AMERICAN UNIVERSITY OF BEIRUT

ON DIOPHANTINE EQUATIONS DEFINING EQUIVALENCE RELATIONS

By

Elie Dik

Approved:

Amin Muwafi
Advisor

David Singmaster
Member of Committee

[illegible]
Member of Committee

Member of Committee

Date of Thesis Presentation : ____________________

ON DIOPHANTINE EQUATIONS DEFINING EQUIVALENCE RELATIONS

By

Elie Dik

Submitted in Partial Fulfillment for the Requirements

of the Degree Master of Sciences

in the Mathematics Department of the

American University of Beirut

Beirut, Lebanon

1968

ON DIOPHANTINE EQUATIONS DEFINING EQUIVALENCE RELATIONS

By

Elie Dik

CONTENTS

NOTATION AND CONVENTIONS

The symbol I will denote the set of all integers, and the set $I - \{0\}$ will be denoted by Z.

$a|b$ means that a divides b.

The greatest common divisor of two integers a and b is denoted by (a,b).

Unless otherwise specified all symbols used represent integers. If A is a subset of I, then $-A = \{-n : n \in A\}$.

ABSTRACT

The thesis is mainly concerned with the discussion of Diophantine equations of the form $P(x, y) = \emptyset(z)$ that define a binary relation, R, over S, a subset of the integers. We say that aRb if and only if there exists an integer $c \in S$ such that $P(a, b) = \emptyset(c)$ where $a, b \in S$. If R is an equivalence relation, the equation is said to define an equivalence relation.

We determine equations that define equivalence relations, and we characterize the equivalence classes associated with these equations. In Chapters II and III equations, of degree $n \leq 3$, satisfying the reflexive and symmetric properties, are discussed. Some of the results obtained are then generalized to equations of arbitrary degree.

Determining the equivalence classes, in general, is a difficult task. In Chapter IV we obtain an inequality satisfied by N(R), the number of equivalence classes, for equations of the form $P(x, y) = mz$.

CHAPTER I

INTRODUCTION

Basic Definitions:

A Diophantine equation is one of the form $P(x,y,z,\ldots,u) = 0$, where $P(x,y,z,\ldots,u)$ is an integral polynomial in the variables $x,y,z,\ldots,u$. Moreover we assume that the variables have integral values only.

Definition 1.1: A binary relation R defined over a set A is said to be an equivalence relation if and only if the following three conditions are satisfied for all a, b, and c in A:

(i) $a R a$ (Reflexive property)

(ii) If aRb, then bRa. (Symmetric property)

(iii) If aRb, and bRc, then aRc. (Transitive property)

In case a is not related to b we write $a \not R b$.

Definition 1.2: If R is an equivalence relation defined over a set A, then a subset B of A is called an equivalence class if and only if the following two conditions are satisfied:

(i) xRy for all $x, y \in B$. , and

(ii) If $x \in A$, $y \in B$, and xRy, then $x \in B$.

Definition 1.3: An equivalence relation over a set A is called a universal equivalence relation over A if and only if xRy for all $x, y \in A$.

Definition 1.4: For a relation R defined over a set A, N(R) denotes the number (or cardinality) of the set of distinct equivalence classes determined by R. If R is not an equivalence relation, N(R) = 0.

An equivalence class B is denoted by $[b]_R$, where $b \in B$. In general, the element b has certain properties, and is referred to as the representative of the equivalence class.

In this work binary relations are defined over the ring of integers. Unless otherwise specified, the representative is the smallest non-negative integer in the equivalence class. If the equivalence class consists of negative integers only, we take the smallest in absolute value as the representative.

Preliminary results:

1a: $b \in [a]_R$ if and only if $[b]_R = [a]_R$.

1b: $[a]_R = [b]_R$ if and only if aRb.

1c: $[a]_R \cap [b]_R = \emptyset$ if and only if $a \not R b$.

1d: If $[a]_R \cap [b]_R \neq \emptyset$, then $[a]_R = [b]_R$.

Statement of the Problem:

Let $\emptyset(z)$ and $P(x,y)$ be two integral polynomials in one and two variables respectively. We define a binary relation R over a subset A of I as follows: xRy if and only if there exists an integer $z \in A$ such that:

$$P(x,y) = \emptyset(z) \quad \text{.............................} \quad (1.1)$$

In this paper we consider Diophantine equations of the form (1.1) that satisfy the following conditions:

$$\text{For all } x \in I,\ P(x,x) = \phi(x) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (I)$$

$$\text{For all } x,\ y,\ z \in I, \text{ if } P(x,y) = \phi(z), \text{ then } P(y,x) = \phi(z) \ldots \quad (II).$$

The first condition ensures the reflexive property of R and the second ensures its symmetric property. We are interested in the case when R is an equivalence relation. Thus the only property to be considered is transitivity.

<u>Definition 1.5</u>: If $P(x,y) = \phi(z)$ satisfies the reflexive, symmetric, and transitive properties we say that the equation defines an equivalence relation.

<u>Definition 1.6</u>: Two equations are equivalent if and only if they define an equivalence relation and have the same equivalence classes.

L. M. Chawla ([1] and [2]) discussed some equations of the form (1.1), of degree $n \leq 3$, that satisfy conditions (I) and (II).

In this paper we investigate more equations, answer some of the questions raised by Chawla, and generalize certain results.

CHAPTER II

FIRST AND SECOND DEGREE EQUATIONS DEFINING EQUIVALENCE RELATIONS

The general Diophantine equation of degree equal to or less than two, and of the form

$$P(x,y) = \emptyset (z)$$

is

$$a_1x^2 + a_2x + a_3xy + a_4y^2 + a_5y = b_1z^2 + b_2z + b_2 \quad \ldots\ldots\ldots \quad (2.1)$$

If conditions (I) and (II), referred to in Chapter I, are satisfied, then:

$$\left.\begin{aligned} a_1 + a_3 + a_4 &= b_1 \\ a_2 + a_5 &= b_2 \\ 0 &= b_3 \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.2)$$

and

$$\left.\begin{aligned} a_1 &= a_4 \\ a_2 &= a_5 \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.3)$$

The sets of equations (2.2) and (2.3) imply that:

$$\left.\begin{aligned} 2a_1 + a_3 &= b_1 \\ 2a_2 &= b_2 \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.4)$$

Thus the general form of equation (2.1) reduces to:

$$a_1(x^2+y^2)+a_2(x+y)+a_3xy = (2a_1+a_3)z^2+2a_2z \quad \ldots\ldots\ldots\ldots \quad (2.5)$$

Altogether eight different cases of the above equation arise depending on the values of the coefficients. They are listed in table 2.1.

Table 2.1: Equations of degree $n \leq 2$ satisfying conditions (I) and II).

a_1	a_2	a_3	$2a_1+a_3$	$2a_2$
0	a_2	0	0	$2a_2$
0	0	a_3	a_3	0
0	a_2	a_3	a_3	$2a_2$
a_1	a_2	0	$2a_1$	$2a_2$
a_1	0	0	$2a_1$	0
a_1	0	a_3	$2a_1+a_3$	0
a_1	a_2	$-2a_1$	0	$2a_2$
a_1	a_2	a_3	$2a_1+a_3$	$2a_2$

Theorem 2.1: The equation

$$x+y = 2z \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.6)$$

defines an equivalence relation over I. The equivalence classes are given by: $[0]_R = \{2n : n \in I\}$, and $[1]_R = \{2n+1 : n \in I\}$.

<u>Proof</u>: Let $A_0 = \{2n : n \in I\}$ and $A_1 = \{2n+1 : n \in I\}$. First, we show that if $x, y \in A_i$, $i = 0$, or 1, then xRy.

If $i = 0$, then $x = 2n_1$ and $y = 2n_2$. Hence $x + y = 2n_1 + 2n_2 = 2(n_1 + n_2)$. Thus we take $z = n_1 + n_2$ and xRy.

If $i = 1$, then $x = 2n_1 + 1$ and $y = 2n_2 + 1$. Hence $x + y = 2n_1 + 1 + 2n_2 + 1 = 2(n_1 + n_2 + 1)$. Thus we take $z = n_1 + n_2 + 1$, and xRy.

Now, we show that if $x \in A_0$ and $y \in A_1$, then $x \not R y$. Let $x = 2n_1$ and $y = 2n_2 + 1$. Hence $x + y = 2n_1 + 2n_2 + 1 = 2(n_1 + n_2) + 1 \not\equiv 0 (\text{mod } 2)$, and $x \not R y$.

Similarly, if $x \in A_1$ and $y \in A_0$, then $x \not R y$.

Thus xRy if and only if both x and y belong to the same set A_i, $i = 0$, or 1.

