An Algebraic Treatment of Diophantine Analysis

Anthony Andrew Aucoin

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Part of the Physical Sciences and Mathematics Commons

Recommended Citation
https://repository.lsu.edu/gradschool_disstheses/8214

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
Unpublished theses submitted for the master's and doctor's degrees and deposited in the Louisiana State University Library are available for inspection. Use of any thesis is limited by the rights of the author. Bibliographical references may be noted, but passages may not be copied unless the author has given permission. Credit must be given in subsequent written or published work.

A library which borrows this thesis for use by its clientele is expected to make sure that the borrower is aware of the above restrictions.

LOUISIANA STATE UNIVERSITY LIBRARY
AN ALGEBRAIC TREATMENT OF DIOPHANTINE ANALYSIS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Anthony Andrew Aucoin
B. A., Rice Institute, 1934
M. A., Rice Institute, 1936
1940

LIBRARY
LOUISIANA STATE UNIVERSITY
Without the help and encouragement of Professor W. V. Parker this dissertation would not have been written.
I. INTRODUCTION, pp. 1-3.

II. QUADRATIC EQUATIONS, pp. 4-12.
   1. \[ \sum_{i} a_{i} x_{i} x_{i} = 0, \] p. 4.
   2. \[ \sum_{i} a_{i} x_{i}^{2} = \sum_{i} b_{i} y_{i}^{2}, \] pp. 5-8.
   3. \[ \sum_{i} (a_{i} x_{i} + b_{i} y_{i})(c_{i} x_{i} + d_{i} y_{i}) = 0, \] pp. 8-9.
   4. \[ (ay + bz)(cy + dz) = y \sum_{i} a_{i} x_{i} + z \sum_{i} b_{i} x_{i} + \sum_{i} c_{i} x_{i} x_{i}, \] pp. 9-12.

   2. \[ x^{2} + y^{2} + z^{2} - 3xyz = u^{2} + v^{2} + w^{2} - 3uvw, \] pp. 15-18.

IV. QUARTIC EQUATIONS, pp. 19-21.
   1. \[ \prod_{i} a_{i} x_{i} = g(x), \] pp. 19-21.

V. EQUATIONS OF DEGREE N, pp. 22-35.
   1. \[ f(x) = g(y) \text{ where the partials of } f \text{ vanish for } x_{i} = a_{i}, \] pp. 22-24.
   2. \[ f(x) \sum_{j} d_{j} x_{j} = R(y), \] pp. 23-24.
   3. \[ \sum_{i} \prod_{j} a_{i,j} x_{i} x_{j} = g(y), \] pp. 25-28.
   4. \[ f(x,y) = g(x,y), \] pp. 28-32.
   5. \[ \frac{ax^{3}u^{*}}{v^{*}} + \frac{by^{*}v^{*}}{u^{*}} = \frac{ox^{*}}{w}, \] pp. 32-33.
   6. \[ \sum_{i} a_{i} x_{i} x_{i} = \sum_{i} b_{i} x_{i}, \] pp. 33-34.
   7. \[ \prod_{i} \sum_{j} a_{i,j} x_{i} x_{j} = \sum_{j} b_{j} y_{j}, \] pp. 34-35.
ABSTRACT

Diophantine analysis, while an old subject, is a collection of special problems. The methods used are very varied and those used to solve one problem will not usually solve a second one. It is possible that this condition exists because Diophantine analysis is usually considered as number theory. While some problems are problems in number theory, a large body of material may be developed by algebraic methods. In this thesis the methods of algebra are exploited.

The material of this thesis divides itself into chapters naturally, according to the degree of the equations. Considered in order are quadratics, cubics, quartics, and equations of degree n. All equations considered are homogeneous polynomials except a few of degree n. All except two equations are generalized to equations of degree n. The solutions are given in terms of arbitrary parameters and are integral for an integral choice of the parameters.

An important concept of this thesis is the introduction of equivalent solutions (due to Professor W. V. Parker).

Consider the Diophantine equation

\[ f(x_1, \ldots, x_p) = g(y_1, \ldots, y_q), \]

where \( f \) and \( g \) are homogeneous polynomials with integral coefficients, of degrees \( m \) and \( n \) respectively. If \( x_i = \alpha_i \), \( y_j = \beta_j \) is a solution of (1) and there are no integers \( s > 1 \), \( \alpha_i' \), \( \beta_j' \) such that \( \alpha_i = \alpha_i' s^\lambda, \beta_j = \beta_j' s^\mu \) where \( \lambda, \mu \) are relatively prime positive integers such that \( \lambda m = \mu n \), then
is defined to be a primitive solution of (1). If \( x_i = \alpha_i, y_j = \beta_j \) is a primitive solution of (1), then
\[
x_i = \alpha_i t^3, \quad y_j = \beta_j t^4,
\]
where \( t \) is a non-zero integer, is also a solution which is said to be derived from this primitive solution. Two solutions are defined to be equivalent if they may be derived from the same primitive solution.

Each solution obtained is shown, within certain limits, to be general. For a given solution of one of the equations considered, the parameters are chosen in such a way that a solution, equivalent to the given one, is obtained, provided the given solution is not also a solution of a certain equation. Usually, if the original equation is of degree \( n \), the "certain" equation is of degree \( n - 1 \).
CHAPTER I

INTRODUCTION

Diophantine analysis treats the problem of finding rational numbers or integers which satisfy the equation

\[ f(x_1, \ldots, x_r) = 0. \]

Usually \( f \) is a polynomial with integral coefficients. Few problems have been solved when \( f \) is not a polynomial. The solutions are given in terms of arbitrary parameters.

This thesis will be concerned with finding, in terms of parameters, solutions which will be integral for an integral choice of the parameters. The functions will be polynomials except in several problems considered at the end of Chapter V.

While Diophantine analysis is an old subject and has been studied extensively, it remains for the most part a collection of special problems. It appears that this is due to the subject's being unfortunately linked with number theory rather than with algebra. It is true that some problems in Diophantine analysis are problems in number theory, but a large body of material may be developed by strictly algebraic methods. As an insight into the state of development of the subject we quote from Carmichael:


of degree higher than the fourth we find but little effective progress has been made. Often it is a matter of great dif-
difficulty to determine whether a given solution is the general solution of a given equation. Indeed this is true, to a large extent, of equations of the third and fourth degrees. Even here there are but few equations for which a general solution is known or for which it is known that no solution at all exists. As the degree of the equation increases, the generality of the known results decreases in a rapid ratio. Only the most special equations of degree higher than the fourth have been at all treated and for only a few of these is one able to answer the question naturally pronounced as to the existence or generality of solutions.

If \( x_i = \alpha_i, \ y_j = \beta_j \) is a solution of the equation

\[
(1:1) \quad f(x_1, \ldots, x_r) = g(y_1, \ldots, y_s)
\]

where \( f \) and \( g \) are homogeneous polynomials of degrees \( m \) and \( n \), respectively, and there are no integers \( s > 1, \alpha'_i, \beta'_j \) such that \( \alpha_i = \alpha'_i s^\lambda, \beta_j = \beta'_j s^\mu \), where \( \lambda, \mu \) are relatively prime positive integers such that \( \lambda m = \mu n \), then \( x_i = \alpha_i, \ y_j = \beta_j \) is defined to be a primitive solution of the equation. If \( x_i = \alpha_i, \ y_j = \beta_j \) is a primitive solution of \((1:1)\), then \( x_i = \alpha_i t^\lambda, \ y_j = \beta_j t^\mu \), where \( t \) is a non-zero integer, is also a solution, which is said to be derived from this primitive solution.

Two solutions are defined to be equivalent if they may be derived from the same primitive solution.

2/ This definition of equivalence of solution as well as its subsequent application is due to Professor W. V. Parker.

A primitive solution of a Diophantine equation has been defined as a set of relatively prime integers which satisfy
the equation. Under this definition some equations, for example, \( x^n - y^n = z^3 \), have solutions but do not have primitive solutions. However, \( x = \alpha (\alpha' - \beta')^3, y = \beta (\alpha'' - \beta'')^3, z = (\alpha' - \beta')^3 \) is a primitive solution of this equation according to the definition of this thesis. From a relative prime (primitive) solution other solutions may be obtained by multiplying each by a power of some constant. In this thesis, a primitive solution is obtained by dividing any solution by a power of some constant. It is believed that one procedure is as general as the other.
CHAPTER II

QUADRATIC EQUATIONS

A. Desboves has shown that, given a solution of the equation $\sum_{ij} a_{ij} x_i x_j = 0$, other solutions may be determined. The method is shown in the first theorem.

Theorem 2:1. If $x_i = \alpha_i$ is a solution of the equation

$$ \sum_{ij} a_{ij} x_i x_j = 0, $$

then every solution, which is not also a solution of

$$ \sum_{ij} a_{ij} \alpha_i x_j = 0, $$

is equivalent to one of the solutions given by

$$ x_i = \alpha i s - \lambda_i t $$

where

$$ s = \sum_{ij} a_{ij} \lambda_i \lambda_j, \quad t = 2 \sum_{ij} a_{ij} \alpha_i \lambda_j $$

and the $\lambda_i$ are arbitrary integers.

Proof. If $x_i$ have the values given by (2:3), then (2:1) becomes

$$ 2st \sum_{ij} a_{ij} \alpha_i \lambda_j = t^2 \sum_{ij} a_{ij} \lambda_i \lambda_j, $$

which is satisfied identically in the $\lambda_i$ if $s$ and $t$ are given by (2:4).

