectively.

Case II. Let \( a, b, c \) be relatively prime, but not in pairs so that \( (b, c) \neq 1 \), \( (a, c) \neq 1 \), \( (a, b) \neq 1 \). By lemma 1.18 \( (b, c) \) does not divide \( a \), and furthermore no factor of \( a \) is a
factor of $(b,c)$ because $(a,b,c) = 1$. Therefore, $x_0$ must be a multiple of $(b,c)$ if $y_0$ and $z_0$ are to exist so that

$$by_0 + cs_0 = -ax_0.$$ 

Let $q$ be an integer such that $x_0 = q(b,c)$. Let $r_0 = q$ and the first equation is satisfied. Now an integer $s_0$ can be found such that the second and third equations are satisfied, that is,

$$y_0 = -ah_0q - cs_0/(b,c)$$
$$z_0 = -ah_0q + bs_0/(b,c).$$

By eliminating the term involving $q$, the system becomes

$$h_0s_0 - n_0y_0 = (b_0b + n_0c)s_0/(b,c).$$

Since $b_0b + n_0c = (b,c)$, $s_0 = h_0s_0 - n_0y_0$. This value for $s_0$ along with $r_0 = q$ are integers which satisfy the equations of (1c).

A similar procedure will produce an $r_0$ and $s_0$ such that (2c) and (3c) are satisfied respectively.

Case III. If at least one pair of coefficients is relatively prime and one pair is not relatively prime, then a combination of case I and case II can be used. To prove (1c) for $(b,c) = 1$ use case I. For $(b,c) \neq 1$ use case II. To prove (2c) for $(a,c) = 1$ use case I. For $(a,c) \neq 1$ use case II. To prove (3c) for $(a,b) = 1$ use case I. For $(a,b) \neq 1$ use case II.

Furthermore, any one of these three representations can be used for a solution $x$, $y$, and $z$. 
1.20 Theorem. -- If $x_0$, $y_0$, $z_0$ and $u_0$, $v_0$, $w_0$ are solutions to
\[ ax + by + cz = k, \]
then there exist integers $r_o$ and $s_o$ such that
\[
\begin{align*}
  u_o &= x_o + (b,c)r_o \\
  v_o &= y_o - ah_o r_o - cs_o/(b,c) \\
  w_o &= z_o - an_o r_o + bs_o/(b,c),
\end{align*}
\]
where $bh_o + cn_o = (b,c)$.

Proof: By the hypothesis
\[
\begin{align*}
  ax_o + by_o + cz_o &= k \\
  au_o + bv_o + cw_o &= k
\end{align*}
\]
and
\[
a(u_o - x_o) + b(v_o - y_o) + c(w_o - z_o) = 0.
\]
From theorem 1.19 there exist integers $r_o$ and $s_o$ such that,
\[
\begin{align*}
  u_o - x_o &= (b,c)r_o \\
  v_o - y_o &= -ah_o r_o - cs_o/(b,c) \\
  w_o - z_o &= -an_o r_o + bs_o/(b,c)
\end{align*}
\]
where $bh_o + cn_o = (b,c)$. Thus
\[
\begin{align*}
  u_o &= x_o + (b,c)r_o \\
  v_o &= y_o - ah_o r_o - cs_o/(b,c) \\
  w_o &= z_o - an_o r_o + bs_o/(b,c).
\end{align*}
\]

1.21 Remark. -- The results of theorem 1.19 and theorem 1.20 are as follows: if $(a,b,c) = 1$ then (1b) of remark 1.17 represents all the solutions to the equation
\[ ax + by + cz = k. \]
If \((a, b, c) \neq 1\), then form (1b) for the equivalent equation
\[
ax/(a, b, c) + by/(a, b, c) + cz/(a, b, c) = k/(a, b, c)
\]
represents all the solutions.

1.22 Theorem. -- The diophantine equation
\[
a_1x_1 + a_2x_2 + \cdots + a_nx_n = c
\]
has a solution if and only if \((a_1, a_2, \ldots, a_n) \mid c\).

Case I. For \(n = 1\), there is an unique solution. If
\(a_1 \mid c\), then \(x_1 = c/a_1\) is a solution. Conversely, if a solu-
tion exists then \(c\) is a multiple of \(a_1\), and therefore \(a_1 \mid c\).

Case II. For \(n = 2\), \(x_1\) and \(x_2\) exist by theorem 1.17, if
and only if \((a_1, a_2) \mid c\).