To establish transitivity, let aRb and bRc. Using the above result we see that a, b, and c belong to the same set A_k; consequently, aRc.

The two sets A_0 and A_1 satisfy the two conditions of definition 1.2 It follows they are equivalence classes.

To prove the next theorem we need the following definition and lemma:

<u>Definition 2.1</u>: P denotes the set consisting of the integer 1 together with all integers J, expressible in the form:

$J = p_1 p_2 \dots p_k$, where $p_1, p_2, \dots, p_k$ are different primes.

<u>Lemma 2.1</u>: Every positive integer a is uniquely expressible in the form:

$$a = Jn^2, \text{ where } J \in P.$$

Proof: By the unique factorization theorem, we can write:

$$a = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}, \quad \text{where } p_1, p_2, \dots, p_m$$

are different primes.

If all of the exponents were even, then

$$a = Jn^2, \quad \text{where } J = 1 \text{ and } n = p_1^{\frac{e_1}{2}} p_2^{\frac{e_2}{2}} \dots p_m^{\frac{e_m}{2}}.$$

If some of the exponents $e_1, e_2, \dots, e_m$ were odd, then rearrange the prime in the canonical representation of a such that $e_1, e_2, \dots, e_k$ denote the odd exponents.

a is now expressed as:

$$a = \left[p_1 p_2 \dots p_k \, p_1^{e_1-1} p_2^{e_2-1} \dots p_k^{e_k-1}\right] p_{k+1}^{e_{k+1}} \dots p_m^{e_m}.$$

So that:

$$a = (p_1 p_2 \dots p_k) \left[p_1^{\frac{e_1-1}{2}} p_2^{\frac{e_2-1}{2}} \dots p_k^{\frac{e_k-1}{2}} \cdot p_{k+1}^{\frac{e_{k+1}}{2}} \dots p_m^{\frac{e_m}{2}}\right]^2$$

$$= Jn^2.$$

The uniquesof this representation follows from the unique factorization theorem.

Theorem 2.2: The equation

$$xy = z^2 \quad \dots\dots\dots\dots\dots\dots \quad (2.7)$$

defines an equivalence relation over Z. The equivalence classes are given by:

$$[J]_R = \{Jn^2 : n \in Z\}, \quad \text{where } J \in P, \text{ or } J \in -P.$$

The equation does not define an equivalence relation over I.

<u>Proof</u>: To establish transitivity, let aRb and bRc, where $a, b, c \in Z$. Then $ab = z_1^2$, for some $z_1 \in Z$, and $bc = z_2^2$, for some $z_2 \in Z$. Hence $ac = (\frac{z_1 z_2}{b})^2 = z_3^2$, where $z_3 = \frac{z_1 z_2}{b} \in Z$. Thus aRc.

We proceed now to show that the above listed classes arw really equivalence classes. Let

$$A_J = \{Jn^2 : n \in Z\}, \ J \in P, \ \text{or} \ J \in -P.$$

Let $x, y \in A_J$, then $x = Jn_1^2$, for some $n_1 \in Z$, and $y = Jn_2^2$, for some $n_2 \in Z$. Hence $xy = (Jn_1^2)(Jn_2^2) = (J.n_1 n_2)^2 = z^2$, where $z = J.n_1 .n_2 \in Z$, and xRy.

Let $x \in A_{J_1}$, and $y \in A_{J_2}$, and let xRy. Thus we have $x = J_1 n_1^2$, $y = J_2 n_2^2$, and $xy = J_1 J_2 (n_1 n_2)^2 = z^2$, for some $z \in Z$. This implies that $J_1 J_2$ is a perfect square.

Noting that, if $J_1, J_2 \in P$ (or $J_1, J_2 \in -P$) and $J_1 . J_2$ is a perfect square then $J_1 = J_2$; it follows that $A_{J_1} = A_{J_2}$. It follows $A_{J_1} = A_{J_2}$.

By lemma 2.1 any positive integer a belongs to one and only one class $[J]_R$, where $J \in P$. Similarly, any negative integer belongs to one and only one class $[J]_R$, where $J \in -P$. Hence

$$Z = \bigcup_{\substack{J \in P \\ \text{or } J \in -P}} A_J .$$

Thus for all $x, y \in Z$, xRy if and only if $x, y \in A_J$.

To show that equation (2.7) does not define an equivalence relation over I, let $x_1 = 5$, $x_2 = 0$, and $x_3 = 2$. $x_1 R x_2$, since $5.0 = 0 = 0^2$; and $x_2 R x_3$, since $0.2 = 0 = 0^2$. But $x_1 \not R x_3$, because

$5.2 \neq z^2$, for all $z \in I$.

<u>Theorem 2.3</u>: The equation

$$a_2(x + y) + a_3xy = a_3z^2 + 2a_2z \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.8)$$

defines an equivalence relation over:

(i) $I - \left\{ -\frac{a_2}{a_3} \right\}$, if $a_3 \mid a_2$.

The equivalence classes are given by:

$$\left[J - a_2\right]_R = \left\{ Jn^2 - a_2 : n \in Z \right\}, \text{ where } J \in P, \text{ or } J \in -P.$$

(ii) I, if $a_3 \nmid a_2$.

<u>Proof</u>: Assume that a_2 and a_3 are relatively prime, because we can divide both sides of the equation by their greatest common divisor.

<u>Case (i)</u>: If $a_3 \mid a_2$, then $a_3 = \mp 1$. We consider the case when $a_3 = 1$, the other case is treated similarly. Equation (2.8) reduces to:

$$XY = Z^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.8a)$$

where $X = x + a_2$, $Y = y + a_2$, and $Z = z + a_2$.

Equation (2.8a) defines an equivalence relation over Z, where X, Y, and Z are not allowed the value zero; that is, x and y are not allowed the value $-a_2$.

Using theorem (2.2), the equivalence classes are those listed above.

<u>Case (ii)</u>: If $a_3 \nmid a_2$, multiply equation (2.8) by a_3 and add a_2^2 to both sides. The equation reduces to:

$$(a_3x + a_2)(a_3y + a_2) = (a_3z + a_2)^2 \quad \ldots\ldots\ldots\ldots \quad (2.8b)$$

Let aRb and bRc, then

$$(a_3a + a_2)(a_3b + a_2) = (a_3z_1 + a_2)^2, \text{ for some } z_1 \in I$$

and

$$(a_3b + a_2)(a_3c + a_2) = (a_3z_2 + a_2)^2, \text{ for some } z_2 \in I.$$

Hence we have:

$$(a_3a + a_2)(a_3c + a_2) = \left[\frac{(a_3z_1 + a_2)(a_3z_2 + a_2)}{(a_3b + a_2)}\right]^2 = q^2$$

where

$$q = \frac{(a_3z_1 + a_2)(a_3z_2 + a_2)}{(a_3b + a_2)} \in I.$$

Let $q \equiv r(\text{mod } a_3)$, where $0 \leq r < a_3$. Then $q \equiv a_3m + r$, for some $m \in I$. Hence

$$(a_3b + a_2)(a_3m + r) = (a_3z_1 + a_2)(a_3z_2 + a_2)$$

or

$$a_3^2(bm - z_1z_2) + a_3br + a_2a_3m - a_2a_3m - a_2a_3(z_1 + z_2) =$$

$$a_2(a_2 - r) \text{ .... } (2.9)$$

Since $(a_2, a_3) = 1$ and a_3 is a divisor of the left hand side of equation (2.9), then $a_3 \mid (a_2 - r)$. Thus $a_2 - r = a_3k$, for some $k \in I$, and $q = a_3m + r = a_3m + a_2 - a_3k = a_3(m - k) + a_2$. If we let $z_3 = m - k$, then

$$(a_1a + a_2)(a_3c + a_2) = (a_3z_3 + a_2)^2$$

i.e. aRc, which establishes transitivity.

In the equation

$$a_1(x - y)^2 + a_2(x + y) = 2a_2z \text{ .... } (2.10)$$

we assume that $(a_1, a_2) = 1$, and that a_2 is positive.