Suppose now that $x_i = \rho_i$ is a given solution of (2:1). If we choose $\lambda_i = \rho_i$, then $s = 0$ and (2:3) becomes $x_i = -\rho_i t$ which is equivalent to the given solution provided $t \neq 0$; that is, provided $x_i = \rho_i$ is not also a solution of (2:2).

Desboves states that (2:3) gives all solutions of (2:1) if two equivalent solutions are regarded as the same solution. That this is not the case is seen from the proof of Theorem 2:1.
Various quadratic equations will now be solved without considering a particular solution. Each equation considered is such, however, that a particular solution may be noted by inspection.

Theorem 2.2. Every solution of the equation
\[ \sum_{i} a_i x_i^2 = \sum_{i} b_i z^2, \]
where all the a's are different from zero and \( \sum_{i} b_i \neq 0 \), is equivalent to one of the solutions given by
\[ x_j = 2K \alpha_j \sum_{i} a_i b_i \alpha_i - K_j b_j \sum_{i} a_i^2 \alpha_i^2, \quad (j = 1, \ldots, n), \]
\[ z = K \sum_{i} a_i^2 \alpha_i^2, \]
where \( K \) is the least common multiple of the a's, \( K_j = K/a_j \) and the \( \alpha_i \)'s are arbitrary integers.

Proof. Write (2.5) in the form
\[ \sum_{i} (b_i z^2 - a_i x_i^2) = 0. \]
If
\[ b_j z + a_j x_j = a_j \alpha_j t, \quad (j = 1, \ldots, n) \]
then (2.7) becomes
\[ 2zt \sum_{i} a_i b_i \alpha_i = t^2 \sum_{i} a_i^2 \alpha_i^2, \]
which is satisfied identically in the \( \alpha_i \)'s if \( z = K \sum_{i} a_i \alpha_i \), \( t = 2K \sum_{i} a_i b_i \alpha_i \). Hence a solution of (2.5) is given by (2.6).

Suppose now that \( x_j = \lambda_j, z = \rho \) is any solution of (2.5). Then
\[ \sum_{i} a_i \lambda_i = \sum_{i} b_i \rho. \]
If
\[ \alpha_j = K \lambda_j + K_j b_j \rho, \quad (j = 1, \ldots, n) \]
then (2.6) becomes
\[ z = \rho R, x_j = \lambda_j R, \quad (j = 1, \ldots, n) \]
where \( R = 2K \sum_{i} b_i (a_i \lambda_i + b_i \rho) \). However if
\[(2:13) \quad \alpha_j = K \lambda_j - K b_j \rho, \quad (j = 1, \ldots, n)\]

then \((2:6)\) becomes
\[(2:14) \quad z = -\rho S, \quad x_j = \lambda_j S, \quad (j = 1, \ldots, n)\]

where \(S = 2K \sum_i b_i (a_i \lambda_i - b_i \rho)\).

Now if either \(R\) or \(S\) is non-zero, then either \((2:12)\) or \((2:14)\) is a solution of \((2:5)\), each of which is equivalent to the solution \(z = \rho, \quad x_j = \lambda_j\).

It will now be shown that \(R\) and \(S\) are not both zero unless the solution is the trivial one \(\rho = \lambda_j = 0\). If \(R = 0\), then since \(K \neq 0\), \(\sum_i b_i (a_i \lambda_i + b_i \rho) = 0\), and hence
\[(2:15) \quad \sum_i b_i \rho (a_i \lambda_i + b_i \rho) = 0.\]

From \((2:10)\), \((2:15)\) becomes
\[(2:16) \quad \sum_i a_i \lambda_i (a_i \lambda_i + b_i \rho) = 0.\]

By adding \((2:15)\) and \((2:16)\) it follows that \(\sum_i (a_i \lambda_i + b_i \rho)^2 = 0\), and hence
\[(2:17) \quad a_j \lambda_j + b_j \rho = 0, \quad (j = 1, \ldots, n).\]

Similarly, if \(S = 0\),
\[(2:18) \quad a_j \lambda_j - b_j \rho = 0, \quad (j = 1, \ldots, n).\]

Since all the \(a_i\)'s are different from zero, each \(\lambda_i\) must be zero in order that \((2:17)\) and \((2:18)\) be true simultaneously, and hence \(\rho = 0\).

If each \(a_i = 1\), \(b_i = 1\), \(b_i = 0\) \((i = 2, 3, \ldots, n)\), \((2:5)\) reduces to the sum of \(n\) squares equal to a square. The solution in this case is given by \(z = \sum_i a_i^2, \quad x_i = a_i^2 = \sum_i a_i^2,\)

---


\[x_j = 2 \alpha_j \xi_j, \quad (j = 2, 3, \ldots, n). \] In particular, for \(n = 3\), the solutions of
(2:19) \[ x^2 + y^2 + z^2 = t^2 \]

are

\[ t = \alpha^2 + \beta^2 + \gamma^2, \quad x = \alpha^2 - \beta^2 - \gamma^2 \]

(2:20)

\[ y = 2 \alpha \beta, \quad z = 2 \alpha \gamma. \]

Catalan has pointed out that these formulas do not give all solutions of (2:19), but that all relatively prime solutions are given by

\[ t = m^2 + n^2 + p^2 + q^2, \quad x = m^2 - n^2 - p^2 + q^2, \]
\[ y = 2mn + 2pq, \quad z = 2mp - 2nq. \]

If in (2:20) the choice \( \alpha = m^2 + q^2, \beta = mn + pq, \gamma = mp - nq \) is made, then

\[ t = (m^2 + q^2)(m^2 + n^2 + p^2 + q^2), \]
\[ x = (m^2 + q^2)(m^2 - n^2 - p^2 + q^2), \]
\[ y = (m^2 + q^2)(2mn + 2pq), \]
\[ z = (m^2 + q^2)(2mp - 2nq), \]

which is equivalent to (2:21) provided \( m^2 + q^2 \neq 0 \). If \( m = q = 0 \), then (2:21) becomes \( t = n^2 + p^2, x = -n^2 - p^2, \)
\( y = z = 0 \), which is given by (2:20) with \( \alpha = 0, \beta = n, \gamma = p \).

Hence in every case, for any solution given by (2:21), an equivalent solution is given by (2:20).

The solutions of the equation

(2:22) \[ \sum_i d_i x_i^* = \sum_i d_i z^* \]

may be determined by Theorem 2:2 by setting \( a_i^* = b_i^* = d_i \). After removing the common factor \( K \) from each expression in (2:6)

(2:23) \[ z = \sum_i d_i a_i^*, \quad x_j = 2a_j \sum_i d_i a_i^*, \quad \sum_i d_i a_i^* = \sum_i d_i a_i^*, \quad (j = 1, \ldots, n) \]
follows as a solution of (2:22). Since (2:23) satisfies (2:22) identically in the \( d_i \)'s, it is not necessary to assume that \( d_i \) be a square or that it be positive. It may be shown as above, that (2:23) gives a solution equivalent to any existing solution of (2:22).

**Theorem 2:3.** The equation

\[
(2:24) \quad \sum (a_i x_i + b_i y_i)(c_i x_i + d_i y_i) = 0,
\]
has solutions and every solution which is not also a solution of

\[
(2:25) \quad \sum a_i c_i (K x_i + b_i K y_i) = 0,
\]
where \( K \) is the least common multiple of the \( a_i \)'s, \( K_i = K/a_i \), is equivalent to one of the solutions given by

\[
(2:26) \quad x_i = \alpha_i t - b_i K_i \beta_i s, \quad y_i = \beta_i K s
\]
where

\[
(2:27) \quad s = \sum a_i c_i \alpha_i, \quad t = K \sum a_i \beta_i (b_i c_i - a_i d_i),
\]
and the \( \alpha_i \) and \( \beta_i \) are arbitrary integers.

**Proof.** Let \( a_i x_i + b_i y_i = a_i x, y_i = \beta_i K s \). Then

\[
x_i = \alpha_i t - b_i K_i \beta_i s. \quad \text{Substituting in (2:24) gives}
\]

\[
t + \sum a_i c_i \alpha_i = stK \sum a_i \beta_i (b_i c_i - a_i d_i)
\]
which is identically satisfied in the \( \alpha_i \) and \( \beta_i \) if \( s \) and \( t \) are given by (2:27). Hence (2:26) is a solution of (2:24).

Suppose \( x_i = \lambda_i, y_i = \mu_i \) is any given solution of (2:24). If \( \alpha_i = K \lambda_i + b_i K \mu_i \), \( \beta_i = \mu_i \), then

\[
t = K \sum \mu_i (b_i c_i - a_i d_i)(K \lambda_i + b_i K \mu_i),
\]

\[
s = \sum a_i c_i (K \lambda_i + b_i K \mu_i)^2
\]
and since

\[
\sum (a_i c_i \lambda_i^2 + b_i c_i \lambda_i \mu_i) = \sum (a_i d_i \lambda_i \mu_i + b_i d_i \mu_i^2),
\]

\[
\sum a_i c_i \lambda_i^2 + b_i c_i \lambda_i \mu_i = \sum a_i d_i \lambda_i \mu_i + b_i d_i \mu_i^2,
\]
and

\[
K^2 \sum (a_i c_i \lambda_i^2 + b_i c_i \lambda_i \mu_i) + K^2 \sum b_i c_i \lambda_i \mu_i - \sum a_i d_i \lambda_i \mu_i + b_i d_i \mu_i^2.
\]
Hence $x_i = \lambda_i Ks$, $y_i = \mu_i Ks$ which is equivalent to the given solution if $x_i = \lambda_i$, $y_i = \mu_i$ is not also a solution of (2:25).