Case III. If \(a_1x_1 + a_2x_2 + \cdots + a_nx_n = c\) has a solution,
then let \(d_n = (a_1, a_2, \ldots, a_n)\). Now there exist integers \(m_1, m_2, \ldots, m_n\) so that \(a_p = d_n m_p\) for \(p = 1, 2, 3, \ldots, n\). Now
\[
a_1x_1 + a_2x_2 + \cdots + a_nx_n = d_n(m_1x_1 + m_2x_2 + \cdots + m_nx_n) = c.
\]
Hence \(d_n\) divides \(c\).

If \(d_n = (a_1, a_2, \ldots, a_n)\) and \(d_n\) divides \(c\), then
\(a_1x_1 + a_2x_2 + \cdots + a_nx_n = c\) has been proven to have a solution
for \(n = 1, 2, 3\). If the condition \(d_k = (a_1, a_2, \ldots, a_k)\) divides
\(b\) implies that there is a solution of
\(a_1x_1 + a_2x_2 + \cdots + a_kx_k = b\), then it will be shown that if
\(d_{k+1}\) divides \(c\), \(a_1x_1 + a_2x_2 + \cdots + a_{k+1}x_{k+1} = c\). Now
\((d_k, a_{k+1}) = d_{k+1}\) which divides \(c\). Hence there is an \(x\) and an
\(x_{k+1}\) so that \(d_kx + a_{k+1}x_{k+1} = c\). Now
\(a_1x_1 + a_2x_2 + \cdots + a_kx_k = d_kx\) has a solution since
\((a_1, a_2, \ldots, a_k) = d_k \text{ divides } d_k x\). Hence

\[ a_1 x_1 + a_2 x_2 + \ldots + a_k x_k + a_{k+1} x_{k+1} = d_k x + a_{k+1} x_{k+1} = c. \]
CHAPTER BIBLIOGRAPHY

CHAPTER II

DIOPHANTINE SYSTEMS OF THE FIRST DEGREE

A system of equations can not have a solution if one of the equations does not have a solution. Hence it will be of interest to examine only systems in which there is a solution for each equation. Throughout this chapter it will be assumed that each equation in a system has a solution.

2.1 Theorem. -- A necessary condition that \( x_0, y_0, z_0 \) exist such that

\[
\begin{align*}
a_1 x_0 + a_2 y_0 + a_3 z_0 &= a \\
b_1 x_0 + b_2 y_0 + b_3 z_0 &= b
\end{align*}
\]

is that

(1) \[
\begin{pmatrix}
a_1 & a_2 \\ b_1 & b_2 \\
a_3 & a_1 \\ b_3 & b_1
\end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}
\]

and

(2) \[
\begin{pmatrix}
a_2 & a_3 \\ b_2 & b_3 \\
a_1 & a_2 \\ b_1 & b_2
\end{pmatrix} = \begin{pmatrix} a_2 \\ a_3 \\ a_1 \\ b_2 \\ b_3 \\ b_1 \end{pmatrix}
\]

and

(3) \[
\begin{pmatrix}
a_3 & a_1 \\ b_3 & b_1 \\
a_2 & a_3 \\ b_2 & b_3
\end{pmatrix} = \begin{pmatrix} a_3 \\ a_1 \\ a_2 \\ b_3 \\ b_1 \end{pmatrix}
\]

Proof: Assume \( x_0, y_0, z_0 \) is a solution, then by eliminating \( x_0 \) from the system, the equations reduce to

\[
(a_1 b_2 - a_2 b_1) y_0 + (a_1 b_3 - a_3 b_1) z_0 = a_1 b - a b_1.
\]
In determinant form the equation becomes

\[
\begin{vmatrix}
a_1 & a_2 \\
b_1 & b_2
\end{vmatrix} y_0 + \begin{vmatrix}
a_1 & a_3 \\
b_1 & b_3
\end{vmatrix} s_0 = \begin{vmatrix}
a_1 & a \\
b_1 & b
\end{vmatrix}.
\]

Conditions (2) and (3) follow similarly by eliminating \( y_0 \) and \( s_0 \) respectively.

2.2 Theorem. -- A sufficient condition for the system

\[
a_1 x + 0 \cdot y + 0 \cdot z = a \\
b_1 x + b_2 y + b_3 z = b
\]
to have a solution is that \((b_2, b_3) \parallel b - b_1 (a/a_1)\).