The following lemmas are needed in the next theorem:

Lemma 2.2: If $x^n \equiv y^n \equiv 0 \pmod{m}$, where m and n are positive integers, then:

$$(ax + by) \equiv 0 \pmod{m}, \text{ for all } a, b \in I.$$

Proof: $x^n \equiv 0 \pmod{m}$ and $y^n \equiv 0 \pmod{m}$ imply that $x^n = q_1 m$ and $y^n = q_2 m$, where $q_1, q_2 \in I$. Therefore,

$$x = (q_1 m)^{\frac{1}{n}} \quad \text{and} \quad y = (q_2 m)^{\frac{1}{n}} .$$

For any integer r, $0 \leq r \leq n$, we have

$$x^{n-r} y^r = \left[(q_1 m)^{\frac{1}{n}}\right]^{n-r} \left[(q_2 m)^{\frac{1}{n}}\right]^r$$

$$= q_1^{\frac{n-r}{n}} \cdot q_2^{\frac{r}{n}} \cdot m \equiv 0 \pmod{m}$$

But

$$(ax + by)^n = \sum_{r=0}^{n} a^{n-r} b^r \binom{n}{r} x^{n-r} y^r$$

$$\equiv 0 \pmod{m}.$$

Lemma 2.3: Let m and n be two positive integers. Let q be the smallest positive integer such that $(qm)^{\frac{1}{n}}$ is an integer, and let $S = \left\{0, 1, 2, \ldots, (qm)^{\frac{1}{n}} - 1\right\}$. Then the only solution of the congruence

$$(x - y)^n \equiv 0 \pmod{m} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.11a)$$

in S is $x = y$.

Proof: $x = y$ is clearly a solution of the congruence (2.11a).

Let now $x \neq y$, with $x, y \in S$, such that $(x - y)^n \equiv 0 (\mathrm{mod}\ m)$. We may assume $x > y$. Hence

$$(x - y) = 1, 2, \ldots, (qm)^{\frac{1}{n}} - 1.$$

Since congruence (2.11a) is satisfied, $(x - y)^n = rm$, for some $r > 0$, and $(x - y) = (rm)^{\frac{1}{n}} \in I$. But

$$rm = (x - y)^n \leq \left[(qm)^{\frac{1}{n}} - 1\right]^n < \left[(qm)^{\frac{1}{n}}\right]^n = qm.$$

Thus we have an integer r smaller than q such that $(rm)^{\frac{1}{n}} \in I$, a contradiction to the hypothesis of the lemma.

<u>Lemma 2.4</u>: Let $a \in I$, then there exists a unique integer $b \in S$, of Lemma 2.2, such that $(a - b)^n \equiv 0 \ (\mathrm{mod}\ m)$.

<u>Proof</u>: For any given integer a, there exists an integer b, $0 \leq b < (qm)^{\frac{1}{n}}$, such that $a \equiv b(\mathrm{mod}\ (qm)^{\frac{1}{n}})$. Thus $a - b \equiv 0(\mathrm{mod}\ (qm)^{\frac{1}{n}})$, and $(a - b)^n \equiv 0(\mathrm{mod}\ qm)$ or $(a - b)^n \equiv 0(\mathrm{mod}\ m)$.

To prove uniqueness, let b_1 and b_2 belong to S such that

$$(a - b_1)^n \equiv 0 \ (\mathrm{mod}\ m) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.11b)$$

and

$$(a - b_2)^n \equiv 0 \ (\mathrm{mod}\ m) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.11c)$$

By lemma (2.2), the congruences (2.11b) and (2.11c) imply that $(b_1 - b_2)^n \equiv 0(\mathrm{mod}\ m)$. Then by lemma (2.3) $b_1 = b_2$.

In the following theorem m and n are any two positive integers. Condition (I) is not satisfied except when $k = 1$. Condition (II) is satisfied when n is even. We assume that a_1 and a_2 are relative prime, and a_2 positive.

<u>Theorem 2.4</u>: For any positive integers m and n, the

equation

$$a_1(x - y)^n + a_2(x + y)^m = 2a_2z \quad \ldots\ldots\ldots\ldots\ldots \quad (2.12)$$

defines an equivalence relation over I such that:

(i) If $a_1 \equiv a_2 \pmod 2$, the equivalence classes are given by:

$$[J]_R = \{n : n \equiv J \pmod{(qa_2)^{\frac{1}{n}}}\},$$

where q is the smallest positive integer such that $(qa_2)^{\frac{1}{n}}$ is an integer, and $J = 0, 1, 2, \ldots, (qa_2)^{\frac{1}{n}} - 1$.

(ii) If $a_1 \not\equiv a_2 \pmod 2$, the equivalence classes are given by:

$$[J]_R = \{n : n = J \pmod{(2qa_2)^{\frac{1}{n}}}\},$$

where q is the smallest positive integer such that $(2qa_2)^{\frac{1}{n}}$ is an integer, and $J = 0, 1, 2, \ldots, (2qa_2)^{\frac{1}{n}} - 1$.

<u>Proof (i)</u>: If $a_1 \equiv a_2 \pmod 2$, then a_1 and a_2 are both even or both odd. The first possibility is ruled out since a_1 and a_2 are assumed to be relatively prime.

Let xRy, then

$$a_1(x - y)^n + a_2(x + y)^m = 2a_1z_1, \text{ for some } z_1 \in I \quad \ldots\ldots \quad (2.12a)$$

We note that the right hand side of equation (2.12a) and the term $a_2(x + y)^m$ are both divisible by a_2. Hence $a_2 \mid a_1(x - y)^n$. But $(a_1, a_2) = 1$, then $(x - y)^n \equiv 0 \pmod{a_2}$.

Conversely, if $(x - y)^n \equiv 0 \pmod{a_2}$, then

$$a_1(x-y)^n + a_2(x+y)^m \equiv 0 \pmod{a_2} \quad \ldots\ldots\ldots\ldots \quad (2.12b)$$

Noting that the left hand side of congruence (2.12b) is even for all x and y, we see that

$$a_1(x - y)^n + a_2(x + y)^m \equiv 0 (\text{mod } 2a_2).$$

or

$$a_1(x - y)^n + a_2(x + y)^m = 2a_2 z_2,$$

for some $z_2 \in I$, and xRy.

Thus for all a_1 and a_2 odd, xRy if and only if $(x - y)^n \equiv 0 \ (\text{mod } a_2)$.

Reflixivity is satisfied since $(x - x)^n \equiv 0(\text{mod } a_2)$.

Symmetry is satisfied since $(x - y)^n \equiv 0 \ (\text{mod } a_2)$ implies $(y - x)^n \equiv 0 \ (\text{mod } a_2)$.

To establish transitivity, let aRb and bRc, we have then

$$(a - b)^n \equiv 0(\text{mod } a_2) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.12c)$$

and

$$(b - c)^n \equiv 0(\text{mod } a_2) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.12c')$$

By lemma 2.2 we have $[(a - b) + (b - c)]^n \equiv 0(\text{mod } a_2)$ or $(a - c)^n \equiv 0(\text{mod } a_2)$, and aRc.

Lemma 2.3 shows that the listed classes are equivalence classes, while lemma 2.4 shows that they are the only ones.

<u>Proof (ii)</u>: If $a_1 \not\equiv a_2 \ (\text{mod } 2)$, then either a_1 is odd and a_2 is even, or a_1 is even and a_2 is odd. In either case we will show that, xRy if and only if $(x - y)^n \equiv 0(\text{mod } 2a_2)$. Using the same reasoning as in part (i), we get the desired result.

Let a_1 be even, a_2 be odd, and let xRy. Then

$$a_1(x - y)^n + a_2(x + y)^m = 2a_2 z_3, \text{ for some } z_3 \in I \ \ldots\ldots \quad (2.12d)$$

Since $a_1(x - y)^n$ and the right hand side of (2.12d) are both even, then $a_2(x+y)^m$ is even; consequently, $x \equiv y \pmod 2$. Furthermore a_2 divides the right hand side of (2.12d) and $a_2(x + y)^m$. Hence $a_1(x - y)^n \equiv 0 \pmod{a_2}$, and $(x - y)^n \equiv 0 \pmod{a_2}$. But $x \equiv y \pmod 2$, therefore, $(x - y)^n \equiv 0 \pmod{2a_2}$.

Conversely, if $(x - y)^n \equiv 0 \pmod{2a_2}$, then $x \equiv y \pmod 2$ and $a_1(x - y)^n + a_2(x + y)^m \equiv 0 \pmod{2a_2}$; that is $a_1(x - y)^n + a_2(x+y)^m = 2a_2z_4$, for some $z_4 \in I$, and xRy.

Let a_1 be odd, a_2 be even, and let xRy. Then

$$a_1(x - y)^n + a_2(x+y)^m = 2a_2z_5, \text{ for some } z_5 \in I \quad \ldots\ldots\ldots \quad (2.12e)$$

Since $a_2(x + y)^m$ and $2a_2z_5$ are even, then $a_1(x - y)^n$ is even; consequently, $x \equiv y \pmod 2$. Furthermore $a_2 \mid a_1(x - y)^n$. Hence $(x - y)^n \equiv 0 \pmod{2a_2}$.

