INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

U·M·I

University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313/761-4700 800/521-0600

Order Number 9130353

Rays of small integer solutions of homogeneous ternary quadratic equations

Mishra, Sudhakara, Ph.D.

City University of New York, 1991

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

RAYS OF SMALL INTEGER SOLUTIONS OF HOMOGENEOUS TERNARY QUADRATIC EQUATIONS

by

Sudhakara Mishra

A dissertation submitted to the Graduate Faculty in
Mathematics in partial fullfilment of the requirements for the
Degree of Doctor of Philosophy
The City University of New York

1991

This manuscript has been read and accepted by the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the Degree of Doctor of Philosophy.

4/30/91
Date

Harvey Cohn
Chairman of Examining Committee

May 6, 1991
Date

Martin M. Moskowitz
Executive Officer

Harvey Cohn

Richard Sacksteder

Burton Randol

Supervisory Committee

The City University of New York

In the hands of my Mother
Mrs. Saraswati Mishra
who also represents my Father
Late Biswanath Mishra
of the village
Karanda,
in the district of
Dhenkanal
of the Province of
Orissa
in
India

ABSTRACT

Rays of Small Integer Solutions of Homogeneous Ternary Quadratic Equations

by
Sudhakara Mishra

Advisor: Harvey Cohn

From the viewpoint of integer-solution-finding, even though the quadratics have been the most amenable class of equations, there are still things left undone. Many of the existing algorithms are also not in a very satisfactory form. Here we have tried to ameliorate this state of the computational quadratic theory to some extent.

We have dealt with the general ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$$

with integer coefficients. After giving a matrix-reduction formula for a quadratic equation in any number of variables, of which the reduction of the above ternary equation is an easy consequence, we have devoted our attention to the reduced equation:

$$ax^2 + by^2 + cz^2 = 0.$$

First we have structured an algorithm for solving this reduced equation. This algorithm is extracted from Dirichlet's proof of the Legendre's theorem stating that: $ax^2 + by^2 + cz^2 = 0$, with abc nonzero and square-free, is non-trivially solvable if and only if not all of the coefficients a, b and c are with the same sign, and moreover $-bc$, $-ca$ and $-ab$ are quadratic residues of $|a|$, $|b|$ and $|c|$ respectively.

Then by examining Mordell's proof of Holzer's theorem asserting that: whenever $ax^2+by^2+cz^2 = 0$ is nontrivially solvable, there is a nonzero solution with

$$|x| \leq \sqrt{|bc|}, \qquad |y| \leq \sqrt{|ca|}, \qquad \text{and} \qquad |z| \leq \sqrt{|ab|},$$

we have devised an algorithm for reducing Dirichlet's possibly larger solutions to this prescribed range of Holzer's.

Then we have generalized Holzer's theorem to the case of the ternary equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0,$$

giving in this context a new range called the CM-range, of which the Holzer's range is a particular case when $d = e = f = 0$. We have described an algorithm for getting a solution of the general ternary within this CM-range.

After that we have devised an algorithm for getting all the solutions of the Legendre's equation $ax^2 + by^2 + cz^2 = 0$ within the Holzer's range — and have shown that if we regard this Legendre's equation as a double cone, these solutions within the Holzer's range lie along some definite rays, here called the CM-rays, which are completely determined by the prime factors of the coefficients a, b and c.

Then after giving an algorithm for detecting these CM-rays of the reduced equation: $ax^2 + by^2 + cz^2 = 0$, we have shown how one can produce some similar rays of solutions of the above general ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$

Note that apart from the method of exhausting all the possibilities, so far there has been no precisely stated algorithm to find the minimum solutions of the above ternary equations. The above-mentioned algorithm of ours for reaching the minimum solution of the Legendre's equation

$$ax^2 + by^2 + cz^2 = 0$$

is even much faster than the existing Dirichlet's algorithm that yielded to this day only a non-minimal solution most of the times.

Towards the end, observing in the context of our main result an inequality involving two functions, namely C and PCM from $\mathbb{Z}_*^3$ to $\mathbb{Z}_+$, and simultaneously presenting some tables of these positive CM-rays or PCM-rays lying in the positive octant, we have concluded this work with a number of hints for some possible future investigations.

At the very end, we have appended this work with an autobiographical note depicting the true genesis of this work.

ACKNOWLEDGEMENTS

To start with, I must express my deepest gratitude to Professor Harvey Cohn for the inspiration he aroused in me for initiating this work. At a point when I thought that my initial goal was already achieved, his insistence and suggestion to search through a class of computational results led me to a very new and pleasing discovery which we have presented in Chapter 6. The supreme experience of finding this new theory, all on a sudden has reinvigorated my computational zeal which gradually was losing its life. For this rediscovery of the mathematical spirit within myself, I owe to Professor Cohn my lifelong indebtedness.

Professor Cohn is the last person I have been linked with in connection to my mathematical involvements. There are a host of descent mathematicians who have tried to instill some firy inspirations into my mind. An incomplete list would chronologically include my elementary school teacher Mr. Bhaskar Chandra Raut, my high-school teacher Mr. Madan Mohan Panda, and university educators Professor Siba Prasad Misra, Dr. Sribatsa Nanda, Dr. Bipin Bihari Panda, Dr. Krushna Chandra Nayak, Dr. Sudarsan Nanda, Professor Renzo Angello Piccinini, Professor S. Thomeier, Professor Peter Hilton, Dr. S. P. Singh, Dr. David A. Edward, Dr. Harold Morris Hastings, Professor Alex Heller, Professor A. T. Vasquez, Professor Eldon Dyer, Professor Gilbert Baumslag, Professor Martin Moskowitz, Dr. Richard Reth, and my good friend Late Dr. Jacek Zieba who very highly appreciated a part of this work but could not stay to see it in its completed form. In my typical style I have absorbed from them something at some point, sometimes may be even without their realizing my receptive role. Even on my own part it is very hard to assess how much of their influences are and will be controlling my growth, in some way or other, in writing and expressing the things I think. I must express my indebtedness to them at this crucial point of my admittance into the so called mature group of mathematicians.

In the social front, I owe the maximum to my wife Rita without whose cooperation, sacrifices and encouragements it would have been almost impossible to accomplish what is in my hand today. I must also thank my children Sambit, Sandeep, and Sangeeta for bearing with my life-style of a devotee of the rigorous science such as ours.

There are two more people in my social life who impelled the mathematical desire in me at some crucial points of my life: first and foremost, my brother Sj. Nishakar Mishra, to whom I owe more than anybody else in my life for the sustenance of my academic career and lifting my ambition to a level probably much higher than I can ever reach; and secondly, another intellectual of the finest calibre → Dr. Govind Chandra Mishra, whose influence and a critical analysis of my personal character has

kept me steadfast in my pursuits sometimes even amid the most blinding difficulties. I express my life-long indebtedness to both of them.

I owe to a number of institutions for their support: Regional Engineering College at Rourkela in India; Memorial University of Newfoundland in St. John's; University of Georgia at Athens, and finally our City University of New York: especially its Research Foundation and its campuses of Baruch College, New York City Technical College, City College, Lehman College, and the last but the Greatest of all: our Graduate Center with its well-equipped Mina-Rees Library. I sincerely express my indebtedness to each of them.

I will be failing in my duty if I do not acknowledge the roles of an IBM PC, a few Casio calculators, and especially an HP-28S and an HP-48SX hand-held computer of the Hewlett Packard Company which were instrumental in discovering the CM-rays that constitute the central theme of this dissertation. Also Donald Knuth's TEX and the Postscript page description language of the Adobe Systems Incorporated gave me the capability of writing this document in the present form and drawing some of the beautiful pictures of our CM-Rays. I express my deep gratitude to each of them who immensely help at this moment in the growth of our Science at a tremendous speed.

I would also like to express my heartiest gratitude to Professor Burton C. Randol for his support at a very crucial juncture of my career.

Finally I express my sincerest thankfulness to my friends Marina and Dimitri Vulis for their initial help in typing some portions of the first three Chapters about two years ago, the outcome of which made me determined to learn the TEX and the LATEX at some point in future, which I partly accomplished over the past couple of months and got this dissertation typed myself. Without their challenging encouragement the pleasing typography of this document would have been unthinkable.

Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

1.1 Defining The Goal

We intend to deal with the integer solutions of the homogeneous ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$

This problem is a highly special case of the extremely general problem of solving a polynomial equation: $P(x_1, x_2, \ldots, x_n) = 0$ in n variables of any arbitrary degree. But this latter case obviously is too general a problem to be handled as a single project. On the other hand, anybody unfamiliar with the present status of the computational number theory runs the risk of considering our goal of dealing with the integer solutions of the above-mentioned homogeneous ternary quadratic equation as a very trivial undertaking. For avoiding such a possible mistake a brief history of the problem of solving the general polynomial equations in integers is very much in order at this point.

1.2 A Brief History

The problem of solving a polynomial equation is actually as old as mathematics itself. The indomitable desire of equation solving has been a common instinct of any inquisitive mind almost since the dawn of our civilization. The existing recorded history gives the evidence that there have been efforts along this line since the olden days of Babylon and the Hindus, which goes as far back as about two millennia before Christ.

Even though the work of Pythagoras (around 500 BC) does reflect some amount of involvement in these equations, an elaborate study of these problems was done first by the Greek mathematician Diophantus of Alexandria who flourished around 250 AD, in whose honor these problems are named as Diophantine Problems. His works compiled in the form of thirteen books of "*Diophantus' Arithmetica,*" ten of which are available at the present with three more still missing, contain numerous equations with rational and integer solutions.

Since then, as to the general methods for finding integer solutions of polynomial equations with integer coefficients, only for the following three types of equations somewhat satisfactory techniques have been specified:

(i) Unary polynomials of any degree;

(ii) Linear equations in any number of variables ; and,

(iii) Quadratic equations in any number of variables (somewhat incompletely).

Of these, the first two cases are rather easy and elementary. Therefore, in a sense, it can be rightly stated that over all these years, general methods have been tractable only up to the level of some quadratic equations. And even in this context of quadratic equations some serious unresolved restrictions do exist uptill now.

Thus, so far as finding integer solutions of integral polynomial equations is concerned, ever since the pre-Pythagorean period, leaving aside some sporadic involvements in a few other equations, the enigma of quadratic equations has been dominating this typical area of computational mathematics almost continuously. A few details of the corresponding history will probably emphasize this claim.

Since any quadratic equation can be reduced to the diagonal form $\sum_{i=1}^{n} a_i x_i^2 = m$ with $a_1 = 1$ by the method of completing the square, (or more effectively, by the matrix-reduction method of ours presented here in Chapter-3 which leads to $m = 0$ in the homogeneous case), let us try to analyze how this equation:

$$\sum_{i=1}^{n} a_i x_i^2 = m$$

has been handled since antiquity.

Solutions of $ax^2 = 0$ and $ax^2 = m \neq 0$ are obvious. In fact, in place of solving the second equation $ax^2 = m$ with $m \neq 0$, to solve its unreduced form:

$$ax^2 + bx + c = 0,$$

methods were attempted at the latest since the days of the Babylonians till the Hindu mathematician Bramhagupta of the seventh century AD gave the most general formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

which is popularly known as the "quadratic formula". We should note the slow development of the symbolically efficient general method for solving this first nontrivial quadratic equation.

Since the homogeneous equation in two variables can be dealt with by the same old quadratic formula with the substitution of rationals in place of the integers, the next equation to be dealt with was of the form $X^2 - Dy^2 = N$, which, since the time of Euler, is known as the Pell equation.

After Bramhagupta, the next major effort was made by the twelfth century Hindu mathematician Bhaskara who attempted to solve the Pell equation $x^2 = 1 + py^2$ and obtained many partial results. Immediately after Bhaskara, even though some efforts

were made by the Italian mathematician Fibonacci, according to well-publicized history there was actually almost no substantial achievement in integral equation-solving till the seventeenth century.

In 1657, Fermat challenged the contemporary British mathematicians to prove the existence and to devise a method for the complete discovery of the infinite number of integral solutions of the Pell equation: $x^2 - Dy^2 = 1$, where $\sqrt{D}$ is irrational. In some sense, this challenge highlighted the next general and fundamental question after the ancient quadratic formula cited in the above.

There was no complete response to Fermat's challenge for about one hundred and nine years, after which, in 1766, the great Lagrange accomplished the job. Actually his work claimed the solution of the more general equation: $x^2 - Dy^2 = N$, which led to the solution of a class of binary quadratic equations of the type:

$$ax^2 + by^2 + dxy + ex + fy + c = 0.$$

The next major achievement along this line was in 1785 by Legendre through his celebrated theorem relating to the solution of the equation: $ax^2 + by^2 + cz^2 = 0$ with abc nonzero and square-free, stating that it is non-trivially solvable if and only if all of a, b and c are not of the same sign, and, $-bc$, $-ca$ and $-ab$ are quadratic residues of $|a|$, $|b|$ and $|c|$ respectively. In fact this is the last theorem which provides some computationally effective technique for getting the integer solutions of a general quadratic equation, and for that matter of any general polynomial equation. And also this is the theorem which is going to play the most pivotal role in this dissertation.

Even though Legendre's proof for the above theorem was complete, a clearer proof appeared in 1801 in Gauss's classic work: *Disquisitiones Arithmeticæ,* (4). This proof of Gauss again was made much more elegant and computationally pinpointed by Dirichlet that appeared in *Vorlesungen über Zahlentheorie* which was Edited by Dedekind around 1894. This proof of Dirichlet outlines an algorithm for yielding a nontrivial integer solution of $ax^2 + by^2 + cz^2 = 0$ whenever such a solution exists. In fact the detection of this algorithm enkindled the genetic inspiration for creating the central theory of this dessertation.

If, without deviating to the discussion of any other equation, one wants to continue tracing the development about the Legendre's equation: $ax^2+by^2+cz^2 = 0$, one would find the next milestone set by a theorem of Holzer that appeared around 1950 in (5), which states that if this equation is nontrivially solvable, then one such solution must exist with

$$|x| \leq \sqrt{|bc|}, \qquad |y| \leq \sqrt{|ca|}, \qquad \text{and} \qquad |z| \leq \sqrt{|ab|} \quad .$$

But Holzer's proof of this theorem, which heavily depended on the generalized prime-number theorem of Hecke, did not provide any clearcut algorithm for finding a solution within the above range. In fact the computational deficiency of the well-celebrated paper of Holzer, namely (5), (containing the above renowned theorem), is indirectly reflected in the incorrect claim of $(x, y, z) = (1, 9, 20)$ as the minimum solution of $157x^2 + 3y^2 = z^2$, even though $(x, y, z) = (1, 2, 13)$ is the actual minimum solution readily obtained by our algorithm presented here in this dissertation.

However, in 1968, Mordell gave a proof of Holzer's theorem in (9) which provided the missing algorithm that can be applied on an already abtained nontrivial solution so as to reach at a solution within the Holzer's range. Thus if one collects all the related computational results systematically up to 1968: by using Dirichlet's algorithm one could get a nontrivial solution of a Legendre's equation whenever such a solution exists, which however, may be far beyond the Holzer's range; and then by applying Mordell's algorithm on this solution of Dirichlet one could reach at a notrivial solution within the Holzer's range. After the above paper (9) of Mordell, the next published result which has come to our eyes that is relevant to integral solutions of the Legendre's equation:

$$ax^2 + by^2 + cz^2 = 0$$

is due to Williams, namely (15), which has liberated the Legendre's equation from the restrictive condition of abc being square-free. As far as we know, that is the last well publicized result relating to the computational treatment of the Legendre's equation, and for that matter, relating to the effective computation of the solution for any general polynomial equation in more than two variables and of degree larger than one.

In the above we digressed to discuss continuously about the Legendre's equation a little longer than that would have been in keeping with the initial speed of this brief historical account of solving polynomial equations in integers. However, we thought it to be appropriate because Legendre's equation is very central to the theory we have developed in this dissertation — and moreover, because so far it is the last general polynomial equation for whose integer solutions effective economical algorithms have been outlined here in this work and earlier elsewhere.

Now to continue and thereby leading to a brief conclusion of our original historical investigation, we should resume by observing that ever since the appearance of Legendre's theorem even though there have been a number of helpful results giving hints about the existence of integer solutions for more general quadratic equations, there exist no effective algorithms for their computations. Though till the 1870's there were many important contributions to the general theory of quadratic equations by several important mathematicians including Gauss, Dirichlet, Eisenstein, and H. J. S. Smith, the next major concrete computational result after Legendre's theorem appeared around 1884 through Meyer's work (7) relating to representations of nonzero integers by ternary forms, and solutions of diagonal homogeneous equations in four and five variables:

$$ax^2 + by^2 + cz^2 + du^2 = 0$$

and

$$ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0.$$

Some of these results were refined and new related results were given by Leonard Eugene Dickson around 1930, and over a period of several decades by Louis Joel Mordell during the first two thirds of this twentieth century. In 1966, Mordell gave

a very restricted result in (8) on the solvability of the four-variable nonhomogeneous equation:

$$ax^2 + by^2 + cz^2 + du^2 = m \quad \text{with} \quad m \neq 0.$$

Before concluding this section giving a historical account of solving the general polynomial equations in integers, which in reality has turned out to be the corresponding history only of the quadratic equations, we want to make a critical remark that: Yes, it is true that as to the general theory of polynomial equations, by now a number of very powerful general results have been in our hand including such as those of Axel Thue and Gerd Faltings claiming that:

> " For a homogeneous irreducible integral polynomial $P(x, y)$ in two variables and of degree $n \geq 3$, the equation $P(x, y) = c$, with c as a constant, can have only a finite number of integral solutions."
>
> — *Axel Thue (1908)*

and,

> "A binary polynomial equation with rational coefficients whose genus is larger than 1 can have only a finite number of rational solutions, (proving the Mordell's conjecture of 1922)."
>
> — *Gerd Faltings (1983)*

But unfortunately, as far as concrete computational algorithms are concerned, not much more than what we have described in this section is available in the current literature.

We conclude this section by giving a list of some of the major contributors to the theory of quadratic equations. But before giving the list, we expressly make it clear that our work will not go beyond the work of the mathematicians named in the beginning part of this section, and that the following list in no sense claims any kind of completeness — and moreover, not that we have included the names of the mathematicians only if they have done some computational contributions, but we have included them because of their contributions to the much more general theory of quadratic equations of which the computational quadratic theory is only an extremely tiny branch. We have done so only for the sake of a chronological chart.

Here is our list:

- Pythagoras (580 BC–500 BC)
- Archimedes (287 BC–212 BC)
- Diophantus (certainly lived sometime during 150 AD–250 AD; fl. during 250 AD, and died at the age of 84.)
- Aryabhatta I (476 AD–550 AD): Indeterminate equations; continued fractions.
- Bramhagupta (598 AD–665 AD): Bramha-Shupta-Siddhanta; arithmetic progressions; quadratic equations.