Proof: If \((b_2, b_3) \parallel b - b_1 (a/a_1)\) then by theorem 1.7 there exist a \( y_0 \) and a \( s_0 \) such that

\[
b_2 y_0 + b_3 s_0 = b - b_1 (a/a_1).
\]

If \( x_0 \) is chosen to be \((a/a_1)\), then \( x_0, y_0, s_0 \) is a solution of the equation

\[
b_1 x + b_2 y + b_3 z = b.
\]
The first equation is likewise satisfied by this solution, since

\[
a_1 (a/a_1) + 0 \cdot y_0 + 0 \cdot s_0 = a.
\]

2.3 Theorem. -- A sufficient condition for the system

\[
a_1 x + a_2 y + 0 \cdot z = a \\
b_1 x + b_2 y + b_3 z = b
\]
to have a solution is that

\[
\begin{vmatrix}
a_2 & a_1 \\
b_2 & b_1
\end{vmatrix} \\
\begin{vmatrix}
(a_1, a_2) \\
b_3
\end{vmatrix}
\]

\[\parallel b - b_1 x_0 - b_2 y_0.\]
where

\[ a_1 x_0 + a_2 y_0 = a. \]

**Proof:** Since it has been assumed that each equation has a solution, there exist a \( x_0 \) and a \( y_0 \) such that

\[ a_1 x_0 + a_2 y_0 = a. \]

Then if

\[
\begin{pmatrix}
  a_2 & a_1 \\
  b_2 & b_1 \\
  (a_1, a_2)
\end{pmatrix}
\begin{pmatrix}
  t_0 \\
  s_0
\end{pmatrix} = \begin{pmatrix} b - b_1 x_0 - b_2 y_0 \end{pmatrix},
\]

by theorem 1.7 there exist a \( t_0 \) and a \( s_0 \) such that

\[
\begin{pmatrix}
  a_2 & a_1 \\
  b_2 & b_1 \\
  (a_1, a_2)
\end{pmatrix}
\begin{pmatrix}
  t_0 \\
  s_0
\end{pmatrix} = \begin{pmatrix} b - b_1 x_0 - b_2 y_0 \end{pmatrix}.
\]

By changing the form, the equation becomes

\[
\frac{a_2 b_1}{(a_1, a_2)} t_0 - \frac{a_1 b_2}{(a_1, a_2)} t_0 + b_3 s_0 = b - b_1 x_0 - b_2 y_0,
\]

and

\[
b_1 \left[ x_0 + a_2 t_0 / (a_1, a_2) \right] + b_2 \left[ y_0 - a_1 t_0 / (a_1, a_2) \right] + b_3 s_0 = b.
\]

Hence \( x = x_0 + a_2 t_0 / (a_1, a_2) \), \( y = y_0 - a_1 t_0 / (a_1, a_2) \), \( s = s_0 \) satisfies the second equation. Then by theorem 1.8 this solution satisfies the first equation.

2.4 **Theorem.** A sufficient condition for the system

(i) \[ a_1 x + a_2 y + a_3 z = a \]

(ii) \[ b_1 x + b_2 y + b_3 z = b \]

to have a solution is that
are integers, and

$$\begin{vmatrix} (a_2, a_3) & a_3 \\ (b_2, b_3) & b_3 \end{vmatrix}$$

and

$$\begin{vmatrix} a_2 & (a_2, a_3) \\ b_2 & (b_2, b_3) \end{vmatrix}$$

are integers, and

$$\begin{pmatrix} (a_2, a_3) & a_1 \\ (b_2, b_3) & b_1 \end{pmatrix} \frac{1}{(a_2, a_3) a_3 - b_2 b_3} \begin{pmatrix} a_2 & b_2 \\ a_3 & b_3 \end{pmatrix} = b - b_1 x_0 - b_2 y_0 - b_3 z_0$$

where $x_0, y_0, z_0$ is any solution to (i).

Proof: By the hypothesis $x_0, y_0, z_0$ is a solution to

(1) so

$$x = x_0 + (a_2, a_3)r$$

$$y = y_0 - a_1 h_0 r - a_3 s/(a_2, a_3)$$

$$s = z_0 - a_1 n_0 r + a_2 s/(a_2, a_3),$$

where $a_2 h_0 + a_3 n_0 = (a_2, a_3)$, represent all the solutions to

(i). On substitution, (ii) reduces to the equation

$$[b_1 (a_2, a_3) - a_1 (b_1 h_0 + b_3 n_0)] r + (a_2 b_3 - a_3 b_2) s/(a_2, a_3) =$$

$$b - b_1 x_0 - b_2 y_0 - b_3 z_0.$$
\[
\begin{pmatrix}
(a_2, a_3) & a_1 \\
(b_2, b_3) & b_1
\end{pmatrix}
\begin{pmatrix}
1 \\
(a_2, a_3)
\end{pmatrix}
\begin{pmatrix}
a_2 & b_2 \\
a_3 & b_3
\end{pmatrix}
s = b - b_1x_0 - b_2y_0 - b_3z_0,
\]

which has an integral solution \( r_0 \) and \( s_0 \) by condition (2) and theorem 1.7.