It will be noted that this also solves the equation

$$\sum_i (a_i x_i + b_i y)(c_i x_i + d_i y) = 0,$$

of which (2:5) is a special case. In this case let $\beta = 1$ in (2:26).

Likewise the general homogeneous quadratic equation may be solved if it contains either two or three terms which are quadratic in two unknowns, and which are factorable into the product of two linear factors with integral coefficients.

This is shown in the next theorem.

Theorem 2:4. The equation

$$(2:28) \quad (\alpha y + \beta z)(\gamma y + \delta z) = y \sum_i b_i x_i + z \sum_i a_i x_i + \sum_i c_i x_i x_j,$$

where $\alpha$ and $\beta$ are not both zero, and $\gamma$ and $\delta$ are not both zero, has solutions, and every solution which is not a solution of

$$(2:29) \quad (bc - ad)(\alpha y + \beta z) + \sum_i (ab_i - ba_i) x_i = 0,$$

is equivalent to one of the solutions given by

$$y = -d \alpha^2 - \alpha \sum_i b_i \alpha_i + b \sum_i c_i \alpha_i \alpha_j,$$

$$z = c \alpha^2 - \alpha \sum_i a_i \alpha_i - a \sum_i c_i \alpha_i \alpha_j,$$

$$x_i = \alpha_i \left[ (bc - ad) \alpha + \sum_i (ab_i - ba_i) \alpha_j \right], \quad (k = 1, \ldots, n),$$

where $\alpha$, $\alpha_i$ are arbitrary integers.

Proof. Let

$$(2:31) \quad ay + bz = \alpha t, \quad x_i = \alpha_i t,$$

then (2:28) becomes

$$s = \sum_i ( - K^2 a_i d_i \lambda_i \mu_i - K b_i d_i \mu_i + K b_i c_i \lambda_i \mu_i + a_i b_i c_i K \mu_i)^2$$

$$= K \sum_i \mu_i (b_i c_i - a_i d_i)(K \lambda_i + b_i K \mu_i).$$

$$= t.$$
The combination of (2:31) and (2:32) gives
\[
[tz = \left[ \frac{(bc - ad)\alpha + \sum_i (ab_i - ba_i)\alpha_i}{t} \right] t + \left[ \frac{(bc - ad)\alpha + \sum_i (ab_i - ba_i)\alpha_i}{t} \right] z = \left[ \frac{2 \sum_a \alpha_i \alpha_i - b \sum_i \alpha_i}{t} \right],
\]
which are satisfied identically in the \( \alpha \)'s if
\[
y = -d\alpha + a \sum_i b_i \alpha_i + b \sum_i c_i \alpha_i \alpha_i,
\]
\[
z = c \alpha^2 - d \sum_i a_i \alpha_i - a \sum_i c_i \alpha_i \alpha_i,
\]
\[
t = (bc - ad)\alpha + \sum_i (ab_i - ba_i)\alpha_i.
\]
Hence (2:30) is a solution of (2:28).

Suppose now that \( y = \rho, z = \sigma, x_k = \lambda_k \) is any solution
of (2:28). If in (2:30), \( \alpha = a\rho + b\sigma, \lambda_k = \lambda_k \), then
\[
y = a\rho P, z = b\sigma P, x_k = \lambda_k P \text{ where}
\]
\[
P = (bc - ad)(a\rho + b\sigma) + \sum_i (ab_i - ba_i)\lambda_i,
\]
which is equivalent to the given solution provided \( P \neq 0 \); that
is, provided \( y = \rho, z = \sigma, x_k = \lambda_k \) is not a solution of (2:29).

Interchanging \( a \) with \( c \), \( b \) with \( d \) in (2:30) gives
\[
y = -b\alpha^2 + a \sum_i b_i \alpha_i + d \sum_i c_i \alpha_i \alpha_i,
\]
\[
z = a \alpha^2 - b \sum_i a_i \alpha_i - c \sum_i c_i \alpha_i \alpha_i,
\]
\[
x_k = \alpha_k \left[ (ad - bc) \alpha + \sum_i (ob_i - da_i) \alpha_i \right], \quad (k = 1, \ldots, n),
\]
a solution equivalent to any existing solution which does
not satisfy
\[
(2:34) \quad (ad - bc)(\alpha^2 + dz) + \sum_i (ob_i - da_i)x_i = 0.
\]
A solution of the sum of \( m \) squares equal to the sum of \( n \)

squares may be obtained by Theorem 2:4 or by Theorem 2:2 after

a transformation of the equation. The equation
\[
(2:35) \quad \sum_i x_i^2 = \sum_i y_i^2 \quad m \geq n,
\]
may be written in the form
\[ (x_i - y_i)(x_i + y_i) = \sum_{j=1}^{n} y_j - \sum_{j=1}^{n} x_j, \]

which is a special case of Theorem 2:4. However, letting \( y_j = x_j t \) \((j = 1, \ldots, n)\), (2:35) becomes

\[ \sum_{j=1}^{n} x_j^2 = \sum_{j=1}^{n} x_j^2 t^2 \]

where \( s_j = 0 \) for \( j > n \). Then (2:36) is a special case of Theorem 2:2, and may be solved for \( x_1, x_2, \ldots, x_m, t \) in terms of \( m \) parameters. It will be noted that the first method gives the solution in terms of \( m+n-1 \), while the second method gives the solution in terms of \( m+n \) parameters.

A combination of Theorem 2:1 and Theorem 2:4 may be used to obtain a solution equivalent to any solution of (2:28). For example, consider the equation

\[ 2x^2 + 3xy + y^2 - xz - yz + yw - 2zw = 0, \]

which may be written in the form

\[ (x+y)(2x+y) = xz + yz + yw + 2zw. \]

From (2:30) and (2:33) the two solutions

\[ x = -p^2 + pq - pr + 2qr, \]
\[ y = 2p^2 - pq - 2qr, \]
\[ z = pq - qr, \]
\[ w = pr - r^2, \]

and

\[ x = -p^2 + pq - pr + 2qr, \]
\[ y = p^2 - pq - 4qr, \]
\[ z = -pq + q^2 - 2qr, \]
\[ w = -pr + qr - 2r^2, \]

are obtained.

Any solution which does not satisfy
\[(2:40) \quad x + y - w = 0\]

is equivalent to one given by \((2:38)\), and any solution which does not satisfy
\[(2:41) \quad 2x + y - z + 2w = 0\]
is equivalent to one given by \((2:39)\).

Now \((2:37)\), \((2:40)\), and \((2:41)\) have the common solutions \((1, -1, 1, 0)\) and \((-7, 10, 2, 3)\). \((2, -2, -1, -1)\) is a particular solution of \((2:37)\) obtained from \((2:38)\) by choosing \(p = 0, q = r = 1\). From this particular solution Theorem 2:1 gives the solution
\[(2:42) \quad x = \alpha^2 + 4\alpha\beta + 2\beta^2 - 4\gamma\delta - 2\gamma\delta + 2\beta\delta - 4\gamma\delta, \]
\[y = -4\alpha^2 - 2\alpha\beta - 4\beta^2 + 2\alpha\delta - 2\beta\delta + 4\gamma\delta, \]
\[z = -2\alpha^2 - 3\alpha\beta - \beta^2 - 2\alpha\delta - \beta\delta - 2\gamma\delta - \beta\delta + 2\gamma\delta, \]
\[w = -2\alpha^2 - 3\alpha\beta - \beta^2 + \alpha\delta + \beta\delta - 3\alpha\delta - 3\beta\delta. \]

Now \((2:42)\) gives a solution equivalent to any existing one which is not a solution of
\[(2:43) \quad 3x + 2y + 2z = 0. \]

But \((2:37)\), \((2:40)\), \((2:41)\), and \((2:43)\) have no solutions in common. Hence given any solution of \((2:37)\) we may find a solution equivalent to it from either \((2:38)\), \((2:39)\), or \((2:42)\).
CHAPTER III
CUBIC EQUATIONS

Several methods have been given for solving the equation $x^3 + y^3 = u^3 + v^3$. Here a more general equation is solved, of which this is a special case. This is given in the following theorem.

Theorem 3.1. The equation

$$3/ \ W. \ V. \ Parker \ and \ A. \ A. \ Aucoin, \ "Solution \ of \ a \ Cubic \ Diophantine \ Equation," \ Tohoku \ Mathematical \ Journal, \ 45, \ 324-328, \ part \ 2, \ March, \ 1939.$$

(3.1) \quad (ax + by)(mx^3 + nxy + py^3) = (cu + dv)(mu^3 + nuv + pv^3)

has solutions and every solution which is not also a solution of

(3.2) \quad (mx^3 + nxy + py^3) \left\{ \frac{[bc - ad]mx + (ben - aop - bdm)y}{cu + dv} \right\} u + (bdm - adn + aop)x + (bo - ad)pyv = 0

is equivalent to one of the solutions given by

$$x = \gamma \left[ b \gamma^2 - \left( \alpha^2 + n \alpha \beta + mp \beta^2 \right) (d \alpha + dn \beta - op \beta) \right],$$

$$y = \gamma \left[ (\alpha^2 + n \alpha \beta + mp \beta^2) (c \alpha + dm \beta) - a \gamma \right],$$

$$u = (b \alpha + ap \beta) \gamma^2 - d (\alpha^2 + n \alpha \beta + mp \beta^2) \gamma,$$

$$v = (mb \beta - a \alpha - an \beta) \gamma^2 + c (\alpha^2 + n \alpha \beta + mp \beta^2) \gamma,$$

where $\alpha, \beta, \gamma$ are arbitrary integers.