- Bhaskara II (1114 AD–1185 AD): Lilavati; Bijaganita; general solutions to Pell equations of the type: $x^2 = 1 + py^2$; solutions of first and second degree equations.
- Leonardo Fibonacci (also known as Leonardo Pisano) (1170 AD–after 1240 AD): *Liber Abaci* (1202); *Liber Quadratorum* (1225).
- Pierre de Fermat (8.17.1601–1.12.1665)
- John Pell (3.1.1611–1685)
- Leonhard Euler (4.15.1707–9.18.1783): Law of quadratic reciprocity (1783)
- Joseph-Louis Lagrange (1.25.1736–4.10.1813)
- Adrien-Marie Legendre (9.18.1752–1.10.1833)
- Karl Friedrich Gauss (4.30.1777–2.23.1855): *Disquisitiones Arithmeticæ* (1801)
- Karl Gustav Jacob Jacobi (12.10.1804–2.18.1851)
- Peter Gustav Lejeune Dirichlet (2.13.1805–5.5.1859)
- Charles Hermite (12.24.1822–1.14.1901): Solutions to quintic equations (1858); e is transcendental (1873)
- Ferdinand Gotthold Max Eisenstein (4.16.1823–10.11.1852)
- Henry John Stephen Smith (11.2.1826–2.9.1883)
- A. Meyer (Main publications relating to Quadratic Theory around the 1880's)
- Hermann Minkowski (6.22.1864–1.12.1909): Geometric theory of numbers
- Leonard Eugene Dickson (1.22.1874–1.17.1954)
- Srinivasa Ramanujan (12.22.1887–4.26.1920)
- Louis Joel Mordell (1.28.1888–1972)
- Helmut Hasse (1898–1979)
- Alaeksandr Osipovich Gelfond (10.24.1906–11.7.1968)

1.3 The Outline of This Dissertation

Here we are going to briefly expound the CONTENTS to this dissertation which preceded this chapter.

After giving the notations to be used in this dissertation in the first section of Chapter-2 and some general results about congruences in the next section, in the third chapter we have described a method of reduction which effectively reduces a general quadratic polynomial in any number of variables, homogeneous or not, to a diagonal one. This is done by reducing the coefficient matrix of the polynomial to a diagonal matrix. Even though the reduction by the matrix method is a very widely discussed concept, our reduction has some special advantage because of two reasons: first, the integrality of the reduced equation is retained in such a manner that the integer solutions of the reduced equation can directly be used for retracing the integer solutions of the original equation; and secondly, while reducing to the diagonal matrix a second upper triangular matrix is formed, which, playing a role similar to that of the coefficient matrix in the Cramer's rule for a linear system, when multiplied with a solution of the reduced equation, yields a solution of the original equation. We have not seen such an effective reduction process in the existing literature which yields the integer solutions of the original unreduced quadratic equation by a single matrix multiplication with a solution of the corresponding reduced equation.

After this reduction, we have presented a solution-generating-formula in §3.5, which, starting with any nontrivial solution of a homogeneous quadratic equation in any number of variables, has the potential to yield all the solutions of the equation under consideration.

Then in Chapter-4, after commenting that by the method of the previous chapter a general homogeneous ternary quadratic equation reduces to the Legendre's equation: $ax^2 + by^2 + cz^2 = 0$, with abc square-free, we have presented Dirichlet's proof of the Legendre's theorem which states that the above equation is nontrivially solvable in integers if and only if not all of a, b and c are with the same sign, and, $-bc$, $-ca$ and $-ab$ are quadratic residues of $|a|$, $|b|$ and $|c|$ respectively. From this proof of Dirichlet, which is slightly modified by us, we have extracted an algorithm for getting a nontrivial solution of the Legendre's equation whenever such a solution exists.

Then in the fifth chapter, we have presented a proof of the Holzer's theorem, which is essentially due to Mordell in (9). Our explanation of this proof is in a sense somewhat more complete because by using our solution-generating-formula of §3.5, we have avoided the mysterious and lengthy formulae for the parametric components which appeared all on a sudden in the beginning of Mordell's proof with absolutely no explanation about where they came from. Then out of this proof we have deduced an algorithm in §5.3, which, if necessary, can be applied on the Dirichlet's solution of Legendre's equation to reach a solution within the Holzer's range with

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ca|}, \quad \text{and} \quad |z| \leq \sqrt{|ab|}.$$

Then in §5.4 we have given a generalization of the Holzer's theorem, which gives

a range, here called the CM-range, for the equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$$

such that, whenever this equation is nontrivially solvable, it also must have a nontrivial solution within this CM-range. We have shown that the afore-mentioned Holzer's range is actually a particular case of this CM-range when $d = e = f = 0$. We have concluded this chapter with the presentation of an algorithm for getting a nontrivial solution within the CM-range whenever the above general ternary quadratic equation is nontrivially solvable.

Then in Chapter-6 we have shown that for a nontrivially solvable Legendre's equation: $ax^2 + by^2 + cz^2 = 0$, all of its integral solutions lying within the Holzer's range actually lie along a very small number of straightlinear rays emanating from the vertex of the double-cone which is the corresponding Euclidean graph of the given equation. Calling all these rays as the CM-rays, and those lying in the positive octant as the positive CM-rays, or PCM-rays, we have shown that the number of these PCM-rays is dependent on the numbers of distinct odd prime factors in the coefficients a, b and c. In fact we have given an upper bound for the number of these PCM-rays which solely depends on the numbers of odd prime factors in these coefficients. And by demonstrating some numerical examples in a later section, we have shown that this bound can in fact be attained, even though it is achievable very rarely in any randomly picked up Legendre's equation.

After giving an algorithm for detecting all the PCM-rays of the Legendre's equation, (and thereby also for all of its CM-rays), and then observing how to get some CM-rays of a nontrivially solvable general ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0,$$

in §6.7 we have presented our main result on PCM-rays in the form an inequality involving two functions, one representing the number of PCM-rays and the other determined by the odd prime factors of the coefficients a, b and c.

Then in the last section of the Chapter-6, we have presented a number of Legendre's Equations along with their PCM-rays in the form of some numerical tables.

We have concluded our work in chapter seven with some conjectures and some suggestions for future investigations, and finally, with a philosophical note of expectation that the CM-rays could possibly be occurring as living natural phonomena.

At the very end, we have appended this work with an autobiographical note which attempts to outline the genesis of this computational involvement that finally led to the discovery of these CM-rays.

1.4 Our Work In A Nutshell

In brief, we regard the following as our contribution to the computational quadratic theory:

1 . A new method of reduction for a general quadratic equation to a diagonal one, — and the simultaneous formation of a matrix which, starting with a solution of the reduced equation, yields a solution of the original equation by a single matrix multiplication.

2 . A solution-generating-matrix-formula to be applied on a nontrivial solution of a homogeneous quadratic equation in any number of variables in order to generate infinitely large number of solutions, in fact by (2), all the solutions of the equation in hand. This generating formula provides some plausible explanations about the origin of some of the lengthy and complicated but unexplained formulae used in Mordell's proof in (9) for the Holzer's theorem concerning the upper bound of the minimal solution of $ax^2 + by^2 + cz^2 = 0$.

3 . Extraction and modification of the Dirichlet's algorithm for finding a nontrivial solution of $ax^2 + by^2 + cz^2 = 0$ whenever this equation is nontrivially solvable.

4 . Extraction of the more precise Mordell's algorithm to reach at a solution within the Holzer's range whenever the Dirichlet's solution of $ax^2 + by^2 + cz^2 = 0$ is beyond that range.

5 . Generalization of the Holzer's theorem to the case of the ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$

6 . Introduction of the concepts of CM-rays, PCM-rays, and some corresponding computational algorithms, one of which is a very fast algorithm for finding the minimal nontrivial solution of a Legendre's equation: $ax^2 + by^2 + cz^2 = 0$ whenever such a solution exists.

7 . Finally, the inequality of §6.7, namely

$$PCM(a, b, c) \leq C(a, b, c),$$

in the context of the Legendre's equation: $ax^2 + by^2 + cz^2 = 0$.

1.5 While Concluding This Introduction

We feel like commenting on one singular advantage of the theory we have developed in Chapter-6. By analysing this theory one observes that in order to get the minimal solution of a Legendre's equation: $ax^2 + by^2 + cz^2 = 0$ one does not need the use of the algorithms of Dirichlet and Mordell. One could directly start with the algorithm presented in §6.5 which yields all the PCM-rays of any nontrivially solvable Legendre's equation, and then the finding of the minimal solution is accomplished by the obvious comparison of the bottom-most solutions along these rays. Thus we observe that finding the minimal nontrivial solution of a Legendre's equation being one of our primary objectives, though the investigation of the theorems of Legendre and Holzer were instrumental in reaching the new computational technique involving CM-rays, — once we get the theory of CM-rays in hand, we see that it stands independently by itself needing none of the theory which compelled its emergence. In that sense, by the time we achieve our intrinsic goal of reaching the minimal solution of a Legendre's equation, we find that a completely independent path has been created that is much more convenient and shorter than the one which actually led to our final destination. However, the lengthy path had a lot of nice things to offer.

Now, let us begin with the notations and the foundational results on which the exposition and the deductions of this thesis will depend.

Chapter 2

THE NOTATIONS AND THE TOOLS

2.1 The Goal

This chapter is going to outline the notations and the tools to be used in this dissertation. In §2.2 we are going to specify our notations and assumptions, and in §2.3 we will state some results relating to congruences, which directly or indirectly play an important role in substantiating the deductions in this work.

2.2 Notations and Assumptions

Unless expressly specified otherwise, apart from the very conventional ones in mathematics, the following are the notations and the restrictions we adopt for the purpose of writing this dissertation.

By an integer, we mean a rational integer.

By an integral equation we mean an equation whose coefficients are integers.

Unless otherwise stated, by a solution or by an integral solution we mean one in which the components are integers. By a nontrivial solution we mean a solution with at least one nonzero component.

By irrational we mean an irrational real number.

Unless stated otherwise, the upper and lower case letters used in any algebraic expression that are attached with no other symbols will stand for integers.

$\underline{A}$, $\underline{a}$, $\underline{B}$, $\underline{b}\cdots$: Letters with underbars will denote matrices.

$\underline{A}^T$ denotes the transpose of the matrix $\underline{A}$.

$\underline{A}^{-1}$ is the inverse of the matrix $\underline{A}$.

$Adj(\underline{A})$ denotes the adjoint of the matrix $\underline{A}$.

$D(\underline{A})$ denotes the determinant of the square matrix $\underline{A}$.

$\hat{A}$, $\hat{a}$, $\hat{B}$, $\hat{b}\cdots$: Letters with hats denote vectors or points in the Euclidean space.

By squares, cubes, ...we mean squares, cubes, ...of integers.

$\mathbb{Z}$ = The set of rational integers.

$\mathbb{Q}$ = The set of rationals.
$\mathbb{R}$ = The set of reals.
$\mathbb{C}$ = The set of complex numbers.
If $\mathbb{X}$ represents either $\mathbb{Z}$, or $\mathbb{Q}$, or $\mathbb{R}$, then

$$\mathbb{X}^n = \underbrace{\mathbb{X} \times \mathbb{X} \times \cdots \mathbb{X}}_{n \text{ factors}} = \{(x_1, x_2, \ldots x_n) \mid x_i \in \mathbb{X} \quad \forall i\};$$

$$\mathbb{X}^{(m)} = \{x^m \mid x \in \mathbb{X}\};$$
$$\mathbb{X}_+ = \{x \mid x \in \mathbb{X} \text{ and } x \geq 0\};$$
$$\mathbb{X}_- = \{x \mid x \in \mathbb{X} \text{ and } x \leq 0\};$$
$$\mathbb{X}_* = \mathbb{X} - \{0\};$$
$$\mathbb{X}_{+*} = \mathbb{X}_+ - \{0\};$$
$$\mathbb{X}_{-*} = \mathbb{X}_- - \{0\}.$$

$\{a, b, c, \cdots\}$ will represent the set of elements $a, b, c, \cdots$.

Given a set $\{a, b, c, \ldots\}$, the symbols 'max$\{a, b, c, \ldots\}$' and 'min$\{a, b, c, \ldots\}$' will represent its maximum and minimum respectively.

$(a_1, a_2, \ldots, a_n)$ will represent an element of the above $\mathbb{X}^n$ or a point in the n-dimensional Euclidean space.

$[a_1, a_2, \ldots, a_n]$ will represent a vector, or a solution for an equation in n-variables: $x_1, x_2, \ldots, x_n$.

$[a_1 \quad a_2 \ldots a_n]$ will represent an $1 \times n$-matrix. (Note that the commas separating the components of a vector are absent in the case of a matrix.)

If $\hat{A}$ or A is a solution, or a vector, or a point in the Euclidean space, then $\underline{A}$ will represent the corresponding row-matrix.

If any of X, Y and M is an element of the above $\mathbb{X}^n$, or a vector, or a row- or column-matrix whose entries are elements of $\mathbb{X}$, and is with n components in it, k is an element of the $\mathbb{X}$, $C_i(X)$ represents the i-th component of X, $\odot$ is a binary composition and $\bowtie$ is a binary relation over $\mathbb{X}$, then we will adopt the following notational conventions:

$$k \odot X \text{ is of type } X, \text{ with } \quad C_i(k \odot X) = k \odot C_i(X) \quad \forall i.$$
$$X \odot Y \text{ is of type } Y, \text{ with } \quad C_i(X \odot Y) = C_i(X) \odot C_i(Y) \quad \forall i.$$
$$k \bowtie X \Leftrightarrow k \bowtie C_i(X) \quad \forall i.$$
$$X \bowtie Y \Leftrightarrow C_i(X) \bowtie C_i(Y) \quad \forall i, \quad \text{e.g.}$$
$$X \equiv Y \pmod{M} \quad \Leftrightarrow \quad C_i(X) \equiv C_i(Y) \pmod{C_i(M)} \quad \forall i.$$

Note that in any of the above algebraic expressions, X could be an n-tuple, Y could be an n-vector and M could be an $1 \times n$-matrix, or vice versa; but of course they should have the same number of components.

Since we are not going to use two-digited subscripts anywhere, we will be freely using the convention such as $a_{11} = a_{1,1}$, and $a_{ij} = a_{i,j}$, and etc.

$\lfloor x \rfloor$, for $x \in \mathbb{R}$, represents the greatest integer, not exceeding x; and,
$\lceil x \rceil$ represents the smallest integer not smaller than x.

$a|b$ means a divides b, and

$a \not| b$ means a does not divide b.

The word *gcd* will be the abbreviation of greatest common divisor.

The word *lcm* will be the abbreviation of least common multiple.

$G(a, b, c, \cdots)$ will denote the *gcd* of $a, b, c, \cdots$.

$L(a, b, c, \cdots)$ will denote *lcm* of $a, b, c, \cdots$.

With c, j, k, l, r, s and t as integers, $(\underline{l})$ will denote the l-th enumerated entity within a section, say the s-th section of the c-th chapter, where this entity may be either an algebraic expression or a statement, such as: an equation, or inequality, or a congruence, or the statement of a theorem or lemma, or a definite sentence or phrase making any assertion. When this entity will be referred to in the k-th section, (different from the s-th section, but within the same c-th chapter in which it occurs), it will be referred to as $(\underline{s.l})$. And when it will be referred to in the k-th section of the j-th chapter, (different from the c-th), it will be referred to as $(\underline{c.s.l})$. The notation $(\underline{l,q,r,t})$ with integers separated by commas, will represent the four entities $(\underline{l})$, $(\underline{q})$, $(\underline{r})$ and $(\underline{t})$ of the same section in which the notation appears.

The k-th enumerated local-entity of a theorem-like environment within a section will be denoted by the symbol $((\underline{k}))$, without affecting the global enumeration of the section which is denoted by the symbol: $(\underline{l})$.

(i), an integer i within a pair of parentheses but with no underbar, will denote the i-th item listed in the bibliography at the end.

§5.2 will denote Section 2 of Chaper 5.

If the congruences: $a \equiv b \pmod{c}$ and $d \equiv e \pmod{c}$ are equivalent, we write:

$$a \equiv b \pmod{c} \approx d \equiv e \pmod{c}.$$

Also if the equations : $f(x) = 0$ and $g(x) = 0$ are isomorphic, (meaning, have identical solutions), we write $f(x) = 0 \approx g(x) = 0$.

Φ will denote the empty set.

The symbol: $\vdash$ within a mathematical statement will stand for the word: 'when', 'where' or 'for', whichever is appropriate.

The symbol: ' & ' will stand for the word: 'and'.

$a \sim b$ will denote the positive difference between the real numbers a and b, i.e., $a \sim b = | \, |a| - |b| \, |$, where $|a|$ denotes the absolute value of a.

$\#(A)$ will denote the cardinality of the set A.

$\square$ will denote the end of a proof.

2.3 Congruences

In this section we intend to recollect some basic facts relating to congruences which are directly or indirectly helpful in the deduction or the computation of some of the results in this work.

For integers a, b and m, the mathematical statement " $a \equiv b \pmod{m}$ " is read as " a is congruent to b modulo m ", which means that $a - c = km$ for some $k \in \mathbb{Z}$. In this case we call this m as the modulus. And note that

$$a \equiv b \pmod{0} \Leftrightarrow a = b,$$

and

$$c \equiv d \pmod{1} \quad \forall c, d \in \mathbb{Z}.$$

Moreover,

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a \equiv b \pmod{-m},$$

so that there is no harm in taking a negative integer as a modulus for any congruence. However, since there is no difference, unless stated otherwise, we will assume a modulus to be positive. Now it is easy to check that this congruence relation modulo any fixed integer is an equivalence relation over $\mathbb{Z}$. And when we have the congruence of two fixed integers with respect to two or more moduli m_i with $i = 1, 2, \ldots, k$, it is easy to see that the following is true:

$$a \equiv b \pmod{m_i} \quad \forall i \in \{1, 2, \ldots k\} \quad \Leftrightarrow \quad a \equiv b \pmod{L(m_1, \ldots, m_k)}, \qquad (\underline{1})$$

If $*$ is a binary operation over a subset of $\mathbb{Z}$, let us define an induced binary operation over the collection C_m of congruences modulo m by:

$$(a \equiv b \pmod{m}) * (c \equiv d \pmod{m}) \Leftrightarrow a * c \equiv b * d \pmod{m},$$

whenever $a * c$ and $b * d$ are well-defined.

It is easy to see that the usual addition, subtraction and multiplication of reals induce obvious binary operations over C_m, whereas the usual division does not. However, with some restriction on the congruence which acts as the divisor, we can define a division over C_m . In fact with c and d as divisors of both a and b respectively, the division given by:

$$(a \equiv b \pmod{m}) \div (c \equiv d \pmod{m}) \Leftrightarrow (a \div c \equiv b \div d \pmod{(m \div G(c, d, m))})$$

is well-defined.

By $\frac{a}{b} \equiv c \pmod{m}$, we will mean $a \equiv bc \pmod{m}$. Note that with what we have described, the two expressions: $\frac{a}{b}$ and $a \div b$, represent different entities within congruences.

By $\sqrt[n]{a} \equiv b \pmod{m}$ we mean $b^n \equiv a \pmod{m}$.