Conversely, if $(x - y)^n \equiv 0 \pmod{2a_2}$, then $x \equiv y \pmod 2$ and $a_1(x - y)^n + a_2(x + y)^m \equiv 0 \pmod{2a_2}$, or $a_1(x - y)^n + a_2(x+y)^m = 2a_2z_6$, for some $z_6 \in I$, and xRy.

<u>Corollary 2.1</u>: The equation

$$a_1(x - y)^2 + a_2(x+y) = 2a_2z \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.13)$$

defines an equivalence relation over I such that:

(i) If $a_1 \equiv a_2 \pmod 2$, then the equivalence classes are given by:

$[J]_R = \{n : n \equiv J \pmod{\sqrt{qa_2}}\}$, where q is the smallest integer such that qa_2 is a perfect square, and $J = 0, 1, 2, \ldots, \sqrt{qa_2} - 1$.

(ii) If $a_1 \not\equiv a_2 \pmod 2$, then the equivalence classes are given by:

$[J]_R = \{n : n \equiv J \pmod{\sqrt{2qa_2}})$, where q is the smallest positive integer such that $2qa_2$ is a perfect square, and $J = 0, 1, 2, 3, \ldots, \sqrt{2qa_2} - 1$.

L. M. Chawla [1] proved that the equation

$$x^2 + y^2 = 2z^2 \quad \ldots\ldots\ldots\ldots \quad (2.14)$$

does not define an equivalence relation over I.

Theorem 2.5: The equation

$$a_1(x^2 + y^2) + a_3xy = (2a_1 + a_3)z^2 \quad \ldots\ldots\ldots\ldots \quad (2.15)$$

is equivalent to equation (2.6), if $a_3 = 2a_1$; and does not define an equivalence relation over I, if $a_1 = -a_3$.

Proof (i): If $a_3 = 2a_1$, equation (2.15) reduces to $(x + y)^2 = (2z)^2$. Hence $x + y = 2z$, or $x + y = -2z$. The second possibility is ruled out since condition (I) would not be satisfied.

Proof (ii): If $a_3 = -a_1$, the equation reduces to

$$(x - y)^2 + xy = z^2 \quad \ldots\ldots\ldots\ldots \quad (2.15a)$$

Let $x_1 = 2$, $x_2 = 0$, and $x_3 = 3$. Then

x_1Rx_2 because $(2-0)^2 + 0.2 = 2^2 = z^2$.

x_2Rx_3 because $(0-3)^2 + 0.3 = 3^2 = z^2$.

x_1Rx_3 because $(1-3)^2 + 1.3 = 7 \neq z^2$,

for all $z \in I$, and transitivity does not hold.

Theorem 2.6: If a_1 divides a_2, the equation

$$a_1(x^2 + y^2) + a_2(x + y) = 2a_1z^2 + 2a_2z \quad \ldots\ldots\ldots \quad (2.16)$$

does not define an equivalence relation over I.

Proof: Multiply both sides of equation (2.16) by $4a_1$ and add $2a_2^2$, to get

$$4a_1^2x^2 + 4a_1a_2x + 4a_1^2y^2 + 4a_1a_2y + 2a_2^2 = 2(4a_1^2z^2 + 4a_1a_2z + a_2^2)$$

which simplifies to

$$(2a_1x + a_2)^2 + (2a_1y + a_2)^2 = 2(2a_1z + a_2)^2 \quad \ldots\ldots\ldots \quad (2.16a)$$

There is no loss of generality if we consider a_1 to be positive and $0 \leq a_2 < 2a_1$. For if $a_2 < 0$ or $a_2 \geq 2a_1$, then $a_2 \equiv a_2^1 (\text{mod } 2a_1)$, where $0 \leq a_2^1 < 2a_1$. Then

$$(2a_1x + 2a_1q + a_2^1)^2 + (2a_1y + 2a_1q \cdot a_2^1)^2 = 2(2a_1z + 2a_1q + a_2^1)^2$$

or

$$(2a_1X + a_2^1)^2 + (2a_1Y + a_2^1)^2 = 2(2a_1Z + a_2^1)^2 \quad \ldots\ldots\ldots\ldots \quad (2.16b)$$

where $X = x + q$, $Y = y + q$, and $Z = z + q$.

Equation (2.16b) is of the same form as equation (2.16a).

Under the above assumption if $a_1 \mid a_2$, then $a_1 = 1$, and $a_2 = 0$, or 1. If $a_2 = 0$, the equation reduces to $(2x)^2 + (2y)^2 = 2(2z)^2$, or $x^2 + y^2 = 2z^2$, which does not define an equivalence relation. If $a_2 = 1$, the equation reduces to

$$(2x + 1)^2 + (2y + 1)^2 = 2(2z + 1)^2 \quad \ldots\ldots\ldots\ldots\ldots \quad (2.16c)$$

Let $x_1 = 0$, $x_2 = 3$, and $x_3 = 11$. Then x_1Rx_2 because $(2\cdot 0 + 1)^2 + (2\cdot 3 + 1)^2 = 2(5)^2 = 2(2\cdot 2 + 1)^2 = 2(2z_1 + 1)^2$, where $z_1 = 2$.

$x_2 R x_3$ because $(2.3+1)^2 + (2.11+1)^2 = 2(17)^2 = 2(2.8+1)^2 = 2(2z_2+1)^2$, where $z_2 = 8$. However $x_1 R x_3$ because $(2.0+1)^2 + (2.11+1)^2 = 2(265) \neq 2(2z+1)^2$, for all $z \in I$.

Thus equation (2.16c) does not define an equivalence relation.

<u>Theorem 2.7</u>: The equation

$$a_1(x^2+y^2)+a_2(x+y)+a_3xy = (2a_1+a_3)z^2+2a_2z \quad \dots\dots\dots\dots \quad (2.17)$$

is equivalent to equation (2.6) if $2a_1 = a_3$. If $a_1 = -a_3$ and $a_1 \mid a_2$, the equation does not define an equivalence relation.

<u>Proof</u>: If $2a_1 = a_3$, the equation reduces to

$$a_1(x+y)^2 + a_2(x+y) = 4a_1z^2 + 2a_2z \quad \dots\dots\dots\dots \quad (2.17a)$$

Multiply both sides of equation (2.17a) by $4a_1$ and add a_2^2, to get

$$4a_1^2(x+y)^2 + 4a_1a_2(x+y) + a_2^2 = 16a_1^2z^2 + 8a_1a_2z + a_2^2$$

or

$$\left[2a_1(x+y)+a_2\right]^2 = (4a_1z+a_2)^2 \quad \dots\dots\dots\dots \quad (2.17b)$$

Hence

$$2a_1(x+y)+a_2 = 4a_2z+a_2, \text{ or } 2a_1(x+y)+a_2 = -4a_1z - a_2.$$

The second possibility is ruled out since it contradicts condition (I). The first possibility implies that $x+y = 2z$, which is equation (2.6).

If $a_1 = -a_3$ and $a_2 = qa_1$, for some $q \in I$, then the equation reduces to

$$(x-y)^2 + (x+q)(y+q) = (z+q)^2 \quad \dots\dots\dots\dots \quad (2.17c)$$

Let $x_1 = 0$, $x_2 = -q$, and $x_3 = q$. Then $(0+q)^2 + (-q+q)(q+q) = (q)^2 = (z_1+q)^2$, where $z_1 = 0$, and $x_1 R x_2$.

$(-q - q)^2 + (-q + q)(q + q) = (2q)^2 = (z_2 + q)^2$, where $z_2 = q$, and $x_2 R x_3$.

$$(0 - q)^2 + (q + q)(0 + q) = 3q^2 \neq (z + q)^2,$$

for all $z \in I$, and $x_1 \not{R} x_3$.

Thus transitivity does not hold.

CHAPTER III

THIRD DEGREE EQUATIONS DEFINING EQUIVALENCE RELATIONS

The general cubic Diophantine equation of the form $P(x, y) = \emptyset(z)$ is

$$a_1x^3 + a_2x^2 + a_3x + a_4x^2y + a_5xy + a_6y^3 + a_7y^2 + a_8y + a_9xy^2 = b_1z^3 + b_2z^2 + b_3z + b_4$$

Condition (I) implies that:

$$\left.\begin{aligned} a_1 + a_4 + a_6 + a_9 &= b_1 \\ a_2 + a_7 + a_9 &= b_2 \\ a_3 + a_8 &= b_3 \\ 0 &= b_4 \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.1)$$

Condition (II) implies that:

$$\left.\begin{aligned} a_1 &= a_6 \\ a_2 &= a_7 \\ a_3 &= a_8 \\ a_4 &= a_5 \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.2)$$

Equations (3.1) and (3.2) imply that:

$$\left.\begin{aligned} 2a_1 + a_4 &= b_1 \\ 2a_2 + a_5 &= b_2 \\ 2a_3 &= b_3 \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.3)$$

Thus the general form of the equation reduces to

$$a_1(x^3+y^3)+a_2(x^2+y^2)+a_3(x+y)+a_4(x^2y+xy^2)+a_5xy =$$

$$(2a_1+a_4)z^3+(2a_2+a_5)z^2+2a_2z \quad \ldots\ldots\ldots\ldots \quad (3.4)$$

We assume throughout the discussion that a_1 and a_4 are not zero at the same time; otherwise the equation would be of the second degree.