Proof. Write (3.1) in the form

$$3/ \ ax + by \over cu + dv = \left( \frac{mu^3 + nuv + pv^3}{mx^3 + nxy + py^3} \right).$$

Since $\gamma (mu^3 + nuv + pv^3) = (mx^3 + nxy + py^3) (\alpha^2 + n \alpha \beta + mp \beta^2)$
(3:5) \[ y u = \alpha x - p \beta y, \quad y v = m x + (\alpha + n \beta)y, \]

(3:6) \[ ax + by = \frac{mu' + n u v + py'}{ou + dv} = \frac{\alpha^2 + n \alpha \beta + mp \beta}{\gamma^2}, \]

may be written in place of (3:4). If \( ou + dv = \delta \), from (3:6) and (3:8) it follows that

\((c + dm \beta)x + [d(\alpha + n \beta) - cp \beta]y = \gamma \delta,\)

(3:7)

Let

\[ \delta = \begin{vmatrix}
  c + dm \beta & d(\alpha + n \beta) - cp \beta \\
  a \gamma & b \gamma
\end{vmatrix} \]

and solve (3:7) for \( x \) and \( y \). With these values, \( u \) and \( v \) may be determined from (3:5), and it is seen that (3:3) is a solution of (3:1).

If \((x, y, u, v)\) is any solution of \( ax + by = 0 \) or \( mx^2 + nxy + py^2 = 0 \) and \((u, v)\) is any solution of \( ou + dv = 0 \) or \( mu' + n u v + py' = 0 \), then \((x, y, u, v)\) is a trivial solution of (3:1). Such solutions will not be considered.

Suppose that \( x = \lambda, y = \mu, u = \rho, v = \sigma \) is any non-trivial solution of (3:1). Choose \( \alpha = m \lambda \rho + n \mu \rho + p \mu \sigma, \beta = \lambda \rho - \mu \rho, \gamma = m \lambda^2 + n \lambda \mu + p \mu^2, \)

\[ \alpha^2 + n \alpha \beta + mp \beta = (m \lambda^2 + n \lambda \mu + p \mu^2)(m \rho^2 + n \rho \sigma + p \sigma^2), \]

so that when these values are substituted in (3:3) it follows that \( x = \lambda K, y = \mu K, u = \rho K, v = \sigma K \), where \( K \) is the left hand member of (3:2) with \( x, y, u, v \) replaced by \( \lambda, \mu, \rho, \sigma \). Hence every solution of (3:1) which does not satisfy (3:2) is equivalent to a solution given by (3:3).
The following observation is made concerning the solution. If a non-trivial solution does satisfy (3:2), then

\[ (3:8) \]
\[
\begin{align*}
& u = \mathcal{S}[(adn - aop - bdm)x - (bo - ad)py], \\
& v = \mathcal{S}[(bc - ad)mx + (bon - aop - bdm)y].
\end{align*}
\]

If the values from (3:8) are substituted in (3:1), then

\[ (3:9) \]
\[
(ax + by)(mx' + nxy + py') = MS'(ax + by)(mx' + nxy + py')
\]

where

\[
M = (c' p + d' m - cdn) \begin{vmatrix} adn - aop - bdm & (ad - bc)p \\ (bo - ad)m & bon - aop - bdm \end{vmatrix}.
\]

Any values \((x, y)\) will satisfy (3:9) if \(MS^3 = 1\) and no value if \(MS^3 \neq 1\). Therefore, in addition to the values given by (3:3), (3:1) is satisfied by all integral solutions of

\[ (3:10) \]
\[
\sqrt{M} u = (adm - aop - bdm)x - (bc - ad)py, \\
\sqrt{M} v = (bo - ad)mx + (bon - aop - bdm)y,
\]

if (3:10) has any integral solutions.

For the equation \(x^2 + y^2 = u^2 + v^2\), \(a = b = c = d = m = p = -n - 1\) and (3:3) becomes

\[
x = \gamma y^4 - (a - 2 \beta)(a^+ - \alpha \beta + \beta^+),
\]
\[
y = \gamma [(a + \beta)(a^+ - \alpha \beta + \beta^+) - y^4],
\]
\[
u = (a + \beta)y^3 - (a^+ - \alpha \beta + \beta^+)y^2,
\]
\[
v = (a^+ - \alpha \beta + \beta^+)y^3 - (a - 2 \beta)y^2.
\]

By the use of a multiplicative domain, Carmichael obtains a solution of the equation

\[ (3:11) \]
\[
x^2 + y^2 + z^2 - 3xyz = u^2 + v^2 + w^2 - 3uvw.
\]
He says, "This solution, so readily obtained, unfortunately lacks generality." By a second method he gets expressions for \(x, y, u, v\) in terms of arbitrary parameters \(a, b, z, w\). These are not shown to give the general solution of (3.11).

A more general problem will now be solved which gives the general solution of (3.11) as a special case. Let 
\[
f(x) = f(x_1, \ldots, x_n)
\]
be a homogeneous polynomial of degree three with integral coefficients. Suppose \(f(x)\) is such that for a set of integers \(a_1, a_2, \ldots, a_n\), not all zero,
\[
\frac{\partial f}{\partial x_j} = 0, \text{ for } x_j = a_j, \quad (1, j = 1, \ldots, n).
\]
If \(x_j = a_j s + \beta_j t\), then
\[
f(x) = s^3 f(a) + s^2 t \sum_j a_j \frac{\partial f}{\partial x_j} + st \sum_j a_j \frac{\partial^2 f}{\partial x^2} + t^3 f(x),
\]
and since \(\frac{\partial f}{\partial x_j} = 0\), \(f(a) = \frac{1}{3} \sum_j a_j \frac{\partial f}{\partial x_j} = 0\), and hence
\[
f(x) = st \sum_j a_j \frac{\partial^2 f}{\partial x^2} + t^3 f(x).
\]

Theorem 3.2: The equation

\[
\]

\[
(3.12) \quad f(x) = g(y),
\]
where \(g(y) = g(y_1, \ldots, y_n)\) is a homogeneous polynomial of degree three with integral coefficients, has solutions and every solution which is not also a solution of

\[
(3.13) \quad \sum_j a_j \frac{\partial f}{\partial x_j} = 0,
\]
is equivalent to one of the solutions given by

\[
(3.14) \begin{align*}
x_j &= a_j s + \beta_j t, \\
y_j &= \beta_j t,
\end{align*}
\]
where \(s\) and \(t\) are given by
and the $\alpha$'s and $\beta$'s are arbitrary integers.

Proof. If $x$ and $y$ have the values given by (3:14), then (3:12) becomes 
\[ st^t = t \left[ g(\beta) - f(\alpha) \right] \]
which is identically satisfied in the $\alpha$'s and $\beta$'s if $s$ and $t$ have the values given by (3:15).

Let $x_i = \lambda_i$, $y_j = \mu_j$ be any given solution of (3:12). If the choice $\alpha_i = \lambda_i$, $\beta_j = \mu_j$ is made in (3:15), then since $s = 0$, the solution becomes $x = \lambda : t$, $y = \mu : t$ which is equivalent to the given solution provided $t \neq 0$; that is, provided $x_i = \lambda_i$, $y_j = \mu_j$ does not satisfy (3:13).

Consider now equation (3:11). Here 
\[ \frac{dx}{dt} = \frac{dy}{dt} = \frac{dz}{dt} = 0, \]
for $x = y = z = 1$. Hence the solution is
\begin{align*}
    x &= (\lambda^3 + \lambda \mu \nu^2 - 3 \lambda \mu \nu) + (\alpha - \beta)^3 + (\alpha - \gamma)^3, \\
    y &= (\lambda^3 + \mu^2 + \nu^2 - 3 \lambda \mu \nu) + (\beta - \alpha)^3 + (\beta - \gamma)^3, \\
    z &= (\lambda^3 + \mu^2 + \nu^3 - 3 \lambda \mu \nu) + (\gamma - \alpha)^3 + (\gamma - \beta)^3, \\
    u &= 3 \lambda (\alpha^2 + \beta^2 + \gamma^2 - \alpha \beta - \alpha \gamma - \beta \gamma), \\
    v &= 3 \mu (\alpha^2 + \beta^2 + \gamma^2 - \alpha \beta - \alpha \gamma - \beta \gamma), \\
    w &= 3 \nu (\alpha^2 + \beta^2 + \gamma^2 - \alpha \beta - \alpha \gamma - \beta \gamma),
\end{align*}
(3:16)

Now (3:16) gives a solution equivalent to any solution of (3:11) if it does not satisfy
\[ x^2 + y^2 + z^2 - xy - xz - yz = 0. \]
(3:17)

It is now shown that (3:17) has no solution other than $x = y = z$. Suppose $x = \alpha$, $y = \beta$, $z = \gamma$ is any solution of (3:17). Then $x = \alpha - 1$, $y = \beta - 1$, $z = \gamma - 1$ is also a solution.