Hence if (1) and (2) hold there exist integers \( r_0 \) and \( s_0 \) such that

\[
x' = x_0 + (a_2, a_3) r_0 \\
y' = y_0 - a_1 h_0 r_0 - a_3 s_0/(a_2, a_3) \\
z' = z_0 - a_1 m_0 r_0 - a_2 s_0/(a_2, a_3)
\]
satisfy (1) and (ii) (1, p. 64).

2.5 Theorem. -- If the system

\[
a_1x_1 + a_2x_2 + \cdots + a_n x_n = a \\
b_1x_1 + b_2x_2 + \cdots + b_n x_n = b
\]

has a solution, then

(1) \[
\begin{pmatrix}
a_1 & a_2 \\
b_1 & b_2
\end{pmatrix}
\begin{pmatrix}
a_1 & a_3 \\
b_1 & b_3
\end{pmatrix}
\begin{pmatrix}
a_1 & a_4 \\
b_1 & b_4
\end{pmatrix}
\cdots
\begin{pmatrix}
a_1 & a_n \\
b_1 & b_n
\end{pmatrix}
\begin{pmatrix}
a_1 \\
b_1
\end{pmatrix}
\begin{pmatrix}
a \\
b
\end{pmatrix}
\]

(2) \[
\begin{pmatrix}
a_2 & a_1 \\
b_2 & b_1
\end{pmatrix}
\begin{pmatrix}
a_2 & a_3 \\
b_2 & b_3
\end{pmatrix}
\begin{pmatrix}
a_2 & a_4 \\
b_2 & b_4
\end{pmatrix}
\cdots
\begin{pmatrix}
a_2 & a_n \\
b_2 & b_n
\end{pmatrix}
\begin{pmatrix}
a_2 \\
b_2
\end{pmatrix}
\begin{pmatrix}
a \\
b
\end{pmatrix}
\]

\vdots

\begin{pmatrix}
a_n & a_1 \\
b_n & b_1
\end{pmatrix}
\begin{pmatrix}
a_n & a_2 \\
b_n & b_2
\end{pmatrix}
\begin{pmatrix}
a_n & a_3 \\
b_n & b_3
\end{pmatrix}
\cdots
\begin{pmatrix}
a_n & a_{n-1} \\
b_n & b_{n-1}
\end{pmatrix}
\begin{pmatrix}
a_n \\
b_n
\end{pmatrix}
\begin{pmatrix}
a \\
b
\end{pmatrix}
\]

Proof: Assume that a solution exists, then by eliminating \( x_1 \) the system becomes

\[
(a_1b_2 - a_2b_1)x_2 + (a_1b_3 - a_3b_1)x_3 + \cdots + (a_1b_n - a_nb_1)x_n
\]

\[
= (a_1b - ab_1)
\]
and
\[
\begin{vmatrix}
  a_1 & a_2 \\
  b_1 & b_2
\end{vmatrix} x_2 + \begin{vmatrix}
  a_1 & a_3 \\
  b_1 & b_3
\end{vmatrix} x_3 + \ldots + \begin{vmatrix}
  a_1 & a_n \\
  b_1 & b_n
\end{vmatrix} x_n = \begin{vmatrix}
  a_1 & a \\
  b_1 & b
\end{vmatrix}.
\]

By theorem 1.22 condition (1) must hold for the last equation to have a solution. Conditions (2) through (n) follow similarly by eliminating \(x_2, \ldots, x_n\) respectively.