In particular,

$$\sqrt{a} \equiv b \pmod{m} \quad \Leftrightarrow \quad b^2 \equiv a \pmod{m}.$$

In this later case we say that a is a quadratic residue of m .

For two polynomials $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$ and $g(x) = \sum_{j=0}^{s} b_j x^{s-j}$ with $n \leq s$, we say that $f(x) \equiv g(x) \pmod{m}$ if and only if $a_i \equiv b_i \pmod{m}$ for $0 \leq i \leq n$ and $b_j \equiv 0 \pmod{m}$ for $n < j \leq s$. Now it is easy to see that if $f(x)$ is congruent to $g(x)$ modulo m , then

$$a \equiv b \pmod{m} \Rightarrow f(a) \equiv g(b) \pmod{m}.$$

For the polynomial $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$, we define the degree of $f(x)$ modulo m as $\max\{n - i \mid a_i \not\equiv 0 \pmod{m}\}$.

Now let us recollect some standard results in the context of congruences.

If ϕ is the Euler-function, so that for a positive integer n, $\phi(n)$ represents the number of positive integers smaller than n which are relatively prime to n, then:

Euler's Theorem. *For* $G(a, n) = 1$, $\quad a^{\phi(n)} \equiv 1 \pmod{n}$. (2)

Wilson's Theorem. *For a prime* p, $\quad (p-1)! \equiv -1 \pmod{p}$ (3)

Solutions of a Linear Congruence. *If* $G(a, m) = g$, *then* $ax \equiv b \pmod{m}$ *is solvable if and only if* $g|b$, *and moreover, when solvable, the number of distinct solutions modulo* m *for this linear congruence is* g *which are given by*

$$x = (bx_0 + tm) \div g \pmod{m} \quad \textit{with} \quad t = 0, 1, \ldots, g-1,$$

where x_0 *is any solution of* $(a \div g)x \equiv 1 \pmod{m \div g}$, *and in particular, (by Euler's Theorem), could be taken as* $(a \div g)^{\phi(m \div g)-1}$ *modulo* $m \div g$. (4)

Chinese Remainder Theorem on Systems of Linear Congruences. *The system of* k *congruences:*

$$x \equiv a_i \pmod{m_i}, \quad \vdash \quad i = 1, 2, \ldots, k \quad \textit{with } G(m_i, m_j) = 1 \textit{ for } i \neq j$$

has a unique solution modulo $M = m_1 m_2 \ldots m_k$ *which is given by*

$$\sum_{i=1}^{k} a_i M_i x_i \pmod{M}$$

where $M_i = \frac{M}{m_i}$ *modulo* m_i, *and* x_i *is a solution of* $M_i x \equiv 1 \pmod{m_i}$, *which, by Euler's Theorem, could be taken as* $M_i^{\phi(m_i)-1}$ *modulo* m_i. (5)

A Theorem on Prime-Power Modulus. *For a polynomial* $f(x)$ *and a prime* p, *both* $f(x) \equiv 0 \pmod{p}$ *and* $f(x) \equiv 0 \pmod{p^\alpha}$ *with* α *as any positive integer, have the same number of solutions.* (6)

A Theorem on the Number of Solutions of a Polynomial Congruence. *If* $m_0 = m_1 m_2 \dots m_k$ *with* $G(m_i, m_j) = 1$ *for* $i \neq j$, *then for a polynomial* $f(x)$, *the congruence* $f(x) \equiv 0 \pmod{m_0}$ *is equivalent to the system*

$$f(x) \equiv 0 \pmod{m_i}, \quad \vdash \quad i = 1, 2, \dots, k.$$

Moreover, if T_i *represents the number of solutions of the congruence*

$$f(x) \equiv 0 \pmod{m_i},$$

then $T_0 = T_1 T_2 \dots T_k$. (7)

RELATING TO QUADRATIC CONGRUENCES:

In the context of a quadratic congruence $x^2 \equiv a \pmod{m}$, let us define the symbol $\left\|\frac{a}{m}\right|$ as follows:

$$\left\|\frac{a}{m}\right| = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{m} \text{ is solvable} \\ -1 & \text{otherwise.} \end{cases} \tag{8}$$

Note that for $m = 0$, $\left\|\frac{a}{m}\right| = 1$ if and only if $a = 0$; and for $m \in \{1, -1, 2, -2\}$, $\left\|\frac{a}{m}\right| = 1 \quad \forall a \in \mathbb{Z}$. Also $\forall m \in \mathbb{Z}_*$, whenever a is 1 or a multiple of m, obviously $\left\|\frac{a}{m}\right| = 1$.

One of the most fundamental results relating to quadratic congruences is:

The Law of Quadratic Reciprocity. *If* p *and* q *are odd primes, then*

$$\left\|\frac{p}{q}\right| = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left\|\frac{q}{p}\right|.$$

Thus, only when both p *and* q *are of the form* $4m+3$, *we have* $\left\|\frac{p}{q}\right| = -\left\|\frac{q}{p}\right|$, *otherwise* $\left\|\frac{p}{q}\right| = \left\|\frac{q}{p}\right|$. (9)

Also in this context we have the following important result regarding the number of solutions of a given quadratic congruence:

A Theorem on Number of Solutions of Quadratic Congruences. *Given* $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *as the canonical prime factorization of* m, *the necessary and sufficient conditions for the solvability of* $x^2 \equiv a \pmod{m}$ *with* $G(a, m) = 1$ *are:*

$$(i) \quad a \equiv \begin{cases} 1 \pmod 4 & \text{for } \alpha = 2 \\ 1 \pmod 8 & \text{for } \alpha \geq 3; \end{cases}$$

and, $$(ii) \quad \left\|\frac{a}{p_i}\right| = 1 \qquad \vdash i = 1, 2, \dots, k.$$

Moreover, when solvable, the number n of distinct solutions modulo m for the above congruence is given by:

$$n = \begin{cases} 2^k & \text{for } \alpha = 0 \text{ or } 1 \\ 2^{k+1} & \text{for } \alpha = 2 \\ 2^{k+2} & \text{for } \alpha \geq 3. \end{cases} \tag{10}$$

In the following we list some more specific results relating to quadratic congruences, where we assume p to be a prime, a to be nonzero and relatively prime to p, and m to be an arbitrary integer.

Euler's Criterion. $\left\|\frac{a}{p}\right| \equiv a^{\frac{p-1}{2}} \pmod{p}$. (11)

A Decomposition Theorem. $\left\|\frac{a_1 a_2 \ldots a_k}{p}\right| = \prod_{i=1}^{k} \left\|\frac{a_i}{p}\right|$. (12)

Corollary. $\left\|\frac{ab^2}{p}\right| = \left\|\frac{a}{p}\right|$. (13)

Theorem. $\left\|\frac{-1}{p}\right| = 1 \Leftrightarrow p$ *is of the form* $4m + 1$. (14)

Theorem. $\left\|\frac{2}{p}\right| = 1 \Leftrightarrow p$ *is of the form* $8m + 1$ *or* $8m - 1$. (15)

Theorem. $\left\|\frac{-2}{p}\right| = 1 \Leftrightarrow p$ *is of the form* $8m + 1$ *or* $8m + 3$. (16)

Theorem. *With* $|a| = 3$, *we have* $\left\|\frac{a}{p}\right| = 1 \Leftrightarrow p$ *is of the form* $6m + 1$. (17)

Gauss's Lemma. *If with respect to the modulus p, s is the number of least positive residues of the integers a, 2a, 3a, ... and* $\frac{p-1}{2}a$ *that are greater than* $\frac{p}{2}$, *then*

$$\left\|\frac{a}{p}\right| = (-1)^s. \tag{18}$$

The list of these results could be extended to make it much larger. But we restrain from that, and start the process of reduction in the following chapter which is the actual beginning of our work.

Chapter 3

REDUCTION OF QUADRATIC EQUATIONS AND A SOLUTION-GENERATING FORMULA

3.1 The Goal

The homogeneous ternary quadratic equation which we intend to deal with is rather a simple particular case of a much more general quadratic equation:

$$\mathcal{P}(x_1, x_2, \ldots, x_n) = \sum_{\substack{i,j=1 \\ i \leq j}}^{n} (a_{ij}x_ix_j + a_ix_i) + a = 0.$$

Naturally an initial step in solving this equation is to see if this can be simplified to another equation which is somewhat easier to handle. This is our major goal in this chapter. In fact we are going to associate $\mathcal{P}$ to a diagonal form:

$$\tilde{\mathcal{Q}}(u_1, u_2, \ldots, u_n) = \sum_{i=1}^{n} q_iu_i^2$$

such that the nontrivial zeroes of $\tilde{\mathcal{Q}}$ eventually yield solutions to $\mathcal{P} = 0$. This process of association may, in a sense, be called as *reduction.*

After this goal is achieved in §3.3, briefly we will suggest in § 3.4 how starting with a solution of the reduced equation one could retrace a solution of the original unreduced equation. Then we will present a formula in § 3.5, which can be applied on a single nontrivial solution of a homogeneous quadratic equation to generate theoretically all of its solutions. We will conclude this chapter in § 3.6 with some remarks on the results in this chapter.

3.2 The Setting

Since the above $\mathcal{P}(x_1, x_2, \ldots, x_n)$ can be regarded as the form:

$$\mathcal{P}(x_1, x_2, \ldots, x_n) = \sum_{\substack{i,j=1 \\ i \le j}}^{n} (a_{ij}x_ix_j + a_ix_iu) + au^2 = 0.$$

evaluated at $u = 1$, clearly we can consider only the problem of reducing a quadratic form:

$$\mathcal{Q}(x_1, x_2, \ldots, x_n) = \sum_{\substack{i,j=1 \\ i \le j}}^{n} a_{ij}x_ix_j$$

with no linear or constant terms. If $\underline{x} = [x_1\, x_2\, \ldots\, x_n]$ is a row matrix, $\underline{x}^T$ is its transpose, and $\underline{A}$ is the $n \times n$-matrix given by

$$\underline{A} = \begin{bmatrix} 2a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & 2a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & 2a_{n2} & \cdots & 2a_{nn} \end{bmatrix}$$

where we assume $a_{ij} = a_{ji} \quad \forall i, j$, then clearly $\underline{x}\,\underline{A}\,\underline{x}^T = 2\mathcal{Q}$. We call $\underline{A}$ as the matrix of the form $\mathcal{Q}$, (which actually, more accurately speaking, represents $2\mathcal{Q}$).

Let, for any $i \in \mathbb{Z}$ with $1 \le i \le n$, $\underline{A}_i$ denote the top left corner submatrix of $\underline{A}$ of dimension $i \times i$:

$$\underline{A}_i = \begin{bmatrix} 2a_{11} & a_{12} & \cdots & a_{1i} \\ a_{21} & 2a_{22} & \cdots & a_{2i} \\ \vdots & & & \vdots \\ a_{i1} & a_{i2} & \cdots & 2a_{ii} \end{bmatrix}.$$

Let $\underline{A}_{i,j}$ with $j > i$ denote the $i \times i$-matrix formed by the intersectional elements of the top i rows, first $i - 1$ columns and the j-th column of $\underline{A}$. And let

$$\underline{A}_{i;r_1,r_2,\ldots,r_i;c_1,c_2,\ldots,c_i}$$

denote the $i \times i$ submatrix of $\underline{A}$ formed by the intersectional elements of the rows: $r_1, r_2, \ldots, r_i$ and the columns $c_1, c_2 \ldots, c_i$. For $(r_1, r_2, \ldots, r_i) = (c_1, c_2 \ldots, c_i)$, let $A_{i;r_1,r_2,\ldots,r_i;c_1,c_2,\ldots,c_i}$ be denoted by $A_{i;r_1,r_2,\ldots,r_i}$. For matrices $\underline{A}$, $\underline{A}_i$, $\underline{A}_{i,j}$ and $\underline{A}_{i;r_1,r_2,\ldots,r_i;c_1,c_2,\ldots,c_i}$, let $\underline{A}_{(r,s)}$, $\underline{A}_{i(r,s)}$, $\underline{A}_{i,j(r,s)}$ and $\underline{A}_{i;r_1,r_2,\ldots,r_i;c_1,c_2,\ldots,c_i(r,s)}$ respectively represent their submatrices obtained by deleting their r-th rows and s-th columns, and for any of these square submatrices of $\underline{A}$ let us denote its determinant by replacing the A in its name by M, e.g., we will denote the determinants of $\underline{A}$, $\underline{A}_{i,j}$ and $\underline{A}_{k(r,s)}$ by M, $M_{i,j}$ and $M_{k(r,s)}$ respectively. Note that according to our notation, $M_{(r,s)}$ is the first order minor of the determinant of $\underline{A}$ at the position (r, s).

Before we start looking at the process of reduction, let us recall a result on matrices:

LEMMA. *If $\underline{A}$ is an $n \times n$ matrix over integers, then*

$$M_{(n-1,n-1)}.M_{(n,n)} - M_{(n-1,n)}.M_{(n,n-1)} = M.M_{n-2} \tag{1}$$

Proof Refer (12). □

The above result in fact is going to help us immensely in accomplishing our immediate goal. Now let us look for the process of reduction.

3.3 The Reduction

Since the underlying proof of the process which we discovered is somewhat messy, let us try to lay out the plan for the reduction briefly.

First we are going to rearrange the terms of $\mathcal{Q}$ into subsets of terms, each of these subsets absorbing one variable completely such that each time a variable is completely absorbed, it does not appear any more in any of the terms in the succeeding subsets. We manage the absorption of variables in a systematic manner starting with x_1, and then continuing with $x_2, x_3, \ldots$ etc., up to x_n successively. Then we try to apply the method of completing the squares successively on these subsets, and by the time we are through with all the subsets in completing the squares, we are with an array of subsets of terms, out of which pop out the coefficients of the diagonal form exactly equal to $\mathcal{Q}$. Now, let us start the actual process.

Let $\mathcal{Q} = \mathcal{Q}_0 = \mathcal{Q}_{0,0}$. Then,

$$\begin{aligned}
\mathcal{Q}_0 &= \sum_{\substack{i,j=1 \\ i \le j}}^{n} a_{ij}x_ix_j \\
&= \left[a_{11}x_1^2 + x_1\sum_{j=2}^{n} a_{1j}x_j\right] + \left[a_{22}x_2^2 + x_2\sum_{j=3}^{n} a_{2j}x_j\right] + \cdots\cdots + \\
&\quad \left[a_{n-1,n-1}x_{n-1}^2 + a_{n-1,n}x_{n-1}x_n\right] + a_{n,n}x_n^2 \\
&= \sum_{i=1}^{n}\left[a_{ii}x_i^2 + x_i\sum_{j=i+1}^{n} a_{ij}x_j\right] \\
&= \sum_{i=1}^{n}\mathcal{Q}_{0,i},
\end{aligned}$$

where $\mathcal{Q}_{0,i}$ denotes

$$a_{ii}x_i^2 + x_i\sum_{j=i+1}^{n} a_{ij}x_j.$$

While writing these equations we assume that whenever any of the suffixes turns to a value larger than n, the corresponding term is zero, i.e., nonexistent in the expression.

Now,

$$\begin{aligned}
\mathcal{Q}_{0,1} &= a_{11}x_1^2 + x_1\sum_{j=2}^{n} a_{1j}x_j \\
&= a_{11}\left[x_1^2 + 2x_1\frac{\sum_{j=2}^{n} a_{1j}x_j}{2a_{11}} + \left(\frac{\sum_{j=2}^{n} a_{1j}x_j}{2a_{11}}\right)^2 - \left(\frac{\sum_{j=2}^{n} a_{1j}x_j}{2a_{11}}\right)^2\right] \\
&= \frac{1}{4a_{11}}\left[2a_{11}x_1 + \sum_{j=2}^{n} a_{1j}x_j\right]^2 - \frac{1}{4a_{11}}\left(\sum_{j=2}^{n} a_{1j}x_j\right)^2 \\
&= \frac{1}{4a_{11}}\left[\sum_{i=1}^{n} M_{1,i}x_i\right]^2 - \frac{1}{4a_{11}}\left(a_{12}^2x_2^2 + 2a_{12}x_2\sum_{j=3}^{n} a_{1j}x_j\right) \\
&\quad -\frac{1}{4a_{11}}\left(a_{13}^2x_3^2 + 2a_{13}x_3\sum_{j=4}^{n} a_{1j}x_j\right) \\
&\quad \cdots \\
&\quad -\frac{1}{4a_{11}}\left(a_{1,n-1}^2x_{n-1}^2 + 2a_{1,n-1}x_{n-1}a_{1,n}x_n\right) \\
&\quad -\frac{1}{4a_{11}}a_{1,n}^2x_n^2 \\
&= \frac{1}{4a_{11}}\left[\sum_{i=1}^{n} M_{1,i}x_i\right]^2 - \frac{1}{4a_{11}}\sum_{j=2}^{n}\left(a_{1j}^2x_j^2 + 2a_{1j}x_j\sum_{k=j+1}^{n} a_{1k}x_k\right) \\
&= \mathcal{Q}_{1,1} + \mathcal{Q}_{1,2} + \mathcal{Q}_{1,3} + \cdots + \mathcal{Q}_{1,n} \\
&= \sum_{j=1}^{n} \mathcal{Q}_{1,j},
\end{aligned}$$

where

$$\mathcal{Q}_{1,1} = \frac{1}{4a_{11}}\left[\sum_{i=1}^{n} M_{1,i}x_i\right]^2,$$

and for $j > 1$

$$Q_{1,j} = \frac{-1}{4a_{11}}\left(a_{1j}^2x_j^2 + 2a_{1j}x_j\sum_{k=j+1}^{n} a_{1k}x_k\right).$$

Now let us denote $\sum_{j=1}^{n} \mathcal{Q}_{1,j}$ by $\mathcal{Q}_1$.

Before proceeding further, let us note that all the x_1's are absorbed in $\mathcal{Q}_{11}$ which is in the form of the square of a linear expression, and, none of the terms in the remaining

$$\mathcal{Q}_{0,2}, \mathcal{Q}_{0,3}, \ldots, \mathcal{Q}_{0,n}, \mathcal{Q}_{1,2}, \mathcal{Q}_{1,3}, \ldots, \mathcal{Q}_{1,n}$$

involve x_1 any more. Our next step is to accomplish a similar objective for x_2.