Now there is no loss of generality in supposing that one of the numbers, say $\alpha$, is positive. By continuing to subtract
one from the values of $x$, $y$, $z$ a solution is obtained in which $x = 0$ and $y$ and $z$ must be a solution of $y^2 - yz + z^2 = 0$. But this equation has no solutions other than $y = z = 0$. Hence $x = y = z = \alpha$ is the only solution of (3.17). It has been shown, incidentally, that all the solutions of the equation $x^6 + y^6 + z^6 - 3xyz = 0$ except the trivial one $x = y = z$ are solutions of $x + y + z = 0$. These may be obtained from (3.16)

by setting $\lambda = \mu = \nu = 0$. Or it is seen by inspection that $x + y + z = 0$ is satisfied by $x = \alpha$, $y = \beta$, $z = -(\alpha + \beta)$.

12/ Leonard E. Dickson, op. cit., p. 590.
CHAPTER IV

QUARTIC EQUATIONS

One function \( f \) which satisfies the conditions of Theorem 3:2 is the product of three linear factors in three unknowns. The next consideration will be an equation in which the left hand member is the product of four linear factors in three unknowns.

Theorem 4:1. The equation

\[
\prod_{i} \sum_{j} a_{ij} x_j = g(y),
\]

where \( g(y) = g(y_1, \ldots, y_p) \) is a homogeneous polynomial of degree \( n, n \not\equiv 0(\text{mod } 4) \), has solutions and every solution for which the members of (4:1) do not vanish is equivalent to either a solution given by

\[
x_j = A^{-1} s^n t^n [t(\alpha, A_{i,j} + \alpha_2 A_{i,j}) + s \alpha_3 A_{i,j}],
\]

\[
y_j = A^* s^n t^n \beta_j,
\]

or a solution given by

\[
x_j = A^{-1} s^n t^n [t(\alpha, A_{i,j} + \alpha_2 A_{i,j}) + s \alpha_3 A_{i,j}],
\]

\[
y_j = A^* s^n t^n \beta_j,
\]

according as \( n = 2m + 1 \) or \( n = 4m + 2 \), where \( A \neq 0 \) is the determinant of the forms \( \sum_{j} a_{ij} x_j \) \((i = 1, 2, 3)\) and \( A_{i,j} \) is the cofactor of \( a_{ij} \) in \( A \), \( s \) and \( t \) are given by

\[
s = \alpha_1 \alpha_2 \alpha_3 \sum_{j} a_{ij} (\alpha, A_{i,j} + \alpha_2 A_{i,j}),
\]

\[
t = \alpha_1 \alpha_2 \alpha_3 \sum_{j} a_{ij} A_{i,j},
\]

the \( \alpha \)'s and \( \beta \)'s being arbitrary integers.

Proof. Let

\[
\sum_{j} a_{ij} x_j = A^* s^n t^n, \quad \sum_{j} a_{ij} x_j = A^{**} s^n t^{**} (i = 1, 2).
\]
The solution of this system of equations is

\[(4:6)\quad x_j = A^{-\nu} s^{-\mu} t^{-\lambda} \left[ t(\alpha_i A_{ij} + \alpha_i A_{ij}) + \alpha_i A_{ij} \right]\]

and hence

\[(4:7)\quad \sum_j a_{ij} x_j = A^{-\nu} s^{-\mu} t^{-\lambda} \left[ t \sum_j a_{ij} (\alpha_i A_{ij} + \alpha_i A_{ij}) + \sum_i a_{ij} A_{ij} \right].\]

The theorem now divides itself into two cases. First let \(n = 2m + 1\). If

\[(4:8)\quad y_k = A^{\nu} s^{\mu} t^{\lambda},\]

then from (4:5), (4:7), and (4:8), (4:1) becomes

\[(4:9)\quad A^{-\nu} s^{-\mu} t^{-\lambda} + a_i A_{ij} \left[ t \sum_j a_{ij} (\alpha_i A_{ij} + \alpha_i A_{ij}) + \sum_i a_{ij} A_{ij} \right] = A^{-\nu} s^{-\mu} t^{-\lambda} g(\beta),\]

which is identically satisfied in the \(\alpha_i\) and \(\beta_i\) if \(s\) and \(t\) are given by (4:4).

Second, let \(n = 4m + 2\). If

\[(4:10)\quad y_k = A^{\nu} s^{\mu} t^{\lambda},\]

then (4:1) becomes (4:9) and hence as before \(s\) and \(t\) are given by (4:4).

Suppose now that \(x_j = \lambda_j, y_k = \mu_k\) is any solution of (4:1). Choose \(\alpha_i = \sum_j a_{ij} \lambda_i, \beta_i = \mu_i, \) and then

\[
s = \left[ \sum_j a_{ij} \lambda_j \right] \sum_k \sum_j \left( a_{ik} A_{ij} + a_{ik} A_{ij} \right) \lambda_k^2
\]

\[
t = A g(\beta) - \left[ \sum_j a_{ij} \lambda_j \right] \sum_k \sum_j \left( a_{ik} A_{ij} \right) \lambda_k^2
\]

\[
= \left[ \sum_j a_{ij} \lambda_j \right] \left\{ A \sum_k \left( a_{ik} A_{ij} \right) \lambda_k^2 - \sum_k \left( a_{ik} A_{ij} \right) \lambda_k \right\}
\]

and hence

\[
s - t = \left[ \sum_j a_{ij} \lambda_j \right] \left\{ A \sum_k \left( a_{ik} A_{ij} \right) \lambda_k^2 - \sum_k \left( a_{ik} A_{ij} \right) \lambda_k \right\}
\]

\[
= 0,
\]

and \(s = t\). Therefore

\[x_j = t \sum_j a_{ij} \lambda_j.\]
In the first case \( y_k = A^* t^w A^* \) and in the second case \( y_k = A^* t^w A^* \) and so in either case a solution is obtained that is equivalent to any solution.

It is evident that this could be extended to \( 2n \) factors in \( 2n - 1 \) variables with the proper restrictions on \( g(y) \).

A special case of (4:1) is

\[
(x + y + z)(-x + y + z)(x - y + z)(x + y - z) = 4A^2,
\]

which is the formula for expressing the area \( A \) of a triangle in terms of its sides \( x, y, z \). It is often reduced by a linear transformation to

\[
uvw(u + v + w) = t^2
\]

and then solved.

---

\( t \sum_i \sum_j a_{ij} A_{ij} \lambda_k \)

\( = tA \lambda_k \).
CHAPTER V

EQUATIONS OF DEGREE N

The theorems of Chapter II as well as Theorem 3:2 will now be generalized.

Suppose \( f(x) = f(x_1, \ldots, x_n) \) is a homogeneous polynomial of degree \( n \), with integral coefficients, and such that for \( x_i = a_i, a_i \) integral and not all zero, all its partial derivatives of all orders less than \( n - 1 \) vanish. If \( x_i = a_i s + \alpha_i t \), then by Taylor's theorem

\[ f(x) = st^{n-1} \sum_{j} a_j \frac{\partial^n f}{\partial x_j^n} + t^n f(a). \]

Theorem 5:1. The equation

\[ f(x) = g(y), \]

where \( g(y) = g(y_1, \ldots, y_j) \) is a homogeneous polynomial of degree \( m \), has solutions, and every solution which is not also a solution of

\[ f(x) = g(y), \]

is equivalent to one of the solutions given by

\[ x_i = a_i st^{\lambda_i} + \alpha_i t^{\lambda_i}, \]

\[ y_k = \beta_k t^{\mu_k}, \]

where \( \lambda, \mu \) are relatively prime positive integers such that
\(\lambda n = \mu m, \alpha, \beta\) are arbitrary integers, and

\[
\begin{align*}
s &= g(\beta) - f(\alpha), \\
t &= \sum_j a_j \frac{\partial f}{\partial x_j}.
\end{align*}
\]

Proof. If in (5:1), \(x, y\) have the values given by (5:3), then

\[
st^{n-1} - \sum_j a_j \frac{\partial f}{\partial x_j} + t^{n-1} f(\alpha) = t^{n-1} g(\beta),
\]

which is satisfied identically in the \(\alpha\)'s and \(\beta\)'s when \(s\) and \(t\) are given by (5:4). Hence (5:3) affords a solution of (5:1).

Suppose \(x, y\) is any solution of (5:1). If \(\alpha = \beta, \beta = \alpha\), \(s = 0\) and (5:3) becomes \(x = \beta t^2, y = \alpha t^m\), which is equivalent to the given solution provided \(x, y\) is not also a solution of (5:2). It will be noted that \(g\) may be identically zero.

Corollary. The equation

\[
f(x) = \sum_j x_j g_j(y) + g(y),
\]

where \(g_j(y) = g_j(y, \ldots, y_j)\) and \(g(y) = g(y, \ldots, y_j)\) are homogeneous polynomials with integral coefficients of degrees \(n-1\) and \(n\) respectively, has solutions, and every solution which is not also a solution of

\[
\sum_j a_j \left[\frac{\partial f}{\partial x_j} - g_j(y)\right] = 0
\]

is equivalent to one of the solutions given by \(x = a_j \alpha + s t, y = \beta t^m\), where \(s = g(\beta) - f(\alpha) + \sum_j a_j g_j(\beta), t = \sum_j a_j \left[\frac{\partial f}{\partial x_j} - g_j(\beta)\right].