2.6 Remark. --- In order to obtain the conditions necessary for the solution of a system of \(n\) equations in \(n-1\) unknowns, the equations can be grouped in pairs; then applying theorem 2.5, conditions for the solution of each will be found. By eliminating one unknown from each pair, the number of new equations will be half that of the original number. Again, by applying theorem 2.5 to each pair of the new equations, more conditions will be found. Continuing this procedure will finally yield one equation in either one or two unknowns, depending on the evenness or oddness of \(r\). Application of theorem 1.7 to this final equation will give the last of the conditions necessary for the solution of the system.
CHAPTER BIBLIOGRAPHY

CHAPTER III

A QUADRATIC DIOPHANTINE EQUATION

Due to the large amount of preliminary definitions, theorems, lemmas, and theory needed for the study of each quadratic diophantine equation, this chapter will be devoted to the examination of only one such equation, the Pythagorean equation $x^2 + y^2 = z^2$.

3.1 Definition. -- If the integers $x, y, z$ satisfy the equation $x^2 + y^2 = z^2$, then $x, y, z$ will be called a triplet.

3.2 Definition. -- A primitive triplet is a triplet in which the integers are relatively prime.

3.3 Definition. -- An imprimitive triplet is a triplet in which the integers are not relatively prime.

3.4 Note. -- If $x^2 + y^2 = z^2$, then there exist an integer $d$ and a primitive triplet $x, y, z$ so that $x = dx$, $y = dy$, and $z = dz$. Conversely if $x, y, z$ is a primitive triplet and $d$ is an integer, then $(d^2 + d^2 = (dz)^2$ (1, p. 86).

3.5 Lemma. -- If two positive integers $r$ and $s$ are relatively prime, and their product is an exact square of an integer, then $r$ and $s$ are exact squares of some relatively prime integers (2, p. 33).

Proof: By the hypothesis

$rs = t^2$. 

26
Let \( a = (r, t) \). Now there are integers \( m \) and \( n \) so that \( r = ma \), \( t = na \) and \( (m, n) = 1 \). By substitution,
\[
ms = n^2 a^2,
\]
and
\[
ms = n^2 a.
\]
It follows that \( n^2 \mid s \) so that \( s = n^2 p \) for some integer \( p \). Substituting this expression for \( s \),
\[
mn^2 p = n^2 a,
\]
and
\[
mp = a.
\]
Now \( (r, s) = 1 \) and since \( a \mid r \) and \( p \mid s \), \( (a, b) = 1 \). Then from the last equation \( m \) must be divisible by \( a \). Thus \( m = ae \) for some integer \( e \), and
\[
aep = a
\]
so that
\[
ep = l.
\]
Then \( e \) and \( p \) must both be equal to one, and \( a \) must be equal to \( m \); from this it follows that \( r = m^2 \) and \( s = n^2 \), and since \((m^2, n^2) = 1\), it follows that \((m, n) = 1\).

3.6 Lemma. -- If \( x \) is an odd integer, then there exists an integer \( k \) such that \( x^2 = 1 + 8k \). \((2, p. 38)\).

Proof: Let \( x \) be an odd integer, then there exists an integer \( n \) such that \( x = 2n + 1 \). Then
\[
x^2 = 4n^2 + 4n + 1,
\]
and
\[ x^2 = 1 + 4n(n + 1), \]

where either \( n \) or \( n + 1 \) is an even number; therefore, 
\[ k = \frac{n(n + 1)}{2} \]
is an integer that satisfies the lemma.

3.7 Lemma. -- If \( x \) and \( y \) are odd integers, then \( x^2 + y^2 \)
is not divisible by four.

Proof: By lemma 3.3 there exists a \( k \) and a \( j \) such that 
\[ x^2 = 1 + 8k, \]
and
\[ y^2 = 1 + 8j. \]

Then
\[ x^2 + y^2 = 2 + 8(k + j), \]
\[ = 2(1 + 4m). \]
The expression \((1 + 4m)\) is odd for all integral values of \( m \);
therefore, \( x^2 + y^2 \) is divisible only by two and the odd num-
ber \((1 + 4m)\).

3.8 Lemma. -- If \( x, y, s \) is a primitive triplet, then \( x, y, s \)
are relatively prime in pairs.

Proof: Let \((x, y) = d, x = md \) and \( y = nd \); then 
\[ x^2 + y^2 = d^2(m^2 + n^2), \]
and
\[ s^2 = d^2(m^2 + n^2). \]
Therefore, \( s^2 \) is divisible by \( d^2 \), and as a result \( d \mid s \). Since 
\((x, y, s) = 1, d \) must be one, and \( x \) and \( y \) are relatively prime.
Similarly \( x, s \) and \( y, s \) are relatively prime, and \( x, y, s \) are
relatively prime in pairs.
3.9 Lemma. -- If \( y \) and \( z \) are relatively prime integers, and \( r \) and \( s \) are integers such that \( y = r - s \) and \( z = r + s \), then \( r \) and \( s \) are relatively prime.