Since beyond $\mathcal{Q}_{1,1}$, all the terms involving x_2 are limited to $\mathcal{Q}_{0,2}$ and $\mathcal{Q}_{1,2}$, let us concentrate on $\mathcal{Q}_{0,2} + \mathcal{Q}_{1,2}$, which we denote as $\mathcal{Q}_2$. Thus

$$
\begin{aligned}
\mathcal{Q}_2 &= \mathcal{Q}_{0,2} + \mathcal{Q}_{1,2} \\
&= \left[a_{22}x_2^2 + x_2\sum_{j=3}^{n} a_{2j}x_j\right] - \frac{1}{4a_{11}}\left[a_{12}^2x_2^2 + 2a_{12}x_2\sum_{j=3}^{n} a_{1j}x_j\right] \\
&= \left[\left(a_{22} - \frac{a_{12}^2}{4a_{11}}\right)x_2^2 + 2x_2\sum_{j=3}^{n}\left(\left(\frac{a_{2j}}{2} - \frac{a_{12}a_{1j}}{4a_{11}}\right)x_j\right)\right] \\
&= \left[\frac{4a_{11}a_{22} - a_{12}^2}{4a_{11}}x_2^2 + 2x_2\sum_{j=3}^{n}\left(\frac{2a_{11}a_{2j} - a_{21}a_{1j}}{4a_{11}}x_j\right)\right] \\
&\quad (\text{since } a_{12} = a_{21}) \\
&= \frac{1}{4a_{11}}\left[M_2x_2^2 + 2x_2\sum_{j=3}^{n} M_{2,j}x_j\right] \\
&= \frac{M_2}{4a_{11}}\left[x_2^2 + 2x_2\left(\frac{\sum_{j=3}^{n} M_{2,j}x_j}{M_2}\right) + \left(\frac{\sum_{j=3}^{n} M_{2,j}x_j}{M_2}\right)^2 - \left(\frac{\sum_{j=3}^{n} M_{2,j}x_j}{M_2}\right)^2\right] \\
&= \frac{M_2}{4a_{11}M_2^2}\left[M_2x_2 + \sum_{j=3}^{n} M_{2,j}x_j\right]^2 - \frac{M_2}{4a_{11}M_2^2}\left[\sum_{j=3}^{n} M_{2,j}x_j\right]^2 \\
&= \frac{1}{2M_1M_2}\left[\sum_{j=2}^{n} M_{2,j}x_j\right]^2 - \frac{1}{2M_1M_2}\left[\sum_{j=3}^{n} M_{2,j}x_j\right]^2 \\
&\quad (\text{since } M_2 = M_{2,2}) \\
&= \frac{1}{2M_1M_2}\left[\sum_{j=2}^{n} M_{2,j}x_j\right]^2 - \frac{1}{2M_1M_2}\sum_{i=3}^{n}\left(M_{2,i}^2x_i^2 + 2M_{2,i}x_i\sum_{j=i+1}^{n} M_{2,j}x_j\right) \\
&= \mathcal{Q}_{2,2} + \sum_{i=3}^{n}\mathcal{Q}_{2,i}
\end{aligned}
$$

where

$$\mathcal{Q}_{2,2} = \frac{1}{2M_1M_2}\left[\sum_{j=2}^{n} M_{2,j}x_j\right]^2$$

and for $i > 2$

$$\mathcal{Q}_{2,i} = \frac{-1}{2M_1M_2}\left(M_{2,i}^2x_i^2 + 2M_{2,i}x_i\sum_{j=i+1}^{n} M_{2,j}x_j\right)$$

Here $\mathcal{Q}_{22}$ absorbs all the x_2's beyond $\mathcal{Q}_{1,1}$ in the square of a linear expression, and there are no more x_2's involved in any of the terms of $\mathcal{Q}$ away from $\mathcal{Q}_{1,1}$ and $\mathcal{Q}_{2,2}$.

Proceeding as in the above, we propose the following step by step presentation:

$$\begin{array}{rcll}
\mathcal{Q}_0 & = & \mathcal{Q}_{0,0} = \mathcal{Q}_{0,1} + \mathcal{Q}_{0,2} + \mathcal{Q}_{0,3} + \mathcal{Q}_{0,4} + \cdots & \cdots + \mathcal{Q}_{0,n-2} + \mathcal{Q}_{0,n-1} + \mathcal{Q}_{0,n} \\
\mathcal{Q}_1 & = & \mathcal{Q}_{0,1} = \mathcal{Q}_{1,1} + \mathcal{Q}_{1,2} + \mathcal{Q}_{1,3} + \mathcal{Q}_{1,4} + \cdots & \cdots + \mathcal{Q}_{1,n-2} + \mathcal{Q}_{1,n-1} + \mathcal{Q}_{1,n} \\
\mathcal{Q}_2 & = & \mathcal{Q}_{0,2} + \mathcal{Q}_{1,2} = \mathcal{Q}_{2,2} + \mathcal{Q}_{2,3} + \mathcal{Q}_{2,4} + \cdots & \cdots + \mathcal{Q}_{2,n-2} + \mathcal{Q}_{2,n-1} + \mathcal{Q}_{2,n} \\
\mathcal{Q}_3 & = & \mathcal{Q}_{0,3} + \mathcal{Q}_{1,3} + \mathcal{Q}_{2,3} = \mathcal{Q}_{3,3} + \mathcal{Q}_{3,4} + \cdots & \cdots + \mathcal{Q}_{3,n-2} + \mathcal{Q}_{3,n-1} + \mathcal{Q}_{3,n} \\
\mathcal{Q}_4 & = & \mathcal{Q}_{0,4} + \mathcal{Q}_{1,4} + \mathcal{Q}_{2,4} + \mathcal{Q}_{3,4} = \mathcal{Q}_{4,4} + \cdots & \cdots + \mathcal{Q}_{4,n-2} + \mathcal{Q}_{4,n-1} + \mathcal{Q}_{4,n} \\
 & \vdots & & \\
\mathcal{Q}_n & = & \mathcal{Q}_{0,n} + \mathcal{Q}_{1,n} + \mathcal{Q}_{2,n} + \mathcal{Q}_{3,n} + \mathcal{Q}_{4,n} + \cdots & \cdots + \mathcal{Q}_{n-2,n} + \mathcal{Q}_{n-1,n} = \mathcal{Q}_{n,n}
\end{array}$$

in which any $\mathcal{Q}_{i,j}$, in the i-th level of the above presentation, with of course $i \leq j$, is such that any $\mathcal{Q}_{i,k}$ in the right-most expression of that same i-th level but with $k > j$, does no further involve x_j in any of its terms.

Now we claim the following:

THEOREM. *If $M_i \neq 0 \quad \forall i$, then*

a) $\mathcal{Q} = \sum_{i=1}^{n} \mathcal{Q}_{i,i}$, where $\mathcal{Q}_{i,i} = \dfrac{1}{2M_{i-1}M_i}\left[\sum_{j=i}^{n} M_{i,j}x_j\right]^2$, with $M_0 = 1$ and M_i, $M_{i,j}$ as defined earlier ;

b) and for a fixed i and any $j > i$,

$$\mathcal{Q}_{i,j} = \frac{-1}{2M_{i-1}M_i}\left[M_{i,j}^2 x_j^2 + 2M_{i,j}x_j \sum_{k=j+1}^{n}(M_{i,k}x_k)\right]. \tag{1}$$

Proof: Looking at the above array of $\mathcal{Q}_{i,j}$'s, it is clear that $\mathcal{Q} = \sum_{i=1}^{n} \mathcal{Q}_{i,i}$. So for proving the first part of the theorem, it is remains to prove that

$$\mathcal{Q}_{i,i} = \frac{1}{2M_{i-1}M_i}\left[\sum_{j=i}^{n} M_{i,j}x_j\right]^2, \quad \text{with} \quad M_0 = 1.$$

Let us prove it by induction on i. According to the given scheme, $\mathcal{Q}_{i,i}$ is the sum of all the terms involving x_i in $\mathcal{Q}_i = \mathcal{Q}_{0,i} + \mathcal{Q}_{1,i} + \mathcal{Q}_{2,i} + \ldots + \mathcal{Q}_{i-1,i}$ presented in the form of the square of a linear expression involving $x_i, x_{i+1}, \ldots, x_n$. Now, by the inductive hypothesis, we have

$$\begin{aligned}
\mathcal{Q}_i &= \mathcal{Q}_{0,i} + \mathcal{Q}_{1,i} + \mathcal{Q}_{2,i} + \ldots + \mathcal{Q}_{i-1,i} \\
&= \left[a_{i,i}x_i^2 + x_i \sum_{j=i+1}^{n}(a_{ij}x_j)\right] \\
&\quad -\frac{1}{4a_{1,1}}\left[a_{1,i}^2 x_i^2 + 2a_{1,i}x_i \sum_{j=i+1}^{n}(a_{1,j}x_j)\right] \\
&\quad -\frac{1}{2M_1M_2}\left[M_{2,i}^2 x_i^2 + 2M_{2,i}x_i \sum_{j=i+1}^{n}(M_{2,j}x_j)\right]
\end{aligned}$$

$$-\frac{1}{2M_2M_3}\left[M_{3,i}^2x_i^2+2M_{3,i}x_i\sum_{j=i+1}^{n}(M_{3,j}x_j)\right]$$

$$\vdots$$

$$-\frac{1}{2M_{i-2}M_{i-1}}\left[M_{i-1,i}^2x_i^2+2M_{i-1,i}x_i\sum_{j=i+1}^{n}(M_{i-1,j}x_j)\right].$$

Thus the coefficient of x_i^2 in $\mathcal{Q}_i$ is

$$\begin{aligned}
&\left[a_{ii}-\frac{a_{1i}^2}{2M_1}-\frac{M_{2,i}^2}{2M_1M_2}-\frac{M_{3,i}^2}{2M_2M_3}-\cdots-\frac{M_{i-1,i}^2}{2M_{i-2}M_{i-1}}\right]\\
=&\ \frac{1}{2}\left[\frac{2M_1a_{i,i}-a_{1,i}^2}{M_1}-\sum_{k=2}^{i-1}\frac{M_{k,i}^2}{M_{k-1}M_k}\right]\\
=&\ \frac{1}{2}\left[\frac{M_{2;1,i;i,1}}{M_1}-\frac{M_{2,i}^2}{M_1M_2}-\sum_{k=3}^{i-1}\frac{M_{k,i}^2}{M_{k-1}M_k}\right]\\
=&\ \frac{1}{2}\left[\frac{M_2M_{2;1,i;i,1}-M_{2,i}^2}{M_1M_2}-\sum_{k=3}^{i-1}\frac{M_{k,i}^2}{M_{k-1}M_k}\right]\\
=&\ \frac{1}{2}\left[\frac{M_1M_{3;1,2,i}}{M_1M_2}-\frac{M_{3,i}^2}{M_2M_3}-\sum_{k=4}^{i-1}\frac{M_{k,i}^2}{M_{k-1}M_k}\right]\\
&\text{(by using Lemma (2.1))}\\
=&\ \frac{1}{2}\left[\frac{M_3M_{3;1,2,i}-M_{3,i}^2}{M_2M_3}-\sum_{k=4}^{i-1}\frac{M_{k,i}^2}{M_{k-1}M_k}\right]\\
=&\ \frac{1}{2}\left[\frac{M_2M_{4;1,2,3,i}}{M_2M_3}-\frac{M_{4,i}^2}{M_3M_4}-\sum_{k=5}^{i-1}\frac{M_{k,i}^2}{M_{k-1}M_k}\right]\\
&\text{(now proceeding similarly with the repeated use of Lemma (2.1) ...)}\\
=&\ \frac{1}{2}\left[\frac{M_{i-3}M_{i-1;1,2,\ldots,i-2,i}}{M_{i-3}M_{i-2}}-\frac{M_{i-1,i}^2}{M_{i-2}M_{i-1}}\right]\\
=&\ \frac{1}{2}\left[\frac{M_{i-1}M_{i-1;1,2,\ldots,i-2,i}-M_{i-1,i}^2}{M_{i-2}M_{i-1}}\right]\\
=&\ \frac{1}{2}\left[\frac{M_{i-2}M_i}{M_{i-2}M_{i-1}}\right]\\
&\text{(again by using Lemma (2.1))}\\
=&\ \frac{1}{2}\frac{M_i}{M_{i-1}}.
\end{aligned}$$

And the coefficient of x_ix_j in $\mathcal{Q}_i$ for a fixed j is observed to be

$$\left[a_{ij}-\frac{a_{1i}a_{1j}}{2a_{11}}-\frac{M_{2,i}M_{2,j}}{M_1M_2}-\frac{M_{3,i}M_{3,j}}{M_2M_3}-\cdots-\frac{M_{i-1,i}M_{i-1,j}}{M_{i-2}M_{i-1}}\right]$$

$$= \left[\frac{2a_{11}a_{ij} - a_{i1}a_{1j}}{M_1} - \sum_{k=2}^{i-1} \frac{M_{k,i}M_{k,j}}{M_{k-1}M_k}\right]$$

$$= \left[\frac{M_{2;1,i;1,j}}{M_1} - \frac{M_{2,i}M_{2,j}}{M_1M_2} - \sum_{k=3}^{i-1} \frac{M_{k,i}M_{k,j}}{M_{k-1}M_k}\right]$$

$$= \left[\frac{M_2M_{2;1,i;1,j} - M_{2,i}M_{2,j}}{M_1M_2} - \sum_{k=3}^{i-1} \frac{M_{k,i}M_{k,j}}{M_{k-1}M_k}\right]$$

$$= \left[\frac{M_1M_{3;1,2,i;1,2,j}}{M_1M_2} - \frac{M_{3,i}M_{3,j}}{M_2M_3} - \sum_{k=4}^{i-1} \frac{M_{k,i}M_{k,j}}{M_{k-1}M_k}\right]$$

(by using Lemma (2.1), and by proceeding as in the above ...)

$$= \frac{M_{i,j}}{M_{i-1}}.$$

So, in $\mathcal{Q}_i$, if we complete the square for x_i in the usual manner, we have

$$\mathcal{Q}_i = \frac{1}{2}\frac{M_i}{M_{i-1}}\left[x_i^2 + 2x_i\frac{1}{M_i}\sum_{j=i+1}^{n} M_{i,j}x_j + \left(\frac{\sum_{j=i+1}^{n} M_{i,j}x_j}{M_i}\right)^2 - \left(\frac{\sum_{j=i+1}^{n} M_{i,j}x_j}{M_i}\right)^2\right]$$

$$= \frac{1}{2M_{i-1}M_i}\left[M_ix_i + \sum_{j=i+1}^{n} M_{i,j}x_j\right]^2 - \frac{1}{2M_{i-1}M_i}\left(\sum_{j=i+1}^{n} M_{i,j}x_j\right)^2$$

$$= \frac{1}{2M_{i-1}M_i}\left[\sum_{j=i}^{n} M_{i,j}x_j\right]^2 - \frac{1}{2M_{i-1}M_i}\left(\sum_{j=i+1}^{n} M_{i,j}x_j\right)^2.$$

Therefore

$$\mathcal{Q}_{i,i} = \frac{1}{2M_{i-1}M_i}\left[\sum_{j=i}^{n} M_{i,j}x_j\right]^2,$$

and we are through with the part (a).

Also by expanding the second summand in the final expression for the above $\mathcal{Q}_i$, we observe that in this summand for any fixed j larger than i, all the terms with x_j but not involving any x_h with $h < j$, are together equal to

$$-\frac{1}{2M_{i-1}M_i}\left[M_{i,j}^2x_j^2 + 2M_{i,j}x_j\sum_{k=j+1}^{n} M_{i,k}x_k\right],$$

which, according to our scheme, has been denoted by $\mathcal{Q}_{i,j}$. So we are through with the second part of our theorem. □

Note that if $i = n$, then

$$\mathcal{Q}_{n,n} = \frac{1}{2M_{n-1}M_n}(M_nx_n)^2 = \frac{M_n}{2M_{n-1}}x_n^2,$$

as a direct consequence of which the n-th variable remains the same as in the original form, and its coefficient in the reduced diagonal form turns out to be $M_n/2M_{n-1}$.

Thus we find that, by completing the squares, the general quadratic equation $\mathcal{Q} = 0$ turns into the equation

$$\sum_{i=1}^{n} \left[\frac{1}{M_{i-1}M_i} \left(\sum_{j=i}^{n} M_{i,j}x_j \right)^2 \right] = 0.$$

So the simplest equation with integer coefficients and without crossed terms of the type x_ix_j with $i \neq j$, whose integral solutions could finally be used to retrace the solutions of the original equation: $\mathcal{Q} = 0$, turns out to be

$$K\left(\sum_{i=1}^{n} \left[\frac{1}{M_{i-1}M_i} \left(\sum_{j=i}^{n} M_{i,j}x_j \right)^2 \right] \right) = 0, \qquad (2)$$

or, say $\mathcal{R} = 0$, where K is the least common multiple of the set of integers:

$$\{M_1M_2, M_2M_3, \ldots, M_{n-2}M_{n-1}\}.$$

Also, if more than $\lfloor \frac{n}{2} \rfloor$ coefficients in this equation have a common factor $s > 1$, then by multiplying the entire equation by s, and then by absorbing all the square factors of the coefficients with the variables, which themselves are squares, we can obtain an equation whose coefficients are square-free and also no $\lfloor \frac{n}{2} \rfloor + 1$ of whose coefficients have a common factor larger than 1.

This resulting equation, $\mathcal{R} = 0$, in a sense, is the most reduced equation which can be used for obtaining the solutions of the original equation $\mathcal{Q} = 0$.

Thus our immediate goal of reduction is accomplished.

3.4 Retracing the Solution

At this point, it is worth noting that if $\hat{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a solution of $\mathcal{R} = 0$, then $Adj(\underline{N}).\underline{\alpha}^T$, i.e., $D(\underline{N}).\underline{N}^{-1}\underline{\alpha}^T$ is a solution of the original equation $\mathcal{Q} = 0$ where $\underline{N}$ is the upper triangular matrix given by

$$\underline{N} = \begin{bmatrix} M_{1,1} & M_{1,2} & M_{1,3} & \cdots & M_{1,n-1} & M_{1,n} \\ 0 & M_{2,2} & M_{2,3} & \cdots & M_{2,n-1} & M_{2,n} \\ \cdots & 0 & M_{3,3} & \cdots & M_{3,n-1} & M_{3,n} \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & 0 & M_{n-1,n-1} & M_{n-1,n} \\ 0 & & & & 0 & 1 \end{bmatrix}.$$

Next, finding some more solutions should be an obvious desire, which is achieved in the following.

3.5 Generating More Solutions

After getting one nontrivial solution of a homogeneous quadratic equation, one could use the following result for generating infinitely large number of new solutions.