Theorem 5:2. The equation

\[
f(x) \sum_j a_j x_j = R(y),
\]

where \(f\) satisfies the hypothesis of Theorem 5:1 and \(R(y) = R(y, \ldots, y_j)\) is a homogeneous polynomial with integral coefficients, of degree \(n-1\), has solutions and every solution
which is not also a solution of
\[ f(x) \sum_{j} \frac{\delta}{\delta x_j} \left[ \sum_{j} a_j \frac{\delta}{\delta x_j} \sum_{j} d_j x_j - f(x) \sum_{j} d_j a_j \right] = 0 \]
is equivalent to one of the solutions given by

\[ x_i = a_i s + \alpha_i t, \]
\[ y_k = \beta_k t, \]

where
\[ s = A^{-1} \left[ \lambda (AD - BC) \right]^{-2} \left[ D \lambda^2 - BR(\mu) \right], \]
\[ t = A^{-1} \left[ \lambda (AD - BC) \right]^{-2} \left[ AR(\mu) - CA \right], \]
\[ \beta_k = A^{-1} \left[ \lambda (AD - BC) \right]^{\mu_k}, \]

where\[ A = \sum_j a_j \frac{\delta}{\delta x_j}, \quad B = f(x), \quad C = \sum_j d_j a_j, \quad D = \sum_j d_j \delta_j, \quad \delta_j, \lambda, \]
\[ \mu_k \]
being arbitrary integers.

Proof. Let \( x_i, y_k \) have the values given by (5:7).

Then (5:5) becomes
\[ (A s^{n-1} + B t^n)(C s + D t) = t^{n-1} R(\beta), \]
which becomes, after dividing out the factor \( t^{n-1} \),

\[ 16/ \]

It will be shown later that \( t \neq 0 \).

(5:9) \[ (A s + B t)(C s + D t) = R(\beta). \]

By Theorem 5:1 the solution of (5:9) is given by \( (5:8). \)

\[ 17/ \]

It will be shown later that (5:9) satisfies the hypothesis of Theorem 5:1.

Suppose \( x_i = \rho_i; \ y_k = \sigma_k \) is any given solution of (5:5).

Then if \( \alpha_i = \rho_i; \ \mu_k = \sigma_k, \ \lambda = f(\rho), \ s = 0 \) and the solution becomes \( x_i = \rho_i k^{n-1}, \ y_k = \sigma_k k^{n-1} \) where \( K = A k (AD - BC) \), which is proportional to the given solution provided \( K \neq 0 \); that is, provided \( x_i = \rho_i; \ y_k = \sigma_k \) is not a solution of (5:6). It will be noted that if \( K \neq 0 \), then \( t \neq 0 \).
One function of interest which satisfies the hypothesis of Theorem 5:1 is the function \( D(x) = \left| a_{\cdot i} x_{\cdot j} \right| \), a determinant of order \( n \) with \( a_{\cdot i} \) integral such that not all the \( a's \) in any row or column are zero. If there is any element, say \( x_{z^*} \), which is distinct from all others, we may select \( x_{z^*} = 1 \) and \( x_{z^*} = 0 \) otherwise. For this choice all partial derivatives of all orders less than \( n - 1 \) vanish. It is interesting to note that in the solution, the form of the expression for all the \( x's \) is the same except for \( x_{z^*} \). This is illustrated by

\[
D = \begin{vmatrix}
3y & z & 0 \\
u & 3v & 3w & p \\
q & u & 3x & z \\
0 & 2w & 5z & 0
\end{vmatrix} = r^n,
\]

the solution of which is \( x = \alpha t^n, y = \beta t^n, z = \gamma t^n, u = \lambda t^n, v = s t^n, w = \sqrt{\omega} t^n, p = \sigma t^n, q = \delta t^n, r = \pi t^n \), where \( s = \Pi^n - D', t = \Delta, D' \) being \( D \) with \( x, y, z, u, v, w, p, q \), replaced by \( \alpha, \beta, \gamma, \lambda, \mu, \sqrt{\omega}, \rho, \delta \) and

\[
\Delta = \begin{vmatrix}
\alpha & 0 & \gamma & 0 \\
\lambda & 7 & 3\sqrt{\omega} & \rho \\
\sigma & 0 & \lambda & \gamma \\
0 & 0 & 5\gamma & 0
\end{vmatrix}.
\]

It is not necessary, however, that there be one element which is distinct from all others in order that this method apply to certain problems. For example, \( D \) may be the circulant, as it was in Theorem 3:2.

Another function which also satisfies the hypothesis of Theorem 5:1 is the function \( \prod_j \sum_j a_{ij} x_j \), where \( a_{ij} \) are integers and the determinant \( A = |a_{ij}| \neq 0 \). For \( x_j \) may be chosen
integral, so that \( n - 1 \) of the above factors vanish and hence for this choice of \( x_j \), all partial derivatives of all orders less than \( n - 1 \) vanish. Hence the equation
\[
\prod_{j=1}^{n} \sum_{i} a_{i,j} x_i = g(y),
\]
where \( g(y) \) is a homogeneous polynomial with integral coefficients, of degree \( m \), may be solved by means of Theorem 5:1.
This equation may, however, be solved by an entirely different method. The method will be illustrated by solving a more general problem.

Let \( P(x) = \sum_{k} \prod_{j} a_{i,j,k} x_j \), where \( a_{i,j,k} \) are integers and the determinant \( A_k \), for each \( k \), of the forms \( \prod_{j} a_{i,j,k} x_j \) is not zero. Without loss of generality, the notation may be chosen so that \( A_{n,n,k} \neq 0 \), where \( A_{i,j,k} \) is the cofactor of \( a_{i,j,k} \) in \( A_k \). Let \( A^{(t)}_{n,n,k} \) be the determinant obtained from \( A_{n,n,k} \) by replacing the \( j \)th column by \( a_{i,j,k} \), \( d_{i,k} \), \ldots, \( d_{n-1,k} \); \( R \) the least common multiple of \( A^{(t)}_{n,n,k} \) for each \( k \), and \( R_k = R/A_{n,n,k} \).

**Theorem 5:3.** The equation
\[
(5:10) \quad P(x) = g(y),
\]
where \( g(y) \) is a homogeneous polynomial with integral coefficients, of degree \( m \), has solutions and every solution which is not also a solution of
\[
(5:11) \quad \sum_{k} \prod_{j} a_{i,j,k} x_j R_k x_{n,k} A_k = 0,
\]
is equivalent to one of the solutions given by
\[
(5:12) \quad \begin{align*}
x_{j,k} &= t^j R^{j-1} R_k A_{n,n,k}^{(j)} + s t^{j-1} R^{j-1} R_k \beta_{k,j,k}, \\
y_j &= \delta_j t^j R^j,
\end{align*}
\]
where
and the $\alpha^i$, $\beta^i$, and $y^i$ are arbitrary integers, $\lambda$, $\mu$, are relatively prime positive integers such that $\lambda n = \mu m$.

Proof. Let
\begin{equation}
(5:14) \quad \sum_{j} a_{ij,k} x_{j,k} = t^R \beta_k \lambda \quad (1 = 1, \ldots, n - 1)
\end{equation}
and set
\begin{equation}
(5:15) \quad x_{n,k} = st_{-1}^R \lambda \beta_k. \quad (k = 1, \ldots, p)
\end{equation}
Now write (5:14) as
\begin{equation}
(5:16) \quad \sum_{j} a_{ij,k} x_{j,k} = t^R \lambda \alpha_{ij,k} - st_{-1}^R \lambda \beta_k \alpha_{ij,k}. \quad (1 = 1, \ldots, n - 1)
\end{equation}
Solving (5:16) gives
\begin{equation}
(5:17) \quad x_{j,k} = t^R \lambda \alpha_{ij,k} + st_{-1}^R \lambda \beta_k \alpha_{ij,k}
\end{equation}
and hence
\begin{equation}
(5:18) \quad \sum_{j} a_{ij,k} x_{j,k} = t^R \lambda \alpha_{ij,k} + st_{-1}^R \lambda \beta_k \alpha_{ij,k}.
\end{equation}

If $y_j = t^R \lambda \beta_j$, then by use of (5:14) and (5:18), (5:10) becomes
\begin{equation}
(t^R)^{-1} R_{n,k} \sum_{n,k} \left[ \sum_{j} a_{ij,k} A^{(i)}_{n,n,k} + s \beta_k A_{n,k} \right] = t^R \lambda \beta_k \lambda \beta_k
\end{equation}
which is identically satisfied in the $\alpha^i$, $\beta^i$, and $y^i$ if $\lambda$ and $t$ are given by (5:13). Hence (5:12) is a solution of (5:10).