Altogether 38 different cases of equation (3.4) arise depending on the values of the coefficients. They are listed tables (3.1) to (3.4).

Table 3.1: Equations of the form (3.4) with $a_1 = 0$.

a_1	a_2	a_3	a_4	a_5	$(2a_1+a_4)$	$2a_2+a_5$	$2a_3$
0	0	0	a_4	0	$2a_4$	0	0
0	0	0	a_4	a_5	$2a_4$	a_5	0
0	0	a_3	a_4	0	$2a_4$	0	$2a_3$
0	0	a_3	a_4	a_5	$2a_4$	a_5	$2a_3$
0	a_2	0	a_4	0	$2a_4$	$2a_2$	0
0	a_2	0	a_4	a_5	$2a_4$	$2a_2+a_5$	0
0	a_2	0	a_4	$-2a_2$	$2a_4$	0	0
0	a_2	a_3	a_4	$-2a_2$	$2a_4$	0	$2a_3$
0	a_2	a_3	a_4	0	$2a_4$	$2a_2$	$2a_3$
0	a_2	a_3	a_4	a_5	$2a_4$	$2a_2+a_5$	$2a_3$

Table 3.2: Equations of the form (3.4) with $a_4 = 0$

a_1	a_2	a_3	a_4	a_5	$(2a_1 + a_4)$	$2a_2 + a_5$	$2a_3$
a_1	0	0	0	0	$2a_1$	0	0
a_1	0	0	0	a_5	$2a_1$	a_5	0
a_1	0	a_3	0	0	$2a_1$	0	$2a_3$
a_1	0	a_3	0	a_5	$2a_1$	a_5	$2a_3$
a_1	a_2	0	0	0	$2a_1$	$2a_2$	0
a_1	a_2	0	0	a_5	$2a_1$	$2a_2 + a_5$	0
a_1	a_2	0	0	$-2a_2$	$2a_1$	0	0
a_1	a_2	a_3	0	$-2a_2$	$2a_1$	0	$2a_3$
a_1	a_2	a_3	0	0	$2a_1$	$2a_2$	$2a_3$
a_1	a_2	a_3	0	a_5	$2a_1$	$2a_2 + a_5$	$2a_3$

Table 3.3: Equations of the form (3.4) with

$2a_1 = -a_4$

a_1	a_2	a_3	a_4	a_5	$(2a_1 + a_4)$	$2a_2 + a_5$	$2a_3$
a_1	0	a_3	$-a_1$	0	0	0	$2a_3$
a_1	0	0	$-a_1$	a_5	0	a_5	0
a_1	0	a_3	$-a_1$	a_5	0	a_2	$2a_3$
a_1	a_2	0	$-a_1$	0	0	$2a_2$	0
a_1	a_2	0	$-a_1$	a_5	0	$2a_2 + a_5$	0
a_1	a_2	a_3	$-a_1$	0	0	$2a_2$	$2a_3$
a_1	a_2	a_3	$-a_1$	$-2a_2$	0	0	$2a_3$
a_1	a_2	a_3	$-a_1$	a_5	0	$2a_2 + a_5$	$2a_3$

Table 3.4: Equations of the form (3.4) with $a_1 a_4 (2a_1 + a_4) \neq 0$.

a_1	a_2	a_3	a_4	a_5	$(2a_1 + a_4)$	$2a_2 + a_5$	$2a_3$
a_1	0	0	a_4	0	$(2a_1 + a_4)$	0	0
a_1	0	0	a_4	a_5	$(2a_1 + a_4)$	a_5	0
a_1	0	a_3	a_4	0	$(2a_1 + a_4)$	0	$2a_3$
a_1	0	a_3	a_4	a_5	$(2a_1 + a_4)$	a_5	$2a_3$
a_1	a_2	0	a_4	0	$(2a_1 + a_4)$	$2a_2$	0
a_1	a_2	0	a_4	a_5	$(2a_1 + a_4)$	$2a_2 + a_5$	0
a_1	a_2	0	a_4	$-2a_2$	$(2a_1 + a_4)$	0	0
a_1	a_2	a_3	a_4	$-2a_2$	$(2a_1 + a_4)$	0	$2a_3$
a_1	a_2	a_3	a_4	0	$(2a_1 + a_4)$	$2a_2$	$2a_3$
a_1	a_2	a_3	a_4	a_5	$(2a_1 + a_4)$	$2a_2 + a_5$	$2a_3$

<u>Theorem 3.1</u>: The equations

$$x^3 + y^3 = 2z^3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.5)$$

$$x^2y + xy^2 = 2z^3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.6)$$

define equivalence relations over Z. For every integer $n \in Z$ the equivalence class $[n]_R$ consists of the integer n only.

<u>Proof</u>: Equations (3.4) and (3.5) are impossible in integers, except for the trivial solution $x = y = z$. Therefore, xRy if and only if $x = y$.

Transitivity holds, since aRb and bRc imply that $a = b = c$, and hence aRc.

If $a \in [n]_R$, then aRn. Hence $a = n$, and the equivalence class $[n]_R$ consists of the integer n only.

The following lemmas are needed for later discussion in this chapter.

<u>Lemma 3.1</u>: Let m and n be two positive integers and p a prime. If any two of the following three congruences are satisfied, then the third is satisfied:

$$(x+y)^m (x-y)^n \equiv 0 \pmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.7)$$

$$(y+z)^m (y-z)^n \equiv 0 \pmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.8)$$

$$(x+z)^m (x-z)^n \equiv 0 \pmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.9)$$

<u>Proof</u>: We prove that the congruences (3.7) and (3.8) imply congruence (3.9). The other cases can be proved similarly.

Congruence (3.7) implies that $p \mid (x+y)$, or $p \mid (x-y)$.

Congruence (3.8) implies that $p \mid (y \quad z)$ or $p \mid (y - z)$.

If $p \mid (x+y)$ and $p \mid (y \quad z)$, then $p \mid (x - z)$. Thus $(x - z)^n \equiv 0 (\text{mod } p)$ and $(x+z)^m (x - z)^n \equiv 0 (\text{mod } p)$.

If $p \mid (x+y)$ and $p \mid (y - z)$, then $p \mid (x+z)$. Thus $(x+z)^m \equiv 0 (\text{mod } p)$ and $(x+z)^m (x - z)^n \equiv 0 (\text{mod } p)$.

If $p \mid (x - y)$ and $p \mid (y+z)$, then $p \mid (x+z)$. Thus $(x+z)^m \equiv 0 (\text{mod } p)$ and $(x+z)^m (x - z)^n \equiv 0 (\text{mod } p)$.

If $p \mid (x - y)$ and $p \mid (y - z)$, then $p \mid (x - z)$. Thus $(x - z)^n \equiv 0 (\text{mod } p)$ and $(x+z)^m (x - z)^n \equiv 0 (\text{mod } p)$.

Lemma 3.2: Let m and n be positive integers, and p a prime. If any two of the following three congruences are satisfied, then the third congruence is satisfied:

$$(x+y+1)^m (x - z)^n \equiv 0 (\text{mod } p) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.10)$$

$$(y+z+1)^m (y - z)^n \equiv 0 (\text{mod } p) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.11)$$

$$(x+z+1)^m (x - z)^n \equiv 0 (\text{mod } p) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.12).$$

Proof: The proof is similar to that of lemma (3.1).

Now we discuss the conditions under which the equation

$$a_1(x+y)(x-y)^2 + a_3(x+y) = 2a_3 z \quad \ldots\ldots\ldots\ldots\ldots \quad (3.13)$$

defines an equivalence relation, and characterize the equivalence classes. It will be assumed that $(a_1, a_3) = 1$, and a_3 is positive.

Theorem 3.2: Let $a_3 = 1$. If a_1 is even, then equation (3.13) is equivalent to equation (2.6). If a_1 is odd, then it defines a universal equivalence relation over I.