The Generating Theorem. *If $\underline{A}$ is the matrix of a quadratic form F in n variables with a column matrix $\underline{\alpha}$ as one of its nontrivial zeros giving $\underline{\alpha}^T \underline{A}\, \underline{\alpha} = 0$, and $\underline{\beta}$ is any arbitrary $n \times 1$ column matrix, then*

$$\underline{\alpha}\, \underline{\beta}^T \underline{A}\, \underline{\beta} - 2\underline{\beta}\, \underline{\beta}^T \underline{A}\, \underline{\alpha}$$

is also a zero of F. (1)

Proof: Let $\underline{\alpha} + \lambda\underline{\beta}$ be a zero of F, where λ is a rational. Then we have

$$\begin{aligned} & (\underline{\alpha} + \lambda\underline{\beta})^T \underline{A}(\underline{\alpha} + \lambda\underline{\beta}) = 0 \\ \Rightarrow\ & \underline{\alpha}^T \underline{A}\, \underline{\alpha} + \lambda\underline{\alpha}^T \underline{A}\, \underline{\beta} + \lambda\underline{\beta}^T \underline{A}\, \underline{\alpha} + \lambda^2 \underline{\beta}^T \underline{A}\, \underline{\beta} = 0 \\ \Rightarrow\ & \lambda\left(2\underline{\beta}^T \underline{A}\, \underline{\alpha} + \lambda\underline{\beta}^T \underline{A}\, \underline{\beta}\right) = 0 \\ \Rightarrow\ & \lambda = \frac{-2\underline{\beta}^T \underline{A}\, \underline{\alpha}}{\underline{\beta}^T \underline{A}\, \underline{\beta}}. \end{aligned}$$

Now if $\underline{\alpha} + \lambda\underline{\beta}$ is a zero of F, then clearly so is $(\underline{\alpha} + \lambda\underline{\beta})\underline{\beta}^T \underline{A}\, \underline{\beta}$, which, in view of the above argument, implies that $\underline{\alpha}\, \underline{\beta}^T \underline{A}\, \underline{\beta} - 2\underline{\beta}\, \underline{\beta}^T \underline{A}\, \underline{\alpha}$ is also a zero of F. □

Note that when the entries in $\underline{A}$, $\underline{\alpha}$ and $\underline{\beta}$ are integers, the generated zero:

$$\underline{\alpha}\, \underline{\beta}^T \underline{A}\, \underline{\beta} - 2\underline{\beta}\, \underline{\beta}^T \underline{A}\, \underline{\alpha}$$

is also with integer entries. Therefore, after getting one nontrivial solution of a homogeneous quadratic equation, by using the above theorem one could generate as many new solutions as desired by changing the entries in $\underline{\beta}$.

3.6 Some Remarks

Now, before leaving this chapter and starting our work on the ternary equations in the next chapter, some observations on the results of this chapter seem to be appropriate here.

First, the reduction we have presented here demands the top left corner determinants, namely the M_i's, to be nonzero. But this requirement, when not satisfied, can sometimes be met by interchanging the ordering of the variables, and thereby causing only a rearrangement in the matrix of the form. Thus, sometimes the difficulty can be avoided only through a mechanical rearrangement.

Secondly, the generating-formula which we have given in the previous section, in the face of all what we have seen, is a conspicuous improvement over the only existing generating formula given by Desboves in (2), which in the ternary case translates to the following:

When (x, y, z) is a given solution of

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$$

a general solution (X, Y, Z) is given by:

$$\begin{aligned} X &= -(bp^2 + cq^2 + fpq)x, \\ Y &= (dx + by + fz)p^2 - cyq^2 + (ex + 2cz)pq, \\ Z &= -bzp^2 + (ex + fy + cz)q^2 + (dx + 2by)pq \end{aligned}$$

where p and q are two independent parameters whose values can be arbitrarily chosen. Also note that this generating-formula of Desboves involves only two parameters, whereas the matrix-formula given by us has three parameters in the ternary case, namely the three components of $\underline{\beta}$, yielding better flexibility in the generation of new solutions.

Moreover, it is easy to see that the above formula of Desboves is a particular case of our formula with two components of $\underline{\beta}$ equal to p and q and the third equal to zero. Therefore since Desboves's Formula generates all the solutions, our formula also generates all the solutions of the equation in hand.

Now with our objective of this chapter accomplished, in the next chapter we are going to start our work with the homogeneous ternary quadratic equations.

Chapter 4

SOLUTIONS OF THE LEGENDRE'S EQUATION: $ax^2 + by^2 + cz^2 = 0$

4.1 The Goal

After solving the Pell equation: $u^2 - Dv^2 = N$, and consequently the general non-homogeneous binary quadratic equation: $ax^2 + by^2 + dxy + ex + fy + c = 0$, one naturally thinks of solving the homogeneous ternary equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$$

which, under the restrictive conditions of the nonzero-ness of M_1, M_2 and M_3, can be reduced by the process described in the previous chapter, to

$$ax^2 + by^2 + cz^2 = 0 \qquad (1)$$

where abc is nonzero and square-free. We refer to this equation(1) as the Legendre's equation.

One tests the solvability of this reduced equation by the wellknown theorem of Legendre which first appeared in his *"Recherches d' Analyse Indeterminée "* in 1785, (Ref.(6)). We are going to devote this entire chapter for analysing this theorem, first by presenting a proof in the next section which is essentially due to Dirichlet but slightly modified by us, and then by extracting an algorithm in §4.3 to solve the above reduced equation: $ax^2 + by^2 + cz^2 = 0$. We conclude this chapter in §4.4 with a comment about this extracted algorithm.

4.2 Legendre's Theorem

Legendre's Theorem. *If abc is nonzero and square-free, and all of a, b, c are not with the same sign, then*

$$ax^2 + by^2 + cz^2 = 0 \tag{1}$$

has a nontrivial solution if and only if $-bc, -ac$ and $-ab$ are quadratic residues of $|a|, |b|$ and $|c|$ respectively.

Proof: ($\Rightarrow$:) With no loss of generality, let (x, y, z) be a primitive solution of (1). Then, we claim that x, y and z have to be pairwise prime, i.e., in notation:

$$G(x, y) = G(x, z) = G(y, z) = 1. \tag{2}$$

Because , if it is not so, let, for example,

$$p|G(x, y) \quad \text{with } p > 1.$$

Then this assumption and the equation (1) together imply that $p^2|cz^2$, which, since abc is square-free, implies that $p|z$ contradicting the primitivity of (x, y, z). Hence x, y, and z are pairwise prime.

Again, we claim that

$$G(a, z) = 1, \tag{3}$$

because if it is not so, let $p|G(a, z)$ with $p > 1$. Then, since (x, y, z) is a solution of (1), it implies $p|by^2$. This in turn demands either $p|b$, which contradicts the square-freeness of abc, or $p|y$ violating the pairwise-prime property of x, y and z which we just established in the above. Therefore $G(a, z) = 1$, which assures that

$$\exists w \in \mathbb{Z}, \quad \text{with} \quad wz \equiv 1 \pmod{a}. \tag{4}$$

Now,

$$bw^2 \times (1) \approx abw^2x^2 + b^2w^2y^2 + bcw^2z^2 = 0,$$

which, because of (4), implies that $-bc$ is a quadratic residue of $|a|$. The rest follows by symmetry.

($\Leftarrow$:) To prove the converse, we assume that abc is nonzero and square-free, and that $-bc$, $-ca$ and $-ab$ are quadratic residues of $|a|$, $|b|$ and $|c|$ respectively. And then we intend to produce a nontrivial solution of the equation (1).

Let the median of the integers $|ab|$, $|bc|$, and $|ac|$ be termed as the index of the equation (1), and let us denote it by $Ind(1)$. Our proof will be by induction on this $Ind(1)$.

If $Ind(1)$ is 1, with no loss of generality, let $|ab| = 1$, which implies that

$$|a| = |b| = 1.$$

Therefore

$$\{\, |ab|, |bc|, |ac| \,\} = \{\, 1, |c|, |c| \,\},$$

and since $Ind(\underline{1}) = 1$, we have $|c| = 1$. And since all of a,b, and c are not of the same sign, with no loss of generality we can assume that $a = 1$ and $b = -1$, whereby (1,1,0) can be taken as a nontrivial solution of ($\underline{1}$), and thus we are through.

So, let $Ind(\underline{1}) = n \geq 2$, and we hypothesize that any equation with its index smaller than n has a nontrivial solution. Our goal is to prove that there is a nontrivial solution of ($\underline{1}$).

With no loss of generality, let

$$|a| \leq |b| \leq |c|. \tag{5}$$

We claim that $|b| \neq |c|$, because, if $|b| = |c|$, then since abc is square-free, we must have $|b| = |c| = 1$, and then since abc is nonzero and $|a| \leq |b|$, we have $|a| = 1$, which implies that $Ind(\underline{1}) = 1$, contradicting our assumption: $Ind(\underline{1}) = n \geq 2$. Therefore $|b| \neq |c|$, and we have

$$|a| \leq |b| < |c| \tag{6}$$

which implies that

$$\begin{aligned} & |ab| < |ac| \leq |bc| \\ \Rightarrow \quad & |ac| = Ind(\underline{1}) = n. \end{aligned}$$

Thus we have

$$|ac| = n. \tag{7}$$

Now, since $-ab$ is a quadratic residue of $|c|$,

$$\begin{aligned} & \exists r' \in \mathbb{Z}, \text{ with} \qquad r'^2 \equiv -ab \pmod{c} \\ \Rightarrow \quad & ar'^2 \equiv -a^2 b \pmod{c}. \end{aligned}$$

And since abc is square-free, implying a and c to be relatively prime and yielding an inverse of a modulo c, from this congruence we derive that

$$\exists r \in \mathbb{Z}, \quad \text{with} \quad |r| \leq |\frac{c}{2}| \tag{8}$$

such that

$$ar^2 \equiv -b \pmod{c},$$

which in turn yields

$$ar^2 + b = cs \qquad \text{for some } s \in \mathbb{Z}. \tag{9}$$

Therefore, if $s = 0$, we have $ar^2 = -b$, and since abc is square-free, r must be equal to 1, and so $a = -b$; and consequently $(1, 1, 0)$ is a nontrivial solution of ($\underline{1}$), and we are through.

So, let $s \neq 0$. Then

$$(\underline{9}) \qquad \Rightarrow |s| = \frac{|ar^2 + b|}{|c|} \leq \frac{|ar^2|}{|c|} + \frac{|b|}{|c|}.$$

Therefore, since $|r| \leq |\frac{c}{2}|$ (as shown in (8)), we have

$$|s| \leq \frac{\left|\frac{ac^2}{4}\right|}{|c|} + \frac{|b|}{|c|} = \frac{|ac|}{4} + \frac{|b|}{|c|}.$$

And since $|b| < |c|$ (as claimed in (6)), and $|ac| = n$ (in (7)), and by assumption $n \geq 2$, we have

$$|s| < \frac{n}{4} + 1 \leq \frac{n}{4} + \frac{n}{2} = \frac{3n}{4} < n$$

Thus,

$$|s| < n. \tag{10}$$

Now, let A be the *gcd* of all the terms in (9). Then, since abc is square-free, A must divide both r, and s. Therefore setting $r = A\alpha$, $b = A\beta$ and $s = AC\gamma^2$ with γ^2 as the largest square factor of $\frac{s}{A}$ so that C is square-free, we have:

$$(9) \approx aA^2\alpha^2 + A\beta = cAC\gamma^2$$

yielding

$$aA\alpha^2 + \beta = cC\gamma^2 \tag{11}$$

Note that in this equation (11), the terms are pairwise prime.

Now, let

$$a\beta = B. \tag{12}$$

Then we claim that the coefficients of the equation:

$$Ax^2 + By^2 + Cz^2 = 0 \tag{13}$$

satisfy the conditions demanded on a, b, c of the original equation (1), but its index is strictly smaller than the index of (1).

Firstly, it is obvious that

$$ABC = Aa\beta C \neq 0. \tag{14}$$

Secondly the terms of (11) being pairwise prime, we have

$$aA\beta C \text{ or } ABC \qquad \text{square-free.} \tag{15}$$

Thirdly, to see that all of A, B and C cannot be of the same sign, let us suppose

$$AB = Aa\beta = ab > 0.$$

Then, since all of a,b and c are not with the same sign, we have both ac and bc as negative integers. So,

$$\begin{aligned} cA \times (11) &\approx acA^2\alpha^2 + cA\beta = ACc^2\gamma^2 \\ &\Rightarrow acA^2\alpha^2 + bc = ACc^2\gamma^2 \\ &\Rightarrow AC \quad \text{is negative,} \end{aligned}$$

which implies that A and C, or consequently

$$\text{all of} \quad A, B \quad \text{and} \quad C \quad \text{are not with the same sign.} \tag{16}$$

Now,

$$aA \times (\underline{11}) \approx a^2A^2\alpha^2 + aA\beta = acAC\gamma^2 \tag{17}$$

from which we derive that

$$-aA\beta \quad \text{or} \quad -AB \quad \text{is a quadratic residue of} \quad |C| \tag{18}$$

For convenience, from this point on, let us use the Legendre's symbol $\left\|\frac{r}{q}\right|$, which is defined by:

$$\left\|\frac{r}{q}\right| = \begin{cases} 1, & \text{if } r \text{ is a quadratic residue of } q; \\ -1, & \text{otherwise.} \end{cases}$$

We have

$$cC \times (\underline{11}) \approx acAC\alpha^2 + cC\beta = c^2C^2\gamma^2 \tag{19}$$

which gives

$$\left\|\frac{cC\beta}{|A|}\right| = 1. \tag{20}$$

Also since $-ac$ is a quadratic residue of $|b|$, and $b = A\beta$, we have

$$\left\|\frac{-ac}{|A|}\right| = 1. \tag{21}$$

So,

$$\begin{aligned} (\underline{20}), (\underline{21}) \quad &\Rightarrow \quad \left\|\frac{(-ac)cC\beta}{|A|}\right| = 1 \\ &\Rightarrow \quad \left\|\frac{-c^2a\beta C}{|A|}\right| = \left\|\frac{-a\beta C}{|A|}\right| = 1, \end{aligned}$$

which means

$$\left\|\frac{-BC}{|A|}\right| = 1. \tag{22}$$

Also, since

$$(\underline{17}) \Rightarrow \left\|\frac{acAC\gamma^2}{\beta}\right| = 1,$$

and

$$\left\|\frac{-ac}{|b|}\right| = 1 \Rightarrow \left\|\frac{-ac}{|A\beta|}\right| = 1 \Rightarrow \left\|\frac{-ac}{\beta}\right| = 1,$$

we have

$$\left\|\frac{(-ac)(acAC\gamma^2)}{\beta}\right| = 1 \Rightarrow \left\|\frac{-AC}{\beta}\right| = 1. \tag{23}$$

Again, since

$$(19) \Rightarrow \left\| \frac{cC\beta}{|a|} \right| = 1,$$

and

$$\left\| \frac{-bc}{|a|} \right| = 1 \Rightarrow \left\| \frac{-A\beta c}{|a|} \right| = 1,$$

we have

$$\left\| \frac{(cC\beta)(-A\beta c)}{|a|} \right| = 1 \Rightarrow \left\| \frac{-AC\beta^2 c^2}{|a|} \right| = 1,$$

from which we deduce that

$$\left\| \frac{-AC}{|a|} \right| = 1. \tag{24}$$

Now, since ab is square-free, implying a and β to be relatively prime,

$$(23) \quad \text{and} \quad (24) \Rightarrow \left\| \frac{-AC}{|a\beta|} \right| = 1,$$

which yields

$$\left\| \frac{-AC}{|B|} \right| = 1. \tag{25}$$

Thus, by (14), (15), (16), (18), (22) and (25), we have verified our claim that the coefficients of the equation (13):

$$Ax^2 + By^2 + Cz^2 = 0$$

satisfy the conditions identical to those imposed on the coefficients a, b and c of the original equation (1).

The only remaining condition for the equation (13) to have a nontrivial solution is to observe that its index is less than n, after which the inductive hypothesis will guarantee such a solution for (13). Now,

$$(6) \quad \& \quad (7) \Rightarrow n = |ac| > |ab| = |AB|,$$

and,

$$(10) \Rightarrow n > |s| = |AC\gamma^2| \geq |AC|.$$

Thus both $|AB|$ and $|AC|$ being smaller than n, the index of (13) has to be smaller than n, and hence by our inductive hypothesis (13) is guaranteed to have a nontrivial solution, say (X, Y, Z).

Now, let

$$\left.\begin{aligned} x &= A\alpha X - \beta Y, \\ y &= X + a\alpha Y, \\ z &= C\gamma Z \quad . \end{aligned}\right\} \tag{26}$$

Then,

$$\begin{aligned} ax^2+by^2+cz^2 &= a(A^2\alpha^2X^2+\beta^2Y^2-2A\alpha\beta XY)+ \\ &\qquad A\beta(a^2\alpha^2Y^2+X^2+2a\alpha XY)+cC^2\gamma^2z^2 \\ &= AX^2(aA\alpha^2+\beta)+a\beta Y^2(\beta+Aa\alpha^2)+cC^2\gamma^2Z^2, \\ &\quad \text{which, by (11) and (12)} \\ &= (AX^2+BY^2+CZ^2)cC\gamma^2 \\ &= 0 \quad . \end{aligned}$$

So, if (X,Y,Z) is a solution of (13), then so is the above (x,y,z) for the original equation (1).

Now the only thing which remains to be shown is the nontriviality of (x,y,z). If it is not so, let

$$x=y=z=0.$$

Now, by (26), if $z=0$, then Z is also 0, and if $x=0$ and $y=0$, by eliminating X from the first two equations of (26), we have:

$$(Aa\alpha^2+\beta)Y=0,$$

which, by (11), yields

$$cC\gamma^2Y=0 \Rightarrow Y=0,$$

(since both c and s are assumed to be nonzero). Now with $y=0$ and $Y=0$, the second equation of (26) demands $X=0$, thus yielding $(X,Y,Z)=(0,0,0)$, and thereby violating the nontriviality of (X,Y,Z), which, by the inductive hypothesis, was obtained as a nontrivial solution of (13).

Hence (x,y,z) must be a nontrivial solution for (1), and thus we are through with the inductive step, and thereby, the proof of Legendre's theorem is complete. □

4.3 Dirichlet's Algorithm

Note that the above proof of Dirichlet actually yields an algorithm to get a nontrivial solution of (1) whenever it exists. Let us extract this algorithm more precisely:

DIRICHLET'S ALGORITHM:

One first checks if there could be an obvious solution of

$$ax^2 + by^2 + cz^2 = 0. \tag{1}$$

If there is such a solution, nothing more is necessary. If not, with no loss of generality assuming

$$|a| \leq |b| \leq |c|,$$

one seeks an r satisfying:

$$ar^2 + b = cs, \qquad \text{for some } s \in \mathbb{Z} \text{ with } \quad |r| \leq |\frac{c}{2}|, \tag{2}$$

which is indirectly guaranteed by the conditions of the Legendre's theorem.

Then let A be the greatest common divisor of the three terms of the equation in (2), and γ^2 the largest sqare factor of $\frac{s}{A}$, and let

$$s = AC\gamma^2.$$

Also, let

$$b = A\beta, \quad \text{and} \quad r^2 = A^2\alpha^2.$$

Then setting $B = a\beta$, one checks if the equation

$$Ax^2 + By^2 + Cz^2 = 0$$

has an obvious solution of the type $(1, 1, 0)$.