Suppose now that $x_{j,k} = \beta_k$, $y_j = \lambda$ is a given solution of (5:10). Choose $\alpha_{ij,k} = \sum_{n} a_{ij,k} \beta_k$, $\beta_k = \beta_k$, $y_j = \lambda$ then
\begin{itemize}
\item[18/]
$A^{(i)}_{n,n,k}$ becomes $\beta_k A_{n,k} - f_{n,k} A_{n,k}$ when $\alpha_{ij,k}$ is replaced by $\sum_{j} a_{ij,k} \beta_k$.
\end{itemize}

\begin{align*}
\sum_{k} \beta_k A_{n,k} - f_{n,k} A_{n,k} &= \sum_{j} \beta_k A_{n,k} - f_{n,k} A_{n,k} \quad (k = 1, \ldots, p) \\
&= \sum_{k} \sum_{j} a_{ij,k} \beta_k A_{n,k} - f_{n,k} A_{n,k} \\
&= \sum_{k} \left[ \sum_{j} a_{ij,k} \beta_k A_{n,k} - f_{n,k} A_{n,k} \right] R_{k} \sum_{n} a_{ij,k} (\beta_k A_{n,k} - f_{n,k} A_{n,k})
\end{align*}
Let \( f(x,y) = f(x_1, \ldots, x_n; y_1, \ldots, y_m) \), \( g(x,y) = g(x_1, \ldots, x_n; y_1, \ldots, y_m) \) be polynomials with integral coefficients, homogeneous in both \( x \) and \( y \). Suppose that \( f(x,y) \) is of degree \( m \) in \( x \), \( q \) in \( y \), and \( g(x,y) \) is of degree \( n \) in \( x \) and \( p \) in \( y \), where \( m, n, p, q \) are positive integers and \( m - n > 0 \) is relatively prime to \( p - q > 0 \). Since \( m - n \) and \( p - q \) are relatively prime, there exist non-negative integers \( u, v \), \( u \leq p - q, v \leq m - n \), such that \( (m - n)u = (p - q)v + 1 \) and \( (m - n)(p - q - u) = (p - q)(m - n - v) - 1 \).

Theorem 5:4. The equation

\[
(x_j, y_j) = t^a R^b, \quad y_j = T t^c R^d,
\]

which is equivalent to the given solution provided \( x_{j_k} = f_k \), \( y_j = T \) is not also a solution of (5:11).

Let \( f(x,y) = f(x_1, \ldots, x_n; y_1, \ldots, y_m) \) and \( g(x,y) = g(x_1, \ldots, x_n; y_1, \ldots, y_m) \) be polynomials with integral coefficients, homogeneous in both \( x \) and \( y \). Suppose that \( f(x,y) \) is of degree \( m \) in \( x \), \( q \) in \( y \), and \( g(x,y) \) is of degree \( n \) in \( x \) and \( p \) in \( y \), where \( m, n, p, q \) are positive integers and \( m - n \) is relatively prime to \( p - q > 0 \). Since \( m - n \) and \( p - q \) are relatively prime, there exist non-negative integers \( u, v \), \( u \leq p - q, v \leq m - n \), such that \( (m - n)u = (p - q)v + 1 \) and \( (m - n)(p - q - u) = (p - q)(m - n - v) - 1 \).
where \( \alpha_i \), \( \beta_j \) are arbitrary integers.

Proof. Let \( x_i = \alpha_i s^t \), \( y_j = \beta_j s^t \). Then (5:20) becomes

\[
f(\alpha, \beta) = s^{m-n} t^{(m-n)u+p(m-n-v)} g(\alpha, \beta),
\]
which is satisfied identically in the \( \alpha_i \) and \( \beta_j \) if \( s = g(\alpha, \beta) \), \( t = f(\alpha, \beta) \). Hence (5:21) is a solution of (5:20).

If \( x_i = \lambda_i \), \( y_j = \mu_j \) is a given solution of (5:20) then \( f(\lambda, \mu) = g(\lambda, \mu) \). If \( \alpha_i = \lambda_i \), \( \beta_j = \mu_j \) then \( x_i = \lambda_i [f(\lambda, \mu)]^{m-n} \), \( y_j = \mu_j [f(\lambda, \mu)]^{m-n} \), which is equivalent to the given solution provided \( f(\lambda, \mu) \neq 0 \).

The proof of Theorem 5:4 is the same if \( m - n < 0 \) and \( p - q < 0 \). The method does not apply, however, in the cases \( m - n > 0 \), \( p - q < 0 \) and \( m - n < 0 \), \( p - q > 0 \).

Suppose now that for the functions \( f \) and \( g \) considered above, \( f \) is of degree \( m \) in \( x \), \( - p \) in \( y \); \( g \) is of degree \( n \) in \( x \), \( - q \) in \( y \), \( m, n, p, q \), are positive integers and \( m - n > 0 \) is relatively prime to \( p - q > 0 \). As before, non-negative integers \( u, v \) exist such that \( (m - n)u = (p - q)v + 1 \) and \( (m - n)(p - q - u) = (p - q)(m - n - v) - 1 \).

Theorem 5:5. The equation

\[
f(x, y) = g(x, y)
\]

has solutions and every solution for which the members of (5:22) do not vanish is equivalent to a solution given by

\[
x_i = \alpha_i [A(\beta) B(\beta)]^{m-n} [g(\alpha, \beta)]^{m-n} [f(\alpha, \beta)]^{m-n},
\]
\[
y_j = \beta_j [A(\beta) B(\beta)]^{m-n} [g(\alpha, \beta)]^{m-n} [f(\alpha, \beta)]^{m-n},
\]

where \( A(\beta) = \prod \beta_j^{j} \), \( B(\beta) = \prod \beta_j^{j} \) and the \( \alpha_i \) and \( \beta_j \) are...
arbitrary integers.

Proof. If (5:22) is multiplied by \(A(y)B(y)\) it becomes

\[
(5:24) \quad A(y)B(y)f(x,y) = A(y)B(y)g(x,y),
\]
each member of which is a polynomial with integral coefficients.

If \(x_i = \alpha_i \cdot s^t t^{m-n}y, \ y_j = \beta_j \cdot s^r t^{m-n}y\), then on substituting in (5:24) it follows that

\[
\begin{align*}
A(\beta)B(\beta)f(\alpha, \beta) &= A(\beta)B(\beta)g(\alpha, \beta), \\
A(\beta)B(\beta)g(\alpha, \beta) &= A(\beta)B(\beta)f(\alpha, \beta),
\end{align*}
\]
which is satisfied identically in the \(\alpha_i\) and \(\beta_i\) if

\[
s = A(\beta)B(\beta)g(\alpha, \beta), \quad t = A(\beta)B(\beta)f(\alpha, \beta).
\]

Hence (5:23) is a solution of (5:22).

If \(x_i = \lambda_i, \ y_j = \mu_j\) is a given solution of (5:22) then

\[
f(\lambda, \mu) = g(\lambda, \mu).
\]

If \(\lambda_i = \lambda_i, \ \beta_j = \mu_j\); the solution becomes

\[
x_i = \lambda_i [A(\mu)B(\mu)f(\lambda, \mu)]^{p-q}, \quad y_j = \mu_j [A(\mu)B(\mu)g(\lambda, \mu)]^{m-n},
\]
which is equivalent to the given solution provided \(f(\lambda, \mu) \neq 0\).

It is necessary that \(\mu_j \neq 0\).

It will be noted that if in Theorem 5:5, \(m - n > 0\) and \(p - q < 0\), then \(u, v\) may be chosen as positive integers such that \((m - n)u = (q - p)v + 1\) and \((m - n)(q - p - u) = (q - p)(m - n - v) - 1\) and the solution in this case is

\[
x_i = \lambda_i [A(\beta)B(\beta)]^{m-n} [f(\alpha, \beta)]^{p-q}, \quad y_j = \mu_j [A(\beta)B(\beta)]^{m-n} [g(\alpha, \beta)]^{m-n}.
\]

If in Theorem 5:4 \(f\) is of degree \(-m\) in \(x\), \(-q\) in \(y\) and \(g\) is of degree \(-n\) in \(x\) and \(-p\) in \(y\) the solution is

\[
x_i = \alpha_i [A(\beta)B(\beta)C(\alpha)D(\alpha)]^{m-n} [f(\delta, \beta)]^{p-q}, \quad y_j = \beta_j [A(\beta)B(\beta)C(\alpha)D(\alpha)]^{m-n} [g(\alpha, \beta)]^{m-n},
\]
where \(C(\alpha) = \prod \alpha_i^m\), \(D(\alpha) = \prod \alpha_j^m\).
The above methods may be extended to solve certain types of non-homogeneous equations, as is illustrated in the next theorem.

**Theorem 5.6.** The equation

\[(5:25) \quad f(x,y) = g(x,y),\]

where \(f(x,y) = \sum a_i \prod x_i^{\alpha_{ij}} y_i^{\beta_{ij}}, \quad g(x,y) = \sum b_i \prod x_i^{\gamma_{ij}} y_i^{\delta_{ij}}, \quad a_i, \quad b_i \) are integers, \(\alpha_{ij}, \beta_{ij}, \gamma_{ij}, \delta_{ij}\) being positive integers, has solutions if there exists positive integers \(u_i, v_i, w_i, z_i, M, N\) such that

\[
\sum a_i \prod x_i^{u_i} y_i^{v_i} = M, \\
\sum b_i \prod x_i^{z_i} y_i^{v_i} = M + 1, \\
\sum a_i \prod x_i^{u_i} y_i^{w_i} = N, \\
\sum b_i \prod x_i^{z_i} y_i^{w_i} = N + 1,
\]

and every solution for which the members of (5:25) do not vanish, is equivalent to one of the solutions given by

\[(5:26) \quad x_i = \alpha_i s^\xi t^\eta, \quad y_i = \beta_i s^\xi t^\eta,
\]

where

\[(5:27) \quad s = f(\alpha, \beta), \quad t = g(\alpha, \beta),\]

and the \(\alpha_i\)s and \(\beta_i\)s are arbitrary integers.