Proof: If $a_1 = 2a_1^1$, then equation (3.13) reduces to

$$2a_1^1(x+y)(x-y)^2+(x+y) = 2z \quad \ldots\ldots\ldots\ldots\ldots (3.14a)$$

$2a_1^1(x+y)(x-y)^2$ is even and so is the right hand side of equation (3.14a). Hence if xRy, then $x+y \equiv 0 \pmod 2$, and $x \equiv y \pmod 2$.

Conversely, if $x \equiv y \pmod 2$, then $x+y \equiv 0 \pmod 2$, and $2a_1^1(x+y)(x-y)^2+(x+y) \equiv 0 \pmod 2$, and hence xRy.

Thus xRy if and only if $x \equiv y \pmod 2$, and (3.14a) is equivalent to equation (2.6).

If $a_1 = 2a_1^1 + 1$, equation (3.13) reduces to

$$2a_1^1(x+y)(x-y)^2+(x+y)\left\{(x-y)^2+1\right\} = 2z \quad \ldots\ldots\ldots (3.14b)$$

Note that $(x+y)\left\{(x-y)^2+1\right\}$ is even for all x and y. Hence $\left[2a_1^1(x+y)(x-y)^2+(x+y)\left\{(x-y)^2+1\right\}\right]$ is even for all x and y. Thus equation (3.14b) is solvable for any choice of x and y. Consequently, xRy for all x and y, and the conclusion of the theorem follows.

Theorem 3.3: If $a_3 = p$, an odd prime, then equation (3.13) defines an equivalence relation over I such that:

If a_1 is odd, the equivalence classes are given by $[J]_R = \{n : n \equiv J, \text{ or } -J \pmod p\}$, where $J = 0, 1, 2, \ldots, \frac{p-1}{2}$.

If a_1, is even, the equivalence classes are given by $[J]_R = \{n : n \equiv J, \text{ or } -J \pmod{2p}\}$, where $J = 0, 1, 2, \ldots, p$.

Proof: Case (i). Let a_1 be odd and let xRy. Then

$$a_1(x+y)(x-y)^2+p(x+y) = 2pz_1, \text{for some } z_1 \in I \quad \ldots\ldots\ldots (3.15a)$$

$p(x+y) \equiv 2p(z_1) \equiv 0 \pmod p$. Hence $a_1(x+y)(x-y)^2 \equiv 0 \pmod p$ and $(x+y)(x-y)^2 \equiv 0 \pmod p$.

Conversely, if $(x+y)(x-y)^2 \equiv 0 \pmod p$, then

$$a_1(x+y)(x-y)^2 + p(x+y) \equiv 0 \pmod p \quad \text{.........} \quad (3.15b)$$

The left hand side of congruence (3.15b) is even for any pair of integers x and y, then $a_1(x+y)(x-y)^2 + p(x+y) \equiv 0 \pmod{2p}$, and xRy.

Thus xRy if and only if $(x+y)(x-y)^2 \equiv 0 \pmod p$.

To show that transitivity holds, let x_1Rx_2 and x_2Rx_3. We have then:

$$(x_1+x_2)(x_1-x_2)^2 \equiv 0 \pmod p \quad \text{...............} \quad (3.15c)$$

$$(x_2+x_3)(x_2-x_3)^2 \equiv 0 \pmod p \quad \text{...............} \quad (3.15d)$$

In lemma 3.1, if we let $m = 1$ and $n = 2$, we get $(x_1+x_3)(x_1-x_3)^2 \equiv 0 \pmod p$, and x_1Rx_3.

Let $A_J = \{n : n \equiv J, \text{ or } -J \pmod J\}$, $J = 0, 1, 2, \ldots, \frac{p-1}{2}$. To show that A_J is an equivalence class, let $x, y \in A_J$, then $x \equiv J \pmod p$ or $x \equiv -J \pmod p$, and $y \equiv J \pmod p$ or $y \equiv -J \pmod p$.

If $x \equiv J \pmod p$ and $y \equiv J \pmod p$, then $x \equiv y \pmod p$, and $x - y \equiv 0 \pmod p$; consequently, $(x+y)(x-y)^2 \equiv 0 \pmod p$ and xRy.

If $x \equiv J \pmod p$ and $y \equiv -J \pmod p$, then $x \equiv -y \pmod p$ and $(x+y) \equiv 0 \pmod p$; consequently, $(x+y)(x-y)^2 = 0 \pmod p$ and xRy.

Similarly if $x \equiv -J \pmod p$ and $y \equiv J \pmod p$, or $x \equiv -J \pmod p$ and $y \equiv -J \pmod p$, then xRy.

Now, let $x \in A_{J_1}$, $y \in A_{J_2}$, and let $J_1 \neq J_2$, say $J_1 > J_2$.

Suppose xRy, then we have $(x+J_1)(x-J_1)^2 \equiv 0 \pmod p$ and $(y+J_2)(y-J_2)^2 \equiv 0 \pmod p$. By lemma (3.1), we get $(J_1+J_2)(J_1-J_2)^2 \equiv 0 \pmod p$. Therefore, $J_1+J_2 \equiv 0 \pmod p$ or $J_1 - J_2 \equiv 0 \pmod p$. The two congruences are impossible since $0 < J_1 + J_2 < p-1$ and $0 < J_1 - J_2 < \frac{p-1}{2}$. Hence $x \not R y$.

<u>Case (ii)</u>: If a_1 is even, then it can be shown as in case (i) that xRy if and only if $(x+y)(x-y)^2 \equiv 0 \pmod{2p}$.

To establish transitivity, let x_1Rx_2 and x_2Rx_3. Then we have:

$$(x_1+x_2)(x_1-x_2)^2 \equiv 0 \pmod{2p} \quad \ldots\ldots\ldots\ldots\ldots \quad (3.15e)$$

$$(x_2+x_3)(x_2-x_2)^2 \equiv 0 \pmod{2p} \quad \ldots\ldots\ldots\ldots\ldots \quad (3.15f)$$

From (3.15e) and (3.15f) we have $x_1 \equiv x_2 \equiv x_3 \pmod 2$. If $x_1 = 2X_1+1$, $x_2 = 2X_2+1$, and $x_3 = 2X_3+1$, then

$$(X_1+X_2+1)(X_1-X_2)^2 \equiv 0 \pmod p \quad \ldots\ldots\ldots\ldots \quad (3.15e')$$

and

$$(X_2+X_3+1)(X_2-X_3)^2 \equiv 0 \pmod p \quad \ldots\ldots\ldots\ldots \quad (3.15f')$$

By lemma (3.2), with $m = 1$ and $n = 2$, we get

$$(X_1+X_3+1)(X_1-X_2)^2 \equiv 0 \pmod p \quad \ldots\ldots\ldots\ldots, \quad (3.15g)$$

Congruence (3.15g) implies that

$$\left[2(X_1+X_3+1)\right]\left[2(X_1-X_3)\right]^2 \equiv 0 \pmod{2p} \quad \ldots\ldots \quad (3.15g')$$

or $(x_1+x_3)(x_1-x_3)^2 \equiv 0 \pmod{2p}$, and x_1Rx_3.

If $x_1 = 2X_1$, $x_2 = 2X_2$, and $x_3 = 2X_3$, then x_1Rx_3 follows by using lemma (3.1).

The remaining part of the theorem can be shown as in case (i).

A generalization of theorem (3.3) is provided by theorem (3.4) in which m, n, and k are any three positive integers. Condition (I) is not satisfied except when k = 1, while condition (II) is satisfied only when n is even.

Theorem 3.4: Let p be an odd prime and $(a_1, p) = 1$. Then the equation

$$a_1(x+y)^m(x-y)^n + p(x+y)^k = 2pz \quad \ldots\ldots\ldots\ldots \quad (3.16)$$

is equivalent to

$$a_1(x+y)(x-y)^2 + p(x+y) = 2pz.$$

Proof: If a_1 is odd and xRy, then

$$a_1(x+y)^m(x-y)^n + p(x+y)^k = 2pz_1, \text{ for some } z_1 \in I \ \ldots \quad (3.16a)$$

$p \mid 2pz_1$ and $p \mid p(x+y)^k$. Hence $p \mid a_1(x+y)^m(x-y)^n$. Therefore $p \mid (x+y)^m(x-y)^n$; and $p \mid (x+y)$ or $p \mid (x-y)$. In either case

$$(x+y)(x-y)^2 \equiv 0 \pmod{p}.$$

Conversely, if $(x+y)(x-y)^2 \equiv 0 \pmod{p}$, then $p \mid (x+y)$ or $p \mid (x-y)$. Thus $(x+y)^m(x-y)^n \equiv 0 \pmod{p}$, and

$$a_1(x+y)^m(x-y)^n + p(x+y)^k \equiv 0 \pmod{p} \quad \ldots\ldots\ldots\ldots \quad (3.16b)$$

Noting that the left hand side of congruence (3.16b) is even for all x and y, we see that $a_1(x+y)^m(x-y)^n + p(x+y)^k \equiv 0 \pmod{2p}$, and xRy.