If not so, then one rearranges these new coefficients: A, B, C as a_1, b_1, c_1 with $|a_1| \leq |b_1| \leq |c_1|$, and repeats the above process of reduction. A finite number of repetitions of this reduction process assures at some point an obvious nontrivial solution of the type $(1, 1, 0)$ for an equation such as

$$A_iX_2 + B_iY^2 + C_iZ^2 = 0.$$

Then assuming the penultimate coefficients to be a_i, b_i and c_i, one retraces the solution for the original equation (1) by repeated use of the solution-retracing matrix-formula:

$$\begin{bmatrix} x_i & y_i & z_i \end{bmatrix} = \begin{bmatrix} |X_i| & |Y_i| & |Z_i| \end{bmatrix} \cdot \begin{bmatrix} |A_i\alpha_i| & S(b_i), & 0 \\ -|\beta_i| & |a_i\alpha_i| & 0 \\ 0 & 0 & |C_i\gamma_i| \end{bmatrix}. \tag{3}$$

where the sign-function $S: \mathbb{R} \longrightarrow \{1, 0, -1\}$ on the set of reals is defined by:

$$S(r) = \begin{cases} 1, & \text{for } r > 0 \\ 0, & \text{for } r = 0 \\ -1, & \text{for } r < 0\,. \end{cases} \tag{4}$$

4.4 A Comment on The Size of Dirichlet's Solution

Note that for each reduction step the values: $A\alpha, a\alpha$, $C\gamma$ and β are usually different. And, in order to avoid the unnecessary increase in the size of the solution for the original equation (1), each time after using the above solution-retracing-formula (3.3), from the components of the obtained solution (x, y, z) one could cancel out their greatest common divisor.

Moreover note that since α could be chosen either positive or negative, there is a possibility of increasing the size of the retraced solution at any level by the inappropriate choice of the sign of α. In order to circumvent this possibility of increasing the size of the solution at any level we have used the absolute values and the sign-function in the solution-retracing-formula(3.3), which is actually a modification of the algorithm prescribed by Dirichlet.

However, even by adopting the best possible choices allowed, the solution obtained by this algorithm of Dirichlet could be much larger than the minimum solution for (1). In fact we have examples where the solution obtained cannot even be within the Holzer's range:

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ca|}, \quad \text{and} \quad |z| \leq \sqrt{|ab|}.$$

in which, as we will see in the next chapter, there must be a nontrivial solution whenever the equation in hand is nontrivially solvable.

In order to authenticate our claim about this deficiency of the above algorithm of Dirichlet, we present the following table:

Table 4.1: Irreducible Larger Solutions of Dirichlet

(a, b, c)	Holzer's Limit	Number of Dirichlet's Reduction steps	Dirichlet's Solution	Minimum Solution
(7 ,53 ,-1)	(7 ,2 , 19)	1	(1,3,22)	(2,1,9)
(7 ,113,-1)	(10,2 , 28)	1	(1,3,32)	(4,1,15)
(13,173,-1)	(13,3 , 47)	1	(1,6,79)	(2,1,15)
(13,191,-1)	(13,3 , 49)	1	(1,6,83)	(5,2,33)

Therefore, very naturally one seeks for a method of reducing the size of a larger Dirichlet's solution to the Holzer's range. We are going to deal with this problem of reduction in the next chapter.

Chapter 5

REDUCING THE SIZE OF A SOLUTION

5.1 The Goal

At the end of the previous chapter we saw that Dirichlet's solution to the nontrivially solvable equation: $ax^2 + by^2 + cz^2 = 0$ could sometimes be undesirably large. In this chapter we will present a theorem of Holzer that first appeared in (5), which assures the existence of a solution in the range:

$$|x| \leq \sqrt{|bc|}, \qquad |y| \leq \sqrt{|ca|}, \quad \textit{and} \qquad |z| \leq \sqrt{|ab|}.$$

We call this range as the Holzer's range, or the H-range.

In the next section we present Mordell's proof for the above existence theorem of Holzer. Our reference for this proof is (9). Then in §5.3, from this proof of Mordell we extract an algorithm that uses the Dirichlet's larger solution to obtain a solution within the Holzer's range. Then in §5.4 we generalize Holzer's theorem to predict the existence of a nontrivial solution within a particular range for a nontrivially solvable equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0. \tag{1}$$

This range, which we prescribe here and name as the CM-range, yields the Holzer's range as a particular case when $d = e = f = 0$. Then in §5.5 we extract a new algorithm for getting a solution of the above general ternary quadratic equation (1) within the CM-range. We conclude this chapter in §5.6 with a comment about the algorithms presented in this chapter.

5.2 Holzer's Theorem

Holzer's Theorem. *Given the positive integers a, b, and c, if the equation:*

$$ax^2 + by^2 - cz^2 = 0 \tag{1}$$

has a nontrivial solution $(x_0, y_0, z_0) \neq (0,0,0)$, then it also has a solution (x, y, z) with

$$(|x|, |y|, |z|) \leq (\sqrt{|bc|}, \sqrt{|ac|}, \sqrt{|ab|}).$$

[Clearly the equality signs may be removed unless two of the coefficients a, b and c are unity.]

Proof: Let (x_0, y_0, z_0) be a primitive solution of (1). If $z_0 > \sqrt{ab}$, we intend to get a solution (x, y, z) with $|z| < |z_0|$. Finite repetition of this process leads to a solution with $|z| < \sqrt{ab}$, which also obviously implies

$$(|x|, |y|, |z|) \leq (\sqrt{bc}, \sqrt{ac}, \sqrt{ab}).$$

Now, by (3.5.1) we know that if (x_0, y_0, z_0) is a solution of (1), $R = (r_1, r_2, r_3)$ is an arbitrary element of $\mathbb{Z}^3$; $\underline{X}_0$, $\underline{R}$ and $\underline{A}$ are the matrices:

$$\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix}, \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & -c \end{bmatrix}$$

respectively; and

$$\underline{X} = \underline{X}_0 \underline{R}^T \underline{A}\, \underline{R} - 2\underline{R}\, \underline{R}^T \underline{A}\, \underline{X}_0 = \delta \begin{bmatrix} x \\ y \\ z \end{bmatrix} \tag{2}$$

where δ is a divisor of all the components of $\underline{X}$, then (x, y, z) is also a solution of (1).

Assuming $z_0^2 > ab$, here is an algorithm for choosing R such that $|z| < |z_0|$:

Let

$$\delta = \begin{cases} \frac{c}{2} & \text{if } c \text{ is even,} \\ c & \text{if } c \text{ is odd.} \end{cases} \tag{3}$$

Find r_1 and r_2 such that

$$y_0 r_1 - x_0 r_2 = \delta. \tag{4}$$

Then find r_3 such that:

$$\left| r_3 + \frac{a x_0 r_1 + b y_0 r_2}{c z_0} \right| \leq \begin{cases} \frac{1}{2} & \text{if } c \text{ is even,} \\ 1 & \text{and } a r_1 + b r_2 + c r_3 \equiv 0 \pmod 2, \text{ if } c \text{ is odd.} \end{cases} \tag{5}$$

Now we want to prove that with

$$\underline{R} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix},$$

the z given by (2) satisfies $|z| < |z_0|$.

First we observe that with the above algorithm, x, y and z in (2) are integers. Also

$$(2) \Rightarrow \quad \delta z = z_0(ar_1^2 + br_2^2 + cr_3^2) - 2r_3(ax_0r_1 + by_0r_2 + cz_0r_3) \qquad (6)$$

$$(4) \Rightarrow \quad r_1 \equiv \frac{x_0r_2}{y_0} \pmod{\delta} \qquad (7)$$

$$(7) \Rightarrow \quad ax_0r_1 + by_0r_2 \equiv \frac{ax_0^2r_2}{y_0} + by_0r_2 \pmod{\delta}$$

$$= (ax_0^2 + by_0^2)\frac{r_2}{y_0},$$

whence, because (x_0, y_0, z_0) is a solution of (4), and by (3) $\delta | c$, and obviously

$$G(\delta, abx_0y_0) = 1, \qquad (8)$$

we have:

$$ax_0r_1 + by_0r_2 \equiv 0 \pmod{\delta} \qquad (9)$$

Also

$$(7) \Rightarrow \quad ar_1^2 + br_2^2 \equiv \frac{ax_0^2r_2^2}{y_0^2} + br_2^2 \pmod{\delta}$$

$$= (ax_0^2 + by_0^2)\frac{r_2^2}{y_0^2}$$

$$= -cz_0^2\frac{r_2^2}{y_0^2}$$

which, since $\delta | c$, implies that

$$ar_1^2 + br_2^2 \equiv 0 \pmod{\delta}. \qquad (10)$$

Now (3), (6), (9) and (10) imply that z is an integer. And with similar reasoning we find that x and y are also integers.

Now to see that $|z| < |z_0|$, we observe that

$$(6) \Rightarrow \frac{-\delta z}{cz_0} = (r_3 + \frac{ax_0r_1 + by_0r_2}{cz_0})^2 + \frac{ab}{c^2z_0^2}(y_0r_1 - x_0r_2)^2 \qquad (11)$$

Therefore, when c is even with $c = 2\delta$, and $z_0^2 > |ab|$, by (4) and (5) we have:

$$\left|\frac{z}{z_0}\right| \leq \frac{c}{\delta}\left(\left|r_3 + \frac{ax_0r_1 + by_0r_2}{cz_0}\right|^2 + \frac{ab}{c^2z_0^2}\left|y_0r_1 - x_0r_2\right|^2\right) < 2(\frac{1}{4} + \frac{1}{4}),$$

which means that

$$|z| < |z_0|.$$

And when c is odd, since r_3 is chosen in (5) in such a manner that $ar_1 + br_2 + cr_3$ is 0 modulo 2, clearly δz, as well as δx and δy are even integers. Therefore we can replace δz of (6) or (11) by 2δ, to get:

$$\frac{-2\delta z}{cz_0} = \left(r_3 + \frac{ax_0r_1 + by_0r_2}{cz_0}\right)^2 + \frac{ab}{c^2z_0^2}\left(y_0r_1 - x_0r_2\right)^2,$$

from which, because of the conditions (3),(4) and (5), if $z_0^2 > |ab|$, we deduce that

$$2\left|\frac{z}{z_0}\right| < 1 + 1,$$

or

$$|z| < |z_0|.$$

Thus the effectiveness of the algorithm is established, and thereby, the theorem is also proved. □

5.3 Mordell's Algorithm

Let us have a precise description of the Mordell's algorithm in the above proof which helps us in detecting a solution of $ax^2 + by^2 = cz^2$ within the Holzer's range when the solution obtained by Dirichlet's algorithm is not a Holzer's solution.

MORDELL'S ALGORITHM:

Let the nontrivial primitive solution in hand be

$$\underline{X}_0 = \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix},$$

and

$$\delta = \begin{cases} \frac{c}{2} & \text{if } c \text{ is even} \\ c & \text{if } c \text{ is odd.} \end{cases}$$

If the penultimate convergents of the continued fraction expansion of the rational number $-\frac{y_0}{x_0}$ are p_{n-1} and q_{n-1}, take

$$r_1 = (-1)^n \delta q_{n-1}, \text{ and } \qquad r_2 = (-1)^{n-1} \delta p_{n-1}.$$

Setting

$$\frac{ax_0r_1 + by_0r_2}{cz_0} = k,$$

let

$$r_3 = \begin{cases} \lfloor \frac{1}{2} - k \rfloor, & \text{when } c \text{ is even;} \\ \lfloor 1 - k \rfloor \text{ or } \lfloor 1 - k \rfloor - 1, \text{ such that } r_3 \equiv ar_1 + br_2 \pmod 2, & \text{when } c \text{ is odd.} \end{cases}$$

Now, if $R = (r_1, r_2, r_3)$, and

$$\underline{R} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix}, \quad \underline{A} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & -c \end{bmatrix}$$

then

$$\underline{X} = \underline{X}_0 \, \underline{R}^T \underline{A} \, \underline{R} - 2\underline{R} \, \underline{R}^T \underline{A} \, \underline{X}_0 \, .$$

is a solution of $ax^2 + by^2 = cz^2$ such that the absolute values of its components are strictly smaller than the the corresponding values of $\underline{X}_0$. Now a repeated use of this algorithm on $\underline{X}_0$ would yield a solution within the Holzer's range. For us it has been an interesting observation that for all the examples of about 15,000 equations we have dealt with, where the coefficients of course were up to only four digited integers, no matter what non-Hozer solution we started with, only one application of the above reduction was sufficient to yield a solution within the Holzer's range. It has been a mystery for us — but it may only be a lucky coincidence. However, on the basis of this observation alone, in Chapter-7 we have made a bold suggestion for future investigations.

5.4 A Generalization of The Holzer's Theorem

In this section we want to demonstrate a result relating to the size of a solution of the nontrivially solvable equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0 \qquad (\underline{1})$$

In spirit our result is going to be very similar to that of Holzer's.

First let us identify some notations for the ternary form:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz$$

which we developed in Chapter-3 while dealing with the general reduction of a quadratic form.

In this context, we have

$$\underline{A} = \begin{bmatrix} 2a & d & e \\ d & 2b & f \\ e & f & 2c \end{bmatrix};$$

$$M_1 = M_{1,1} = 2a, \qquad M_{1,2} = d, \qquad M_{1,3} = e;$$

$$M_2 = M_{2,2} = 4ab - d^2, \qquad M_{2,3} = 2af - de;$$

$$M_3 = M_{3,3} = 8abc + 2def - 2af^2 - 2be^2 - 2cd^2;$$

and assuming that

$$a \neq 0, \qquad d^2 \neq 4ab,$$

and

$$4abc + def \neq af^2 + be^2 + cd^2,$$

which in other words assure M_1, M_2 and M_3 to be nonzero, we have the reduced equation:

$$M_2 u^2 + v^2 + M_1 M_3 w^2 = 0 \qquad (\underline{2})$$

where

$$\left.\begin{array}{rcl} u &=& 2ax + dy + ez \\ v &=& M_2 y + M_{2,3} z \\ w &=& z \end{array}\right\} \qquad (3)$$

Since the nontrivial solvability of (1) assures the nontrivial solvability of (2), the Holzer's theorem assures the existence of a solution for (2) with

$$|u| \leq \sqrt{|M_1 M_3|}, \qquad (4)$$

$$|v| \leq \sqrt{|M_1 M_2 M_3|}, \qquad (5)$$

and

$$|w| \leq \sqrt{|M_2|}. \qquad (6)$$

Now,

$$\begin{array}{rcl} (3) \Rightarrow \quad z &=& w, \\ y &=& \dfrac{v - M_{2,3} w}{M_2}, \\ \text{and} \quad x &=& \dfrac{u - dy - ez}{M_1}. \end{array}$$

Note that when $G(M_1, M_2) = 1$, and the numerators in the above expressions for y and z are relatively prime to the corresponding denominators, in order to have an integral solution (x, y, z) for (1), we have to multiply the above x, y and z by $M_1 M_2$, as a result of which we may be forced to have:

$$\left.\begin{array}{rcl} z &=& M_1 M_2 w, \\ y &=& M_1 (v - M_{2,3} z), \\ \text{and} \quad x &=& M_2 (u - dy - ez) \end{array}\right\} \qquad (7, 8, 9)$$

as the solution components for (1).

Note that because once a solution (u, v, w) for (2) is obtained we can choose the signs of u, v and w arbitrarily, whereas similar sign-changes in the case of x, y and z may lead to a non-solution of (1). To demonstrate this claim we observe that any choice of $(\pm 3, \pm 2, \pm 1)$ is a solution of

$$7u^2 - 5v^2 - 43w^2 = 0;$$

whereas, eventhough both $(2, -3, -1)$ and $(-2, 3, 1)$ are solutions of

$$5x^2 + y^2 + 84z^2 + 18xy + 7xz + 3yz = 0,$$

neither $(2, 3, 1)$ nor $(2, -3, 1)$ is a solution.

Now,

$$(6) \quad \text{and} \quad (7) \Rightarrow |z| \leq |M_1 M_2| \sqrt{|M_2|}. \qquad (10)$$

And by choosing the sign of v as that of $M_{2,3} z$, we note that

$$(8) \Rightarrow |y| \leq |M_1| \max\{\, |v|, |M_{2,3} z| \,\};$$

and, therefore, in view of (5) and (10), we have

$$|y| \le |M_1| \max\left\{ \sqrt{|M_1 M_2 M_3|}, \quad |M_1 M_2 M_{2,3}| \sqrt{|M_2|} \right\}. \tag{11}$$

Similarly in (9) choosing the sign of u as that of $dy + ez$, we have

$$|x| \le |M_2| \max\{ |u|, |dy + ez| \}. \tag{12}$$

Now by (4), (10), (11) and (12), we have

$$\begin{aligned} |x| \;\le\; |M_2| \max\Big\{ \sqrt{|M_1 M_3|}, \quad \Big(|dM_1| \max\Big\{ \sqrt{|M_1 M_2 M_3|},\ |M_1 M_2 M_{2,3}| \sqrt{|M_2|} \Big\} \\ + |eM_1 M_2| \sqrt{|M_2|} \Big) \Big\}. \end{aligned} \tag{13}$$

Thus, in view of the above reasonings, we have the following:

Theorem. *If the equation:*

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0 \tag{1}$$

is nontrivially solvable, and among the determinants

$$M_1 = |2a|, \quad M_2 = \begin{vmatrix} 2a & d \\ d & 2b \end{vmatrix}, \quad M_3 = \begin{vmatrix} 2a & d & e \\ d & 2b & f \\ e & f & 2c \end{vmatrix}$$

$$\text{and} \qquad M_{2,3} = \begin{vmatrix} 2a & e \\ d & f \end{vmatrix},$$

M_1, M_2, and M_3 are nonzero, then there is a nontrivial solution (x, y, z) of (1) such that

$$\begin{aligned} |x| \;\le\; |M_2| \max\Big\{ \sqrt{|M_1 M_3|}, \quad \Big(|dM_1| \max\Big\{ \sqrt{|M_1 M_2 M_3|},\ |M_1 M_2 M_{2,3}| \sqrt{|M_2|} \Big\} \\ + |eM_1 M_2| \sqrt{|M_2|} \Big) \Big\}, \end{aligned} \tag{13}$$

$$|y| \le |M_1| \max\left\{ \sqrt{|M_1 M_2 M_3|}, \quad |M_1 M_2 M_{2,3}| \sqrt{|M_2|} \right\}, \tag{11}$$

$$\text{and,} \qquad |z| \le |M_1 M_2| \sqrt{|M_2|}. \tag{10}$$

□

Let us call the above limits for x, y and z as the CM-limits of the equation (1), and the region in the three dimensional Euclidean space defined by them as the CM-range of (1). Also let us call a nontrivial solution of (1) within the CM-range as a CM-solution.

Now note that when $d = e = f = 0$, and abc is nonzero and square-free, by the relations in (3) the equation (2) translates to

$$16a^3 bx^2 + 16a^2 b^2 y^2 + 16a^2 bcz^2 = 0,$$

$$\text{or,} \qquad 16a^2b(ax^2 + by^2 + cz^2) = 0,$$

and therefore the above CM-limits change to

$$\begin{aligned} |x| &\leq \frac{1}{|16a^2b|} \cdot |4ab| \max\left\{\sqrt{|16a^2bc|},\, 0\right\} &&= \sqrt{|bc|}, \\ |y| &\leq \frac{|2a|}{|16a^2b|} \cdot \max\left\{\sqrt{|64a^3b^2c|},\, 0\right\} &&= \sqrt{|ac|}, \\ \text{and,} \quad |z| &\leq \frac{|2a.4ab|}{|16a^2b|} \cdot \sqrt{|4ab|} &&= \sqrt{|ab|}, \end{aligned}$$

which are exactly the Holzer's limits for $ax^2 + by^2 + cz^2 = 0$.