Proof: Let \((r, s) = d\), \( r - s = dm \), and \( r + s = dn \). Now \((r - s, r + s) = (y, z) = 1\), so \((dm, dn) = 1\). Then \( d = 1 \) and \((m, n) = 1\). Therefore \( r \) and \( s \) are relatively prime.

3.10 Theorem. -- If \( x \), \( y \) and \( z \) is a triplet, then there exist integers \( k \), \( m \) and \( n \), where \((m, n) = 1\), so that

\[
x = 2kmn, \quad y = k(m^2 - n^2), \quad z = k(m^2 + n^2)
\]

Conversely if \( k \), \( m \) and \( n \) are integers, then

\[
x = 2kmn, \quad y = k(m^2 - n^2), \quad z = k(m^2 + n^2)
\]

is a triplet.

Proof: If \( x \), \( y \), \( z \) is a triplet, then by note 3.4 there exist integers \( k, x, y, z \) so that \( x, y, z \) is a primitive triplet and \( X = kx, \ Y = ky, \) and \( Z = kZ \). By lemma 3.8 \( x, y, z \) are relatively prime in pairs, so at most one of the integers may be even. Now one of the integers must be even, for the square of an odd integer is odd, and the sum and difference of two odd integers is even.

Suppose that \( z \) is the even integer and that \( x \) and \( y \) are odd. Now \( z^2 \) is divisible by four, but lemma 3.7 shows that \( x^2 + y^2 \) is not divisible by four. Hence there is a contradiction, and either \( x \) or \( y \) must be even. Let \( x \) be even. Then there exists an integer \( t \) such that \( x = 2t \). Now \( y \) and \( z \) are odd, so there exist integers \( r \) and \( s \) such that \( z + y = 2r \) and
\[ z - y = 2s. \] Thus
\[ x^2 = z^2 - y^2, \]
\[ x^2 = (z + y)(z - y), \]
\[ = 4rs. \]

Since \( x^2 = 4t^2, \) \( rs = t^2. \) Solving for \( z \) and \( y, \) \( z = r + s \) and \( y = r - s. \) By lemma 3.9 \( r \) and \( s \) are relatively prime, and by lemma 3.5 there exist integers \( m \) and \( n \) such that \( r = m^2 \) and \( s = n^2 \) where \( (m,n) = 1. \) Consequently \( x^2 = 4m^2n^2 \) and \( x = \pm 2mn, \)
\[ y = m^2 - n^2 \] and \( z = m^2 + n^2. \) Now the sum of \( r \) and \( s \) is equal to the odd number \( z, \) so either \( r \) or \( s \) must be even; then it follows that either \( m \) or \( n \) must be even.

Therefore,
\[ X = 2kmn, \quad Y = k(m^2 - n^2), \quad Z = k(m^2 + n^2) \]
is a solution. Conversely, if \( k, m \) and \( n \) are integers, a direct substitution of \( X = 2kmn, \) \( Y = k(m^2 - n^2) \) and \( Z = k(m^2 + n^2) \) will show that \( X^2 + Y^2 = Z^2. \)

3.11 Theorem. --- If the values of the triplet \( x, y, z \) are used for the length of the sides of a right triangle, then the radius of a circle inscribed in this triangle is an integer (I, p. 89).

Proof: Let \( r \) denote the radius of the inscribed circle. The triangle may be divided into three smaller triangles by connecting the center of the circle to each of the vertices of the triangle. Each of the small triangles has an altitude of length \( r \) and a base of length \( x, \) \( y \) or \( z. \)
By equating the sum of the areas of the small triangles to the area of the original triangle

\[ \frac{rx}{2} + \frac{ry}{2} + \frac{rz}{2} = \frac{xy}{2}, \]

and

\[ r(x + y + z) = xy. \]

Since \( x, y, z \) is a triplet, by theorem 3.10 there exist positive integers \( m, n \) and \( k \) such that

\[ x = 2kmn, \quad y = k(m^2 - n^2), \quad z = k(m^2 + n^2), \]

where \( (m, n) = 1 \). Substituting these values in the last equation, the following equation is obtained

\[ 2kr(m^2 + mn) = 2k^2mn(m^2 - n^2), \]

which reduces to

\[ r = km(m - n). \]

Therefore, \( r \) is an integer.
CHAPTER BIBLIOGRAPHY


BIBLIOGRAPHY

Books