Thus if a_1 is odd, xRy if and only if $(x+y)(x-y)^2 \equiv 0 \pmod{p}$. Similarly if a_2 is even, then xRy if and only if

$$(x+y)(x-y)^2 \equiv 0 \pmod{2p}, \quad \text{and}$$

the conclusion of the theorem follows.

If, in theorem (3.4), $p = 2$ then the equation (3.16) is equivalent to equation (2.6). For in this case the equation reduces to:

$$a_1(x+y)^m(x-y)^n + 2(x+y)^k = 4z \quad \ldots\ldots\ldots\ldots\ldots \quad (3.17)$$

with a_1 odd. It can be shown that, xRy if and only if $x \equiv y \pmod 2$, and hence the two equations are equivalent.

<u>Theorem 3.5</u>: Let a_1 be odd. Then the equation

$$a_1(x+y)(x-y)^2 + 2^m(x+y) = 2^{m+1} z \quad \ldots\ldots\ldots\ldots \quad (3.18)$$

is equivalent to equation (2.6), if $m = 2$. If $m = 3$, the equivalence classes are given by:

$$[J]_R = \{4n + J : n \in I\}, \; J = 0, \text{ or } 2.$$

$$[1]_R = \{4n \mp 1 : n \in I\}.$$

<u>Proof</u>: Let $m = 2$ then the equation reduces to

$$a_1(x+y)(x-y)^2 + 4(x+y) = 8z \quad \ldots\ldots\ldots\ldots\ldots \quad (3.18a)$$

Let xRy, then $a_1(x+y)(x-y)^2 \equiv 0 \pmod 2$. Hence $x \equiv y \pmod 2$. Conversely, if $x \equiv y \pmod 2$ then $a_1(x+y)(x-y)^2 \equiv 0 \pmod 8$ and $4(x+y) \equiv 0 \pmod 8$. Therefore, $a_1(x+y)(x-y)^2 + 4(x+y) \equiv 0 \pmod 8$.

Thus xRy if and only if $x \equiv y \pmod 2$, and the conclusion follows.

When $m = 2$, the equation reduces to

$$a_1(x+y)(x-y)^2 + 8(x+y) = 16z \quad \ldots\ldots\ldots\ldots \quad (3.18b)$$

Let $A_J = \{4n + J : n \in I\}$, $J = 0$, or 2, and $A_1 = \{4n \mp 1 : n \in I\}$. First we show that, if $x \in A_i$ and $y \in A_J$, with $i \neq J$, then $x \not R y$.

Note that, if $x \not\equiv y \pmod 2$, then $a_1 (x+y)(x-y)^2$ is odd. Consequently, $a_2 (x+y)(x-y)^2 + 8(x+y) \not\equiv 0 \pmod{16}$, and $x \not R y$. In view of this remark we need only consider the case when $i = 0$ and $J = 2$.

Let $x \in A_0$ and $y \in A_2$, then $x = 4x^1$ and $y = 4y^1 + 2$. Substituting the values of x and y in equation (3.18b) we get

$$8a_1(2x^1 + 2y^1 + 1)(2x^1 - 2y^1 - 1)^2 + 16(2x^1 + 2y^1 + 1) = 16z.$$

Therefore

$$8a_1(2x^1 + 2y^1 + 1)(2x^1 - 2y^1 - 1)^2 \equiv 0 \pmod{16},$$

and hence $a_1 \equiv 0 \pmod 2$, a contradiction to our hypothesis that a_1 is odd. Hence $x \not R y$.

Second we show that, if $x, y \in A_i$, where $i = 0, 1$, or 2, then xRy. We give the proof for $i = 0$, the other cases are similar. Let $x = 4x^1$ and $y = 4y^1$. Then we have

$$a_1(4x^1 + 4y^1)(4x^1 - 4y^1)^2 + 8(4x^1 + 4y^1) = \left[64(x^1 + y^1)(x^1 - y^1)^2 + 32(x^1 + y^1)\right] \equiv 0 \pmod{16}, \text{ and } xRy.$$

Thus xRy if and only if $x, y \in A_i$, $i = 0, 1$, or 2.

To establish transitivity, let aRb and bRc. Then $a, b, c \in A_k$, for some $k = 0, 1$, or 2, and aRc.

Finally, the sets A_0, A_1, and A_2 satisfy the two conditions of definition 1.2, hence they are equivalence classes.

In general, theorem (3.5) does not hold for all positive integers n. We give an example where transitivity is not satisfied for $n = 4$.

<u>Example</u>: Let $n = 4$, $x_1 = 5$, $x_2 = 27$, and $x_3 = 7$. Then

$a_1(5+27)(5-27)^2 + 2^4(5+27) = 2^5 z_1$, where $z_1 = 484a_1 + 16$, and $x_1 R x_2$.

$a_1(27+7)(27-7)^2 + 2^4(27+7) = 2^5 z_2$, where $z_2 = 85a_1 + 17$, and $x_2 R x_3$.

$a_1(5+7)(5-7)^2 + 2^4(5+7) = 2^4(a_1+12) \not\equiv 2^5 z$, for all $z \in I$, since a_1 is odd, and $x_1 \not R x_3$.

Now we discuss the equation

$$a_1(x+y)(x-y)^2 + a_2(x-y) + a_3(x+y) = 2a_3 z \quad \ldots\ldots\ldots\ldots (3.19)$$

which satisfies condition (I), but not (II). There is no loss of generality if we assume that a_3 is positive.

Let $a_1 \equiv b_1 \pmod{2a_3}$ and $a_2 \equiv b_2 \pmod{2a_3}$, where $0 \le b_1, b_2$ $b_1, b_2 < 2a_3$. Therefore, $a_1 = b_1 + 2q_1 a_3$ and $a_2 = b_2 + 2q_2 a_3$. Thus equation (3.19) reduces to

$$2q_1 a_3(x+y)(x-y)^2 + 2q_2 a_3(x-y) + b_1(x+y)(x-y)^2 + b_2(x-y) + a_3(x+y) = 2a_3 z$$

or

$$b_1(x+y)(x-y)^2 + b_2(x-y) + a_3(x+y) = 2a_3 Z \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.20)$$

where

$$Z = z - q_1(x+y)(x-y)^2 + q_2(x-y).$$

Equations (3.19) and (3.20) are equivalent. We will assume throughout the discussion that $(b_1, b_2, a_3) = 1$.

In case $b_1 = b_2 = 0$, we get $x + y = 2Z$, and equation (3.20) is equivalent to equation (2.6)

In case $b_2 = 0$, equation (3.20) reduces to equation (3.13) which has been already discussed.

If $b_1 = 0$, the equation reduces to

$$b_2(x - y) + a_3 (x+y) = 2a_3Z \quad \dots\dots\dots\dots\dots\dots \quad (3.20a)$$

In this case, if $b_2 \equiv a_3 \pmod 2$, then b_2 and a_3 are both odd, since it is assumed that $(b_1, b_2, a_3) = 1$. Let xRy, then $x - y \equiv 0 (\mathrm{mod}\ a_3)$. Conversely, if $x - y \equiv 0(\mathrm{mod}\ a_3)$, then $b_2(x - y) + a_3(x+y) \equiv 0(\mathrm{mod}\ a_3)$. Noting that $b_2(x - y) + a_3(x \quad y)$ is even for all x and y, we see that $b_2(x-y) + a_3(x+y) \equiv 0(\mathrm{mod}\ 2a_3)$, and xRy.

Thus xRy if and only if $x \equiv y(\mathrm{mod}\ a_3)$. Therefore, the equivalence classes are $[J]_R = \{n : n \equiv J(\mathrm{mod}\ a_3)\}$, $J = 0,1,2,\dots,a_3-1$.

Again, if $b_1 = 0$ and $b_2 \not\equiv a_3 \pmod 2$, then it can be shown that xRy if and only if $x \equiv y \ (\mathrm{mod}\ 2a_3)$. Hence the equivalence classes are $[J]_R = \{n : n \equiv J(\mathrm{mod}\ 2a_3)\}$, where $J = 0, 1, 2, \dots, 2a_3 - 1$.

If neither b_1 nor b_2 is zero and $b_1, b_2 < 2a_3$, then with $a_3 = 1$, $b_1 = b_2 = 1$, equation (3.20) reduces to $(x+y)(x-y)^2 + 2x = 2Z$, which is equivalent to equation (2.6), because xRy if and only if $x \equiv y(\mathrm{mod}\ 2)$

If $a_3 = 2$, then 8 different cases of equation (3.20) arise, depending on the value of the coefficients. They are listed in table 3.5.