Thus we observe that our CM-limits are generalized H-limits, and the H-solutions are particular CM-solutions when in the general ternary quadratic equation (1) $d = e = f = 0$.

5.5 An Algorithm For Getting A CM-solution of: $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$

Let us prescribe an algorithm to get a CM-solution (x, y, z) for a nontrivially solvable equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0\,. \tag{1}$$

With the notations of the previous section, let r^2 and t^2 be the largest square factors of M_2 and M_1M_3 respectively, and let l be the greatest common divisor of $\frac{M_2}{r^2}$ and $\frac{M_1M_3}{t^2}$. Note that if

$$k = \frac{M_2}{r^2 l} \quad \text{and} \quad m = \frac{M_1M_3}{t^2 l},$$

then klm is square-free.

Now we solve the equation

$$ku'^2 + lv'^2 + mw'^2 = 0 \tag{2}$$

by the Dirichlet's algorithm given in §4.3 . Then by applying the Mordell's algorithm of §5.3 we get a positive-octant-solution (u', v', w') of (2) within its H-range. Now, if

$$u = tu', \quad v = lrtv', \quad \text{and} \quad w = rw',$$

then (u, v, w) is an H-solution of the diagonalized equation

$$M_2u^2 + v^2 + M_1M_3w^2 = 0. \tag{3}$$

Note that if the greatest common divisor of u,v and w is larger than 1, then by dividing it out, this solution (u, v, w) can be further reduced.

Now we take this (u, v, w) and generate a solution (x, y, z) for (1) in its CM-range in the following manner:
First we take

$$z = |M_1M_2w|\,; \tag{4}$$

and then we set

$$y = M_1.\,(\,v.S(M_{2,3}) - M_{2,3}z\,)\,.S(M_2) \quad ; \tag{5}$$

and finally we set

$$x = M_2\ (\,uS\,(dy + ez) - dy - ez\,)\ S(M_1). \tag{6}$$

where S is the sign-function (4.3.4).

Now the above x, y and z constitute a solution of (1) within its CM-range.

In subsequent sections we will refer to this algorithm as the CM-algorithm for (1).

5.6 The Status Quo

At this point we know that when the Legendre's equation:

$$ax^2 + by^2 + cz^2 = 0 \qquad (\underline{1})$$

is nontrivially solvable, the Dirichlet's algorithm of §4.3 produces a nontrivial solution which of course could be far beyond the Holzer's range. In order to arrive at a solution within the Holzer's range one applies the Mordell's algorithm of §5.3 on the solution obtained by the Dirichlet's method. And we also saw that by the CM-algorithm of the previous section one could get a CM-solution of a nontrivially solvable general ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0. \qquad (\underline{2})$$

In fact this CM-solution obtained is nothing but an H-solution of (2) in the case when $d = e = f = 0$, from which we conclude that the concept of CM-limits is a generalization of the Holzer's limits. Also note that the CM-algorithm uses both the Dirichlet's algorithm of §4.3 and the Mordell's algorithm of §5.3 .

At this point one naturally should aspire to look at the other solutions which are also within the Holzer's range in the case of (1), or within the CM-range in the case of the equation (2). Note that if all the H-solutions or the CM-solutions can be detected, one among them would be the minimum solution for the corresponding equation, the detection of which could be regarded as one of the most desirable goals one can think of in this context.

We are going to explore along this line in our next chapter.

Chapter 6

RAYS OF SOLUTIONS: THE CM–RAYS

6.1 The Goal

As pointed out at the end of the previous chapter, now we are going to search for all the H-solutions of

$$ax^2 + by^2 + cz^2 = 0 \qquad (\underline{1})$$

after one such solution is obtained by the algorithms of Dirichlet and Mordell.

First we observe that even though the solution-generating formula of §3.5 has the potential to produce all the solutions of (1), its inability to control the sizes of the generated solutions compels one to seek for other algorithms in order to find the remaining solutions within the Holzer's range, the ultimate optimism being centered at the minimal nontrivial solution. In fact finding all the solutions including the minimal solution within the Holzer's range of (1) is the central goal of this chapter.

After preparing a geometric setting in the next section, in §6.3 we plan to deal with the equation (1) in which the coefficients a, b and c are noncomposite. We accomplish this by breaking all the possibilities into several special cases and then treating them one after another in the order of their increasing complexities. Then in §6.4 we deal with the case of composite coefficients.

By the time we are through with §6.4, we will be finding that all the solutions of the equation (1) lying within its Holzer's range are not haphazardously scattered in that region, on the other hand, they are very systematically aligned along some well-determined rays, which we call here as the CM-rays.

In §6.5 we develop an algorithm for finding the CM-rays of $ax^2 + by^2 + cz^2 = 0$ which lie in the positive octant of the three-dimensional Euclidean space. We do not speak about the others, since they are mere reflections of these positive-octant-rays or the PCM-Rays. Then in §6.6 we observe how similar rays can be detected in the context of the general homogeneous ternary quadratic equation:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$

Then in §6.7, after defining two functions: namely C and PCM from $\mathbb{Z}_*^3$ to $\mathbb{Z}_+$, we have observed that our main result concerning the CM-rays translates to an inequality involving these two functions.

Then we have concluded this chapter in §6.8 with some numerical tables presenting a number of Legendre's equations along with the complete lists of their PCM-rays. If we classify all the Legendre's equations on the basis of how many prime factors they have in their square-free coefficients, each of the equations presented here, with the only exception of the very last one, has the maximum possible number of PCM-rays for its class. And in the case of the last equation, each of whose coefficients is a composite number, there are 31 PCM-rays, whereas the maximum number possible for its class is 32.

Now let us start with the description of the necessary geometric background.

6.2 The Geometric Setting And The Concept of CM-Rays

In the environment of the cone:

$$ax^2 + by^2 + cz^2 = 0 \tag{1}$$

let the parallelopiped:

$$(|x|, |y|, |z|) \leq \left(\left\lfloor\sqrt{|bc|}\right\rfloor, \left\lfloor\sqrt{|ac|}\right\rfloor, \left\lfloor\sqrt{|ab|}\right\rfloor\right),$$

defined by the Holzer's limits, be called the H-box, and its faces the H-faces. To be more definite, let the face of the H-box with strictly negative x-coodinates and parallel to the yz-plane be called the first face of the H-box or the HF_1, and the other face parallel to HF_1 be referred to as the fourth H-face or the HF_4. Similarly, let the faces parallel to the xz-plane be HF_2 and HF_5, and the ones parallel to the xy-plane be referred to as HF_3 and HF_6 respectively.

Let the central rectangular section of the H-box by the yz-plane be called the First Parallel H-Section, or the LHS_1, and the other two similar sections by the xz- and xy-planes be referred to as LHS_2 and LHS_3 respectively.

Note that for the above H-box there are two diagonal plane sections containing the x-axis . Let the one passing through the positive octant, (where all the coordinates are nonnegative), be called the First Diagonal H-section, or DHS_1, and the other diagonal section containing the x-axis be referred to as DHS_4. Similarly, let the pair of diagonal sections containing the y-axis be DHS_2 and DHS_5 , and those containing the z-axis be DHS_3 and DHS_6 respectively.

Let the part of the H-box which lies in the positive octant be called the PH-box, and its faces be referred to as the PH-faces. Again to be more definite, let its face coinciding with the yz-plane be called the first positive H-face or PF_1, and the other face parallel to this PF_1 be the PF_4. Similarly, the other two pairs of faces

corresponcing to the xz- and xy-planes be referred to as PF_2 & PF_5 and PF_3 & PF_6 respectively. Let the setions of this PH-box through its center by planes parallel to the LHS_i and DHS_j be denoted by LPS_i and DPS_j respectively where $i = 1, 2$ or 3 and $j = 1, 2, 3, 4, 5$ or 6.

Note that all the other subregions of the H-box secluded in the remaining seven octants, alongwith similar sections of theirs could be denoted with no ambiguity by symbols such as $H_{(+,-,+)}$-box, $LH_{(+,-,+)}S_i$, or $DH_{(-,+,-)}S_j$ with $i = 1, 2$ or 3, and $j = 1, 2, 3, 4, 5$ or 6. Also it may be worth noting that in the above symbolic terminology we have used the letters D, F, H, L, P and S to indicate the terms Diagonal, Face, Holzer, paraLlel, Positive and Section respectively.

At this point, while restraining ourlelves from any further elaborate generalization of these symbols, we confess that even though we are not going to use all the above symbolisms in the present chapter, we have intentionally gone a little beyond our immediate need in order to accommodate some of our deeper observations in Chapter-7 in the form of some open problems and conjectures , which, of course, are formed in the light of a large number of computational evidences.

Now, let the straight-lines on the cone (1) passing through the origin $(0, 0, 0)$ be termed as rays, and the portion of any ray starting at the origin and lying in the positive-octant be called a positive ray. The portion of any ray starting from the origin and lying inside the H-box will be called an H-ray, and its portion inside the PH-box will be called a positive Holzer's ray, or an H_+-ray.

Any H-ray containing a nontrivial lattice point, (i.e., different from $(0, 0, 0)$), will be called a CM-ray. A CM-ray containing exactly one lattice point will be referred to as a singleton CM-ray, or an SCM-ray, but if it contains more than one lattice point it will be called a multiple CM-ray, or an MCM-ray. A CM-ray lying in the positive octant will be referred to as a positive CM-ray or a PCM-ray. Similarly a CM-ray lying in the negative octant, (i.e., the octant in which all the components are negative), will be referred to as a negative CM-ray, or an NCM-ray. A CM-ray which is neither negative nor positive will be referred to as an indefinite CM-ray or an ICM-ray. Note that according to our convention the PCM- and NCM-rays of (1) have to occur in pairs as reflections of each other.

Similarly in the case of SCM- or MCM-rays, when they are positive or negative or indefinite, if necessary, the adjectives SCM and MCM could be augmented by the initial letters P or N or I respectively to denote the type of octant in which the ray is positioned. Note that corresponding to any given CM-ray of (1), there is one PCM-, one NCM- , and six ICM-rays such that the absolute values of the corresponding components of all the eight rays are the same, possibly differing only in their signs.

At this point we assert that the search for these CM-rays for various cases of the Legendre's equation:

$$ax^2 + by^2 + cz^2 = 0 \qquad (1)$$

is going to be the main objective in the remainder of this chapter.

However, before we start working on that, let us have a pictorial presentation of the above geometic concepts.

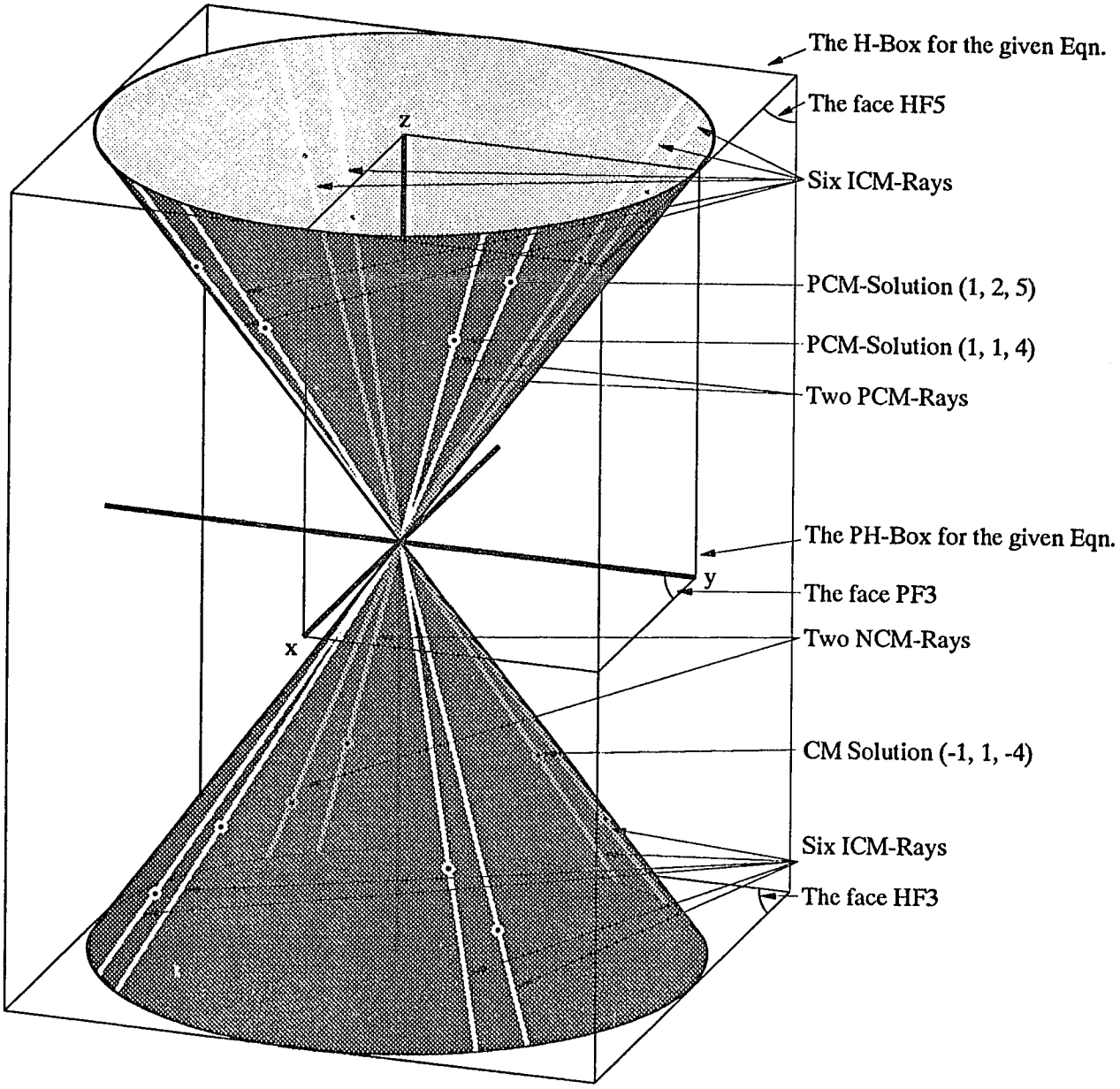

Figure 6.1: The sixteen CM-Rays of the Legendre's Equation: $13x^2 + 3y^2 - z^2 = 0$ which has twelve Indefinite CM-Rays, two Positive CM-Rays and two Negative CM-Rays

6.3 In Search of The CM-Rays: Noncomposite Coefficients

For the equation:

$$ax^2 + by^2 + cz^2 = 0 \qquad (\underline{1})$$

with a, b, c as nonzero integers and abc square-free, let us reiterate our assumption that by solutions we will mean only the nontrivial, primitive, and nonnegative integral solutions. Note that the primitivity of a solution compels its components to be pairwise prime.

Now, without any loss of generality we will assume $b \geq a > 0$, so that $a = b$ only when both a and b are equal to 1. Note that with this assumption we are forcing c to be negative for the nontrivial solvability of $(\underline{1})$.

When $[x, y, z] = [x_1, y_1, z_1]$ is a solution of $(\underline{1})$, we will say that any of:

$$\{x_1, y_1, z_1\}, \quad \{y_1, x_1, z_1\}, \quad \cdots \quad \{z_1, x_1, y_1\}$$

is a pseudo-solution of $(\underline{1})$, the components of which may not be in the same order as in $[x_1, y_1, z_1]$.

Let us now look for the PCM-rays of various cases of the equation:

$$ax^2 + by^2 + cz^2 = 0.$$

For us, in this section, the absolute value of any of the coefficients could be either 1, or 2, or an odd prime. Note that for any nontrivially solvable equation $ax^2 + by^2 + cz^2 = 0$ with $abc \neq 0$, we are assuming exactly one coefficient to be negative. And moreover, looking at the following table:

Table 6.1: The Sign-Dependence of the CM-Rays

Equation		*The set of H_+-solutions*
$x^2 + 2y^2 - 7z^2 = 0$		Φ
$x^2 - 2y^2 + 7z^2 = 0$		$\{[1, 2, 1]\}$
$-x^2 + 2y^2 + 7z^2 = 0$		$\{[3, 1, 1]\}$

we observe that the number of CM-rays definitely depends on which of the coefficients is with a sign different from the other two. Now, in view of these two observations and our assumption about the coefficients restricting their absolute values to be either 1 or a prime, we classify all the possibilities for (a, b, c) to the following cases:

$$\begin{array}{lll} (1,1,-1); & (1,-1,p); & (1,1,-p); \\ (p,q,-1); & (-p,q,1); & (p,q,-r); \end{array}$$

where p,q and r are primes.

Except the third case of $(1,1,-p)$, we will treat the remaining classes indivisually. Only in the case of $(1,1,-p)$, for the convenience of stating a result more concisely, we break it into two cases of $(1,1,-2)$, and $(1,1,-p)$, where p is an odd prime. Thus we have divided all the possibilities up to the primal coefficients into seven cases, and now let us deal with them one by one. We start with the most trivial case:

CASE-I: $(a,b,c) = (1,1,-1)$

Observation. *Clearly* $[1,0,1]$ *and* $[0,1,1]$ *are the only* H_+*-solutions of the Pythagorean equation* $x^2+y^2=z^2$*, so that there are exactly two PCM-rays, each of which obviously is a singleton.* (2)

CASE-II: $(a,b,c) = (1,-1,p)$, with p as a prime.

Clearly $[k,k,0]$ is an H_+-solution of

$$x^2 - y^2 + pz^2 = 0 \tag{3}$$

where k is a positive integer with $1 \leq k \leq \lfloor\sqrt{p}\rfloor$. Now

$$(3) \Rightarrow pz^2 = y^2 - x^2 = (y+x)(y-x).$$

And since for an H-solution the absolute values of both x and y have to be smaller than $\sqrt{p}$, we observe that there cannot be any H_+-solution with either $p|(y+x)$ or $p|(y-x)$, as a consequence of which we conclude that in this case of $(a,b,c) = (1,-1,p)$, the above trivial solutions are the only H_+-solutions, and consequently we have the following:

Proposition. *When* p *is an odd prime, there exists a unique PCM-ray for* $x^2+py^2 = z^2$*, which is a singleton (i.e., SCM) for* $p=3$*, but multiple (i.e., MCM) for* $p>3$. (4)

CASE-III: $(a,b,c) = (1,1,-2)$

Observation. *In this case of* $x^2+y^2 = 2z^2$*, obviously there is only one PCM-ray which is a singleton containing the only* H_+*-solution* $[1,1,1]$. (5)

CASE-IV: $(a, b, c) = (1, 1, -p)$ with p as an odd prime.