**Proof.** If \(x_i, y_i\) have the values given by (5:27) then by (5:26), (5:25) becomes \(s^m t^n f(\alpha, \beta) = s^{m+1} t^n g(\alpha, \beta),\)

which is satisfied identically in the \(\alpha_i\)s and \(\beta_i\)s if \(s\) and \(t\) are given by (5:28).

If (5:26) is satisfied, there exist non-negative integers \(K, u_i^1, v_i^1\) such that

\[
\sum a_i \prod x_i^{u_i} y_i^{v_i} = K, \quad (i = 1, \ldots, m), \\
\sum b_i \prod x_i^{z_i} y_i^{v_i} = K, \quad (h = 1, \ldots, p).
\]

If \(a_i = \lambda_, \quad y_i = \mu,\) is any integral solution of (5:25) and
there are no integers \( u^i, w^i \) satisfying (5:29), \( d > 1 \), and
\( \lambda_i, \mu_i \) such that \( \lambda_i = \lambda^i d^u^i, \mu_i = \mu^i d^w^i \), then \( x_i = \lambda_i, y_i = \mu_i \), is said to be a primitive solution of (5:25).

If \( x_i = \lambda_i, y_i = \mu_i \) is a primitive solution of (5:25), then
\( x_i = \lambda^i d^u^i, y_i = \mu^i d^w^i, \) derived from the primitive solution,
where \( d \neq 0 \) is an integer and \( u^i, w^i \) are non-negative integers satisfying (5:29), is also a solution. Two solutions are said to be equivalent if they may be derived from the same primitive solution.

With this definition we may show that for any solution of (5:25) for which the members do not vanish, an equivalent solution is given by (5:27).

If \( x_i = \lambda_i, y_i = \mu_i \) is any given solution of (5:25) and the choice \( x_i = \lambda_i, \beta_i = \mu_i \) is made then
\[
(5:30) \quad x_i = \lambda_i \left[f(\lambda, \mu)\right]^{u^i + w^i}, \quad y_i = \mu_i \left[f(\lambda, \mu)\right]^{w^i + x^i}.
\]

Since
\[
\sum \left[ \alpha_{ij} (u_j + v_j) + \beta_{ij} (z_j + w_j) \right] = \sum \left[ \alpha_{ij} (u_j + v_j) + \delta_{ij} (z_j + w_j) \right] = M + N + 1,
\]
the solution is equivalent to the given solution if \( f(\lambda, \mu) \neq 0 \).

Theorem 5:6 may be extended, as was Theorem 5:4, to cover equations in which the members are no longer polynomials. The method will be illustrated by a particular example.

Consider
\[
\frac{ax^i u^i}{v^i} + \frac{by^i v^i}{u^i} = \frac{cx^i}{w^i}
\]
which may be written as
\[
a x^i u^i w + b y^i v^i w = c x^i u^i v^7.
\]
The solution of this equation is \( x = \alpha s^t, y = \beta s^t, u = \lambda s^t, v = \mu s^t, w = \sqrt{s} t^t \) where \( s = a \alpha + b \beta + c \lambda + \sqrt{d} \mu \), \( t = 0 \alpha + \lambda \mu \). It is necessary that \( u, v, \) and \( w \) be different from zero.

If \( x = x', y = y', u = u', v = v', w = w' \) is a solution of the above equation and the choice \( \alpha = x', \beta = y', \lambda = u', \mu = v', \sqrt{s} = w' \) is made then \( s = t \) and the solution becomes \( x = x't', y = y't', u = u't', v = v't', w = w't' \) which, by a natural extension of the definition of equivalence, is equivalent to the given solution.

Two final theorems will now be proved. Both of these theorems are included in the above theory, but because of their interest they will be solved in detail.

Theorem 5:7. The equation

\[
\sum_{i} \frac{a_i}{x_i} = \frac{0}{y_k}
\]

where all the letters represent integers \( x_i \), \( y_k \) are unknown, has integral solutions and every solution is equivalent to one of the solutions given by

\[
x = a_i C(\alpha) B(\beta), \quad y_k = 0 \frac{d_k}{A_i} \sum_{i} a_i A_i(\alpha) B(\beta)
\]

where \( A_i(\alpha) = \frac{d_i}{a_i} a_i, B_i(\alpha) = \sum d_i A_i(\alpha), B(\alpha) = \frac{d_i}{a_i} B_i(\alpha), C(\beta) = \frac{d_k}{a_i} \beta_k, D(\beta) = \frac{d_k}{a_i} C(\beta), \) and \( a, \beta, (\neq 0) \) are
arbitrary integers.

Proof. Equation (5:31) may be written in the form

\[(5:33) \quad D(y) \sum_{j} \frac{a_j A_j(x) B(x)}{B_j(x)} = cC(y)B(x).\]

If \(x_{ij} = \lambda_{ij}, y_j = \mu_j\) be any solution of (5:31). Let \(x_{ij} = \lambda_{ij}, y_j = \mu_j\) be any solution of (5:31). If

\[a \cdot c = 1, a = a_1 = \ldots = 0 (5:31) \text{ reduces to} 22/\]

22/ Leonard E. Dickson, op. cit., pp. 688 - 691.

\[\sum_{i} \frac{b_{ij}}{x_{ij}} = \sum_{x_{ij}} \frac{c_j}{y_{ij}}.\]

Theorem 5:8. The equation 23/


\[(5:34) \quad f(x) = g(y),\]

where \(f(x) = \sum_{j} \frac{a_{ij}}{x_{ij}}, g(y) = \sum_{j} \frac{b_{ij}}{y_{ij}},\) all the letters represent integers, and \(x_{ij}, y_j\) are unknown, has integral solutions and every solution for which the members do not
vanish is equivalent to one of the solutions given by

\[(5:35) \quad x_{ij} = \alpha_{ij} A(\alpha)B(\beta)f(\alpha), \quad y_{ij} = \beta_{ij} A(\alpha)B(\beta)g(\beta)\]

where \(A(\alpha) = \prod^{n}_{i=1} A_{i}(\alpha), B(\beta) = \prod^{m}_{j=1} B_{j}(\beta)\), and \(\alpha_{ij}, \beta_{ij} \neq 0\) are arbitrary integers.

Proof. Equation (5:34) may be written in the equivalent form

\[(5:36) A(x)B(y)f(x) = A(x)B(y)g(y).\]

If \(x_{ij} = \alpha_{ij} t, y_{ij} = \beta_{ij} st^{m-1}\), then (5:36) becomes

\[s^{r} t^{n+1(m-1)} A(\alpha)B(\beta)f(\alpha) = s^{r} t^{n+1(m-1)} A(\alpha)B(\beta)g(\beta),\]

which is satisfied identically in the \(\alpha's\) and \(\beta's\) if

\[s = A(\alpha)B(\beta)g(\beta), t = A(\alpha)B(\beta)f(\alpha).\]

Hence a solution of (5:34) is given by (5:35).

If \(x_{ij} = \lambda_{ij}, y_{ij} = \mu_{ij}\) is a solution of (5:34) and the choice \(\alpha_{ij} = \lambda_{ij}, \beta_{ij} = \mu_{ij}\), is made, \(s = t\) and the solution becomes \(x_{ij} = \lambda_{ij} t, y_{ij} = \mu_{ij} t^{m}\) which is equivalent to the given solution provided \(t \neq 0\). But since \(\lambda_{ij}, \mu_{ij} \neq 0\), \(t = A(\lambda)B(\mu)f(\lambda) = 0\) if and only if \(f(\lambda) = 0\).
BIBLIOGRAPHY

A. A. Aucoin, "A Note on a Diophantine Equation", National Mathematics Magazine (To be published later).

A. A. Aucoin, "Diophantine Equations of Degree n", Bulletin of the American Mathematical Society (To be published later).


A. A. Aucoin, "Solution of a Diophantine Equation", Boletin Matematico, XII: 45-46, April, 1939.


Volume II of Dickson's History of the Theory of Numbers is a comprehensive listing of all the important results and methods in Diophantine analysis up to its time of publication.
BIOGRAPHY

The author was born on May 14, 1910 in Houston, Texas. He received his primary education from the parochial schools of Houston, Texas and was graduated in 1930 from San Jacinto High School of that city. He matriculated at Rice Institute in 1930, graduating, with honors in mathematics, in 1934. In 1936 he received the M. A. degree in mathematics from Rice Institute. In 1936 he entered Louisiana State University, where he is at present enrolled.
EXAMINATION AND THESIS REPORT

Candidate: Anthony Andrew Aucoin

Major Field: Mathematics

Title of Thesis: An Algebraic Treatment of Diophantine Analysis

Approved:

W. V. Parker
Major Professor and Chairman

Charles W. Bax
Dean of the Graduate School

EXAMINING COMMITTEE:

Robert A. Goss

R. C. Reid

R. L. O'Driscoll

J. A. Nethercot

S. W. Rickey

S. T. Sanders

Date of Examination: May 9, 1940