Table 3.5: Equations of the form (3.20) with $a_3 = 2$.
and $(b_1, b_2, a_3) = 1$.

b_1	b_2	a_3	$2a_3$
1	1	2	4
1	2	2	4
1	3	2	4
2	1	2	4
2	3	2	4
3	1	2	4
3	2	2	4
3	3	2	4

Of the equations listed in table 3.5 the following do not define equivalence relations over I:

$$(x+y)(x-y)^2 + (x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21a)$$

$$3(x+y)(x-y)^2 + (x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21b)$$

$$3(x+y)(x-y)^2 + 3(x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21c)$$

$$(x+y)(x-y)^2 + 3(x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21d)$$

In equation (3.21a) $0R1$ but $1 \not R 0$.

In equation (3.21b) $4R1$ but $1 \not R 4$.

In equation (3.21c) $1R0$ but $0 \not R 1$.

In equation (3.21d) $4R1$ but $1 \not R 4$.

Of the remaining four equations the following two are equivalent to equation (2.6):

$$(x+y)(x-y)^2 + 2(x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21e)$$

and

$$3(x+y)(x-y)^2 + 2(x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21f)$$

The equivalence follows from the fact that in both equations xRy if and only if $(x+y)(x-y)^2 \equiv 0 \pmod 4$.

The last two equations are:

$$2(x+y)(x-y)^2 + (x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21g)$$

and

$$2(x+y)(x-y)^2 + 3(x-y) + 2(x+y) = 4z \quad \ldots\ldots\ldots\ldots \quad (3.21h)$$

In equations (3.21g) and (3.21h) if xRy, then $x \equiv y \pmod 2$. Therefore $2(x+y)(x-y)^2 \equiv 2(x+y) \equiv$ (mod 4); Consequently,

$x - y \equiv 0 \pmod 4$ i.e. $x \equiv y \pmod 4$. Conversely, if $x \equiv y \pmod 4$, then $2(x+y)(x-y)^2 + b_2(x-y) + 2(x+y) \equiv 0 \pmod 4$, where $b_2 = 1$ or $3.$, and xRy.

Thus xRy if and only if $x \equiv y \pmod 4$. Therefore the equivalence classes are $[J]_R = \{n : n \equiv J \pmod 4\}$, where $J = 0, 1, 2, 3$.

CHAPTER IV

NUMBER OF EQUIVALENCE CLASES OF R_P^m

This chapter is devoted to a discussion of equations of the form

$$P(x, y) = mz \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4.1)$$

where P(x,y) is an integral polynomial in x and y, and where conditions (I) and (II) do not necessarily hold. For convenience we will deal with the congruence

$$P(x, y) \equiv 0 \pmod{m} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4.2)$$

rather than equation (4.1). Without loss of generality we may assume m to be positive.

Definition 4.1: P(x,y) is said to be favorable (mod m) if and only if equation (4.1) defines an equivalence relation over I. In this case the equivalence relation is denoted by R_P^m, and the set of distinct equivalence classes by E(P, m).

Definition 4.2: For a given x = a, N(P, a, m) denotes the number of distinct solutions of the congruence $P(a, y) \equiv 0 \pmod{m}$.

Note that if $[a]_{R_P^m}$ is an equivalence class of R_P^m, then there exists an integer b, $0 \leq b < m$ such that $[b]_{R_P^m} = [a]_{R_P^m}$, and N(P, a, m) = N(P, b, m). Thus, in definition 4.2, we may assume that $0 \leq a < m$.

<u>Theorem 4.1</u>: For any divisor d of m if $P(x,y)$ is favorable (mod m), then it is favorable (mod d) and $N(R_P^m) \geq N(R_P^d)$.

<u>Proof</u>: If $P(x,y)$ is favorable (mod m), then it is favorable (mod d), because $P(x,y) \equiv 0 \pmod m$ implies that $P(x,y) \equiv 0 \pmod d$.

To prove the inequality, let

$$E(P,d) = \{[a_i]_{R_P^d} : i = 1, 2, 3, \ldots, N(R_P^d)\},$$

and

$$E(P, m) = \{[b_i]_{R_P^m} : i = 1, 2, \ldots, N(R_P^m)\}.$$

Let $x \in [b_i]_{R_P^m}$, then $P(x, b_i) \equiv 0 \pmod m$. Hence $P(x, b_i) \equiv 0 \pmod d$, and $x R_P^m b_i$. Thus

$$x \in [b_i]_{R_P^d}. \text{ But } [b_i]_{R_P^d} = [a_{k_i}]_{R_P^d},$$

for some k_i depending on i and where, $1 \leq k_i \leq N(R_P^d)$. Therefore,

$$[b_i]_{R_P^m} \subseteq [a_{k_i}]_{R_P^d}, \text{ for all } i = 1, 2, \ldots, N(R_P^m).$$

If $[b_i]_{R_P^m} \subseteq [a_{J_i}]_{R_P^d}$, then $[a_{k_i}]_{R_P^d} = [a_{J_i}]_{R_P^d}$

and $k_i = J_i$. That is every equivalence class in $E(P, m)$ is contained in exactly one equivalence class of $E(P,d)$.

Sine

$$\bigcup_{i=1}^{s} b_i{}_{R_P^m} = \bigcup_{i=1}^{t} a_i{}_{R_P^d} = I, \; s = N(R_P^m)$$

and $t = N(R_P^d)$, then every equivalence class in $E(P, d)$ contains an equivalence class of $E(P, m)$.

The mapping $f: E(P, m) \rightarrow E(P, d)$ defined by

$$f([a_i]_{R_P^m}) = [b_{k_i}]_{R_P^d},$$

is well defined and onto. Therefore, $N(R_P^m) \geq N(R_P^d)$.

Theorem 4.2: Let $P(x, y) = P_1(x, y)\, P_2(x, y)$. If $P_1(x, y)$ is favorable (mod m), then $N(R_P^m) \leq N(R_{P_1}^m)$.

Proof: If $P(x, y)$ is not favorable (mod m), then $N(R_{P_1}^m) = 0$, and the inequality is satisfied.

If $P(x, y)$ is favorable (mod m), then it can be shown as in theorem (4.1) that every equivalence class in $E(P_1, m)$ is contained in exactly one equivalence of $E(P, m)$, and that every equivalence class in $E(P, m)$ contains an equivalence class of $E(P_1, m)$. Thus $N(R_{P_1}^m) \leq N(R_{P_2}^m)$.

Theorem 4.3: If $P(x, y)$ is favorable (mod m), then $N(R_P^d) \leq (m + 1 - \max\{N(P, a, m) : 0 \leq a < m\})$, for any divisor d of m.

Proof: Let $A = \{[J]_{R_P^m} : J = 0, 1, 2, \ldots, m - 1\}$ be a set of equivalence classes that are not necessarily distinct. In particular if $y \equiv s \pmod{m}$, $0 \leq s < m$, is a solution of the congruence

$$P(a, y) \equiv 0 \pmod{m} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (4.3)$$

then $P(a, s) = 0 \pmod{m}$. Consequently, $[s]_{R_P^m} = [a]_{R_P^m}$.

Noting that $y \equiv a \pmod{m}$ is a solution of (4.3), we see that there are $\{N(P, a, m) - 1\}$ incogruent solutions (mod m) of (4.3), all different from a.

Hence there are at most $(m - \{N(P, a, m) - 1\})$ distinct classes in A. That is $N(R_P^m) \leq [m + 1 - N(P, a, m)]$ for all $a = 0, 1, 2, \ldots, m - 1$, and $N(R_P^m) \leq (m + 1 - \max\{N(P, a, m): a = 0, 1, 2, \ldots, m - 1\})$. By theorem (4.1),

$$N(R_P^d) \leq (m + 1 - \max\{N(P, a, m): 0 \leq a < m\}).$$

REFERENCES

1. Chawla, L. M. On Diophantine Equations Defining Equivalence Relations Over the Integers; Journal of Natural Sciences and Mathematics. Vol. 3(1963), No. 1, pp. 83 - 98.

2. Chawla, L. M., Shafaat, On Certain Classes of Diophantine Equations Defining Equivalence Relations Over Integers. Journal of Natural Sciences and Mathematics. Vol. 3 (1963) No. 2 pp. 163 - 173.

3. Dickson, L. E., History of the Theory of Numbers. Vol. II, Chelsea Publishing Company, 1952.

4. Carmichael, R. D., The Theory of Numbers and Diophantine Analysis. Dover Publications, Inc. 1914.

5. Grosswald, E., Topics From the Theory of Numbers; the Macmillan Company, 1966.