This, in fact, is the first nontrivial case. Here,

$$\begin{aligned} & x^2 + y^2 = pz^2 && ((\underline{1})) \\ \Rightarrow \quad & x^2 \equiv -y^2 \pmod{p} \\ \Rightarrow \quad & \left(\frac{y}{x}\right)^2 \equiv -1 \pmod{p} && ((\underline{2})) \end{aligned}$$

which demands the prime p to be of the form $4m + 1$ for the nontrivial solvability of $((\underline{1}))$. Conversely, whenever the prime p is of the form $4m + 1$, by Legendre's theorem, $((\underline{1}))$ is nontrivially solvable, and therefore by Holzer's theorem there exists an H-solution whose z-component must be 1, whereby the corresponding PCM-ray has to be a singleton. Also since $((\underline{2}))$ demands x- and y-components to be unequal, by interchanging them one gets another H-solution, and consequently another distinct singleton PCM-ray for $((\underline{1}))$.

Moreover, since more than 2 PCM-rays will demand more than two solutions of $\frac{y}{x}$ satisfying $((\underline{2}))$, which is impossible since p is prime, we finally conclude that:

Proposition. *For an odd prime p, $x^2 + y^2 = pz^2$ is nontrivially solvable if and only if p is of the form $4m+1$, and when solvable it has exactly two positive SCM-rays.* (6)

CASE-V: $(a, b, c) = (p, q, -1)$ where p and q are distinct primes.

In this context we claim the following:

The Primal Ray Theorem. *If a and b are distinct primes, then the equation $ax^2 + by^2 = z^2$ has at most two PCM-rays.* (7)

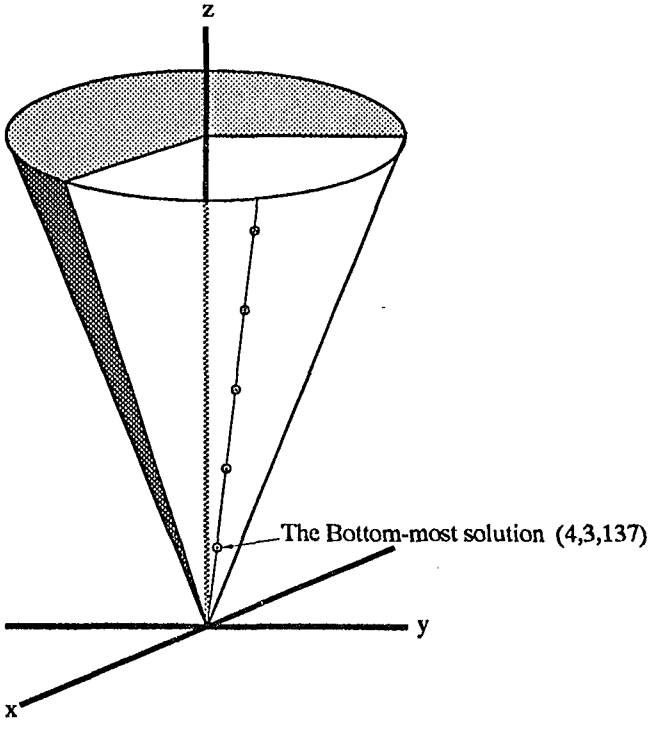

Fig.6.2

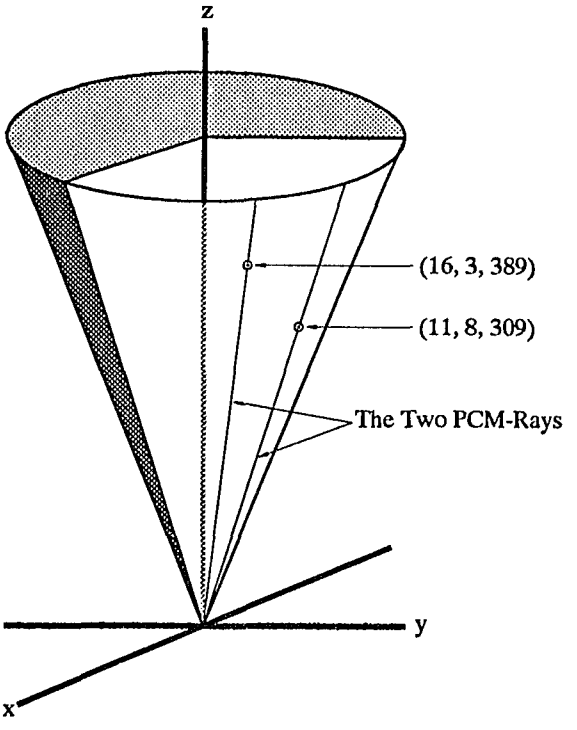

Fig.3

Two possible Distributions of PCM-Rays:

Figure 6.2: A Single PCM-Ray of $853x^2 + 569y^2 - z^2 = 0$;

Figure 6.3: Two PCM-Rays of $577x^2 + 401y^2 - z^2 = 0$

Proof:

$$ax^2 + by^2 = z^2 \qquad ((1))$$

$$\Rightarrow y^2 \equiv \frac{z^2}{b} \pmod{a} \qquad ((2))$$

which implies that for a fixed value of z,

$$y \equiv \pm\frac{z}{\sqrt{b}} \pmod{a}.$$

Since for an H_+-solution y has to be smaller than $\sqrt{a}$, we observe that within the Holzer's range, for a fixed value of z there can be at best one value of y satisfying ((1)).

A similar argument with

$$x \equiv \pm\frac{z}{\sqrt{a}} \pmod{b}$$

leads to the conclusion that within the Holzer's range, for a fixed value of z there could be at most one H_+-solution. Therefore if there is a solution with $z = 1$, then clearly all the H_+-solutions lie along one ray, yielding only one PCM-ray.

Now let us see why there could be at most two rays containing positive H-solutions.

Let us reiterate our assumption that $a < b$, and also, since ((1)) is nontrivially solvable, let us assume that the uniquely determined pair of square-roots of a modulo b are a_1 and a_2 with $a_1 + a_2 = b$.

First we observe that when x- and z-values of a point on the cone ((1)) are given, they determine the corresponding value of y by the equation: $ax^2 + by^2 = z^2$. Therefore it is enough to consider only the two congruences:

$$z \equiv \pm x\sqrt{a} \pmod{b} \qquad ((3))$$

Now we claim that the solutions of the congruence:

$$z \equiv xa_1 \pmod{b} \qquad ((4))$$

in ((3)) which correspond to the positive H-solutions of ((1)) must lie on a single ray, and similarly the other congruence:

$$z \equiv xa_2 \pmod{b} \qquad ((5))$$

could determine another ray. As a consequence, there could be at most two rays containing positive H-solutions.

Let us establish our claim for

$$z \equiv xa_1 \pmod{b},$$

and the theorem will follow by a similar treatment of ((5)). Now, let

$$S_1 = \{\, (x, z) \mid z \equiv xa_1 \pmod{b} \text{ with } 1 \leq x < \sqrt{b}, \quad 0 < z < b \,\}.$$

Let us arrange the elements of S_1 in the non-decreasing order of their z-values, and let this ordered set be

$$S = \{ (x_1, z_1), (x_2, z_2), \cdots, (x_m, z_m) \}.$$

Thus when S has more than one element, for $i < j$, we have $z_i \leq z_j$, and also clearly the x_i's are distinct positive integers within the range of 1 to $\lfloor \sqrt{b} \rfloor$. Now we claim that the z_i's also have to be distinct, because

$$\begin{aligned} z_i = z_j &\Leftrightarrow x_i a_1 \equiv x_j a_1 \pmod{b} \\ &\Leftrightarrow x_i \equiv x_j \pmod{b} \\ &\Leftrightarrow x_i = x_j, \end{aligned}$$

since both x_i and x_j are positive integers strictly smaller than $\sqrt{b}$.

Now, since z_1 is the smallest and z_2 is the second smallest value of z, and, $0 < z_2 - z_1 < z_2$,

$$\begin{aligned} & z_2 - z_1 \equiv a_1(x_2 - x_1) \pmod{b} \\ \Rightarrow\ & z_2 - z_1 \equiv z_1 \pmod{b} \\ \Rightarrow\ & z_2 \equiv 2z_1 \pmod{b} \end{aligned}$$

Therefore both z_1 and z_2 being positive and smaller than b and $z_2 > z_1$, we must have

$$\begin{array}{ccc} z_2 & = & 2z_1 \\ \| & & \| \\ a_1 x_2 & \equiv & 2a_1 x_1 \pmod{b} \end{array} \qquad (\underline{(6)})$$

$$\Rightarrow\ x_2 \equiv 2x_1 \pmod{b}, \quad (\text{since } G(a_1, b) = 1)\ .$$

Now we know that $b > a \geq 2 \Rightarrow b \geq 3$. Since $x_i < \sqrt{b}$, in order to have distinct x_1 and x_2 we must have $b > 4$. Therefore, with $b > 4$, and both x_1 and x_2 as positive integers smaller than $\sqrt{b}$,

$$x_2 \equiv 2x_1 \pmod{b} \Rightarrow x_2 = 2x_1. \qquad (\underline{(7)})$$

Thus, ($\underline{(6)}$) and ($\underline{(7)}$) imply

$$(x_2, z_2) = 2(x_1, z_1).$$

Now obviously for $i \geq 1$, if (x_{i+1}, z_{i+1}) is in S, then

$$z_{i+1} = z_i + z_1, \quad \& \quad x_{i+1} = x_i + x_1,$$

because, clearly

$$z_{i+1} \leq z_i + z_1.$$

Now if $z_{i+1} < z_i + z_1$, then

$$z_{i+1} - z_i < z_1, \quad \textit{and} \quad z_{i+1} - z_i \equiv a_1(x_{i+1} - x_i) \pmod{b}$$

yield contradiction to the fact that z_1 is the smallest z-value for the pairs in S or S_1.

Thus S_1 consists of distinct multiples of its smallest pair, which geometrically implies that all the corresponding solutions of ((1)) lie along one ray.

Thus whenever ((1)) is nontrivially solvable, its positive H-solutions whose x- and z- component-pairs are in S_1, must lie along a single ray.

Now after a similar treatment of the congruence ((5)), we are through with the proof of this Primal-Ray-Theorem. □

Let us observe something about the rays in this theorem. Let x_1 be the smallest positive integral value of x satisfying the congruence:

$$z \equiv xa_1 \pmod{b},$$

and be such that the radical $\sqrt{(z^2 - ax^2)/b}$ is an integer, which of course is the corresponding value for y in ((1)). Let the corresponding point on the cone be (x_1, y_1, z_1), which in fact is either the smallest or the second smallest solution of ((1)) depending on the existence, and if it exists, on the size of the corresponding solution obtained from

$$z \equiv xa_2 \pmod{b},$$

satisfying the integrality condition of $\sqrt{(z^2 - ax^2)/b}$. We note that if there is no second solution yielding integral value to $\sqrt{(z^2 - ax^2)/b}$, then there must be only one PCM-ray, and moreover, even under such circumstances, this existing ray may contain only one positive H-solution, because sometimes the size of z in the starting smallest solution being larger than $\sqrt{ab}/2$, it does not leave enough room for the second solution along the ray to be within the Holzer's limit. Some of such examples for $ax^2 + by^2 = z^2$ are:

Table 6.2: Some Legendre's Equations with Unique H-Solutions

(a,b,x,y,z) =			
	(2,7,1,1,3)	(2,199,9,1,19)	(3,193,1,1,14)
	(7,37,3,1,10)	(7,113,4,1,15)	(7,149,5,1,18)
	(13,17,1,2,9)	(13,107,1,2,21)	(17,43,3,1,14)
	(17,191,7,1,32)	(19,101,5,1,24)	(19,157,6,1,29)
	(23,73,4,1,21)	(23,101,5,1,26)	(109,173,2,5,69)
	...	...	...

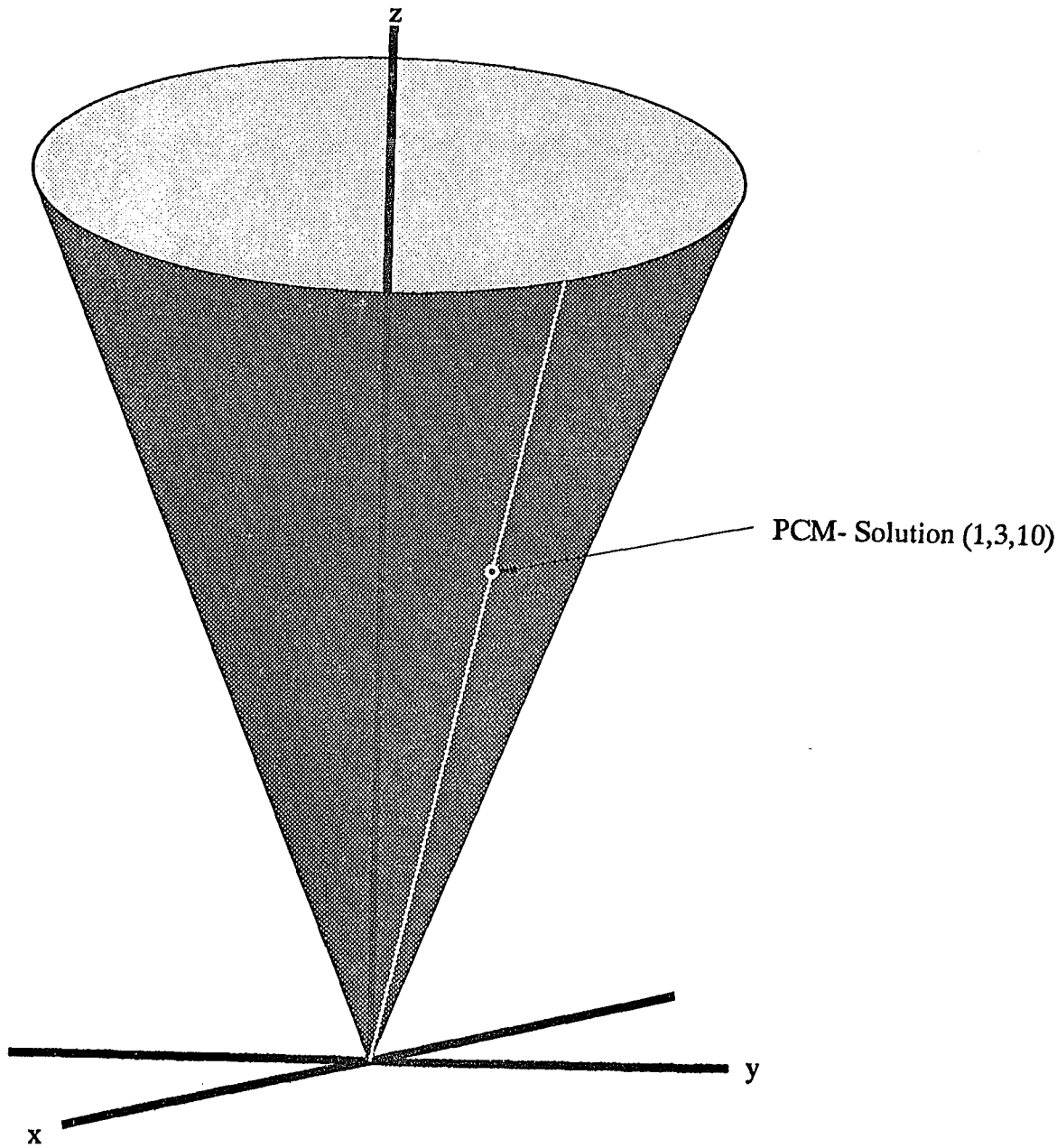

Figure 6.4: The Unique Singleton PCM-Ray of the Eqn.: $37x^2 + 7y^2 - z^2 = 0$.

Now before we deal with the next general case, let us look at a particular example of the CASE-V, namely $(a,b,c) = (2,p,-1)$ where p is an odd prime. Note that in the primal-ray-theorem when $a = 2$, for an H_+-solution we must have $y = 1$, i.e., we must have

$$\begin{aligned} 2x^2 + b = z^2 &\Rightarrow 2x^2 \equiv z^2 \pmod{b} \\ &\Rightarrow z \equiv \pm x\sqrt{2} \pmod{b}. \end{aligned}$$

Now if z_1 corresponds to one H_+-solution, then the second value of z, say z_2, with $0 < z_2 < b$ satisfying the above congruence must be equal to $b - z_1$. But since z_1 corresponds to an H_+-solution we must have $z_1 \leq \sqrt{2b}$, which implies that

$$z_2 \geq b - \sqrt{2b} = \sqrt{b}(\sqrt{b} - \sqrt{2}).$$

Therefore, when

$$\begin{aligned} \sqrt{b} - \sqrt{2} &> \sqrt{2}, \\ \text{or} \quad \sqrt{b} &> 2\sqrt{2}, \\ \text{or} \quad b &> 8, \end{aligned}$$

z_2 cannot be within the Holzer's range. Now since 2 is a quadratic residue of a prime p if and only if p is of the form $8m+1$ or $8m-1$, and therefore, for the only remaining nontrivially solvable equation $2x^2+7y^2 = z^2$ there being only one H_+-solution, namely $[1,1,3]$, we conclude that:

Theorem. *For an odd prime p, $2x^2 + py^2 = z^2$ is solvable if and only if p is of the form $8m+1$ or $8m-1$; and when solvable it has only one PCM-ray which again is a singleton.* (8)

CASE-VI: $(a,b,c) = (-p,q,1)$,

where p and q are distinct primes.
Here we claim the following:

Theorem. *If a and b are distinct primes, then the equation $ax^2 - by^2 = z^2$ has at most two PCM-rays.* (9)

Proof. Since the positive- or negativeness of the coefficients do not affect the reasonings in the primal-ray-theorem (7), essentially the same proof validates this theorem. □

As in the case of the primal-ray-theorem, we can make similar observations in this context.

For example, let us look at the

PARTICULAR CASE: $(a,b,c) = (-2,p,1)$, where p is an odd prime.

Note that in this case of: $2x^2 - py^2 = z^2$, an H_+-solution must have $y = 1$. Then, with exactly identical arguments as in the case of Theorem-(8), we conclude that:

Theorem. *For an odd prime p, $2x^2 - py^2 = z^2$ is solvable if and only if p is of the form $8m+1$ or $8m-1$, and when solvable it has only one PCM-ray which again is a singleton.* □ (10)

Also let us look at another particular example of the **CASE-VI**, namely $(a,b,c) = (a,-p,1)$ where $a = 2$ or 3 and p is an odd prime different from a. First let us have the following:

Lemma. *Let a be either 2 or 3. Then the number of representations of a prime $p > a$ in the form:*

$$p = x^2 + ay^2, \qquad x > 0, y > 0 \tag{(1)}$$

is equal to half the number of solutions of the congruence

$$z^2 + a \equiv 0 \pmod{p}. \tag{(2)}$$

(11)

Proof:

$$\begin{aligned} p &= x^2 + ay^2 \\ \Rightarrow x^2 &\equiv -ay^2 \pmod{p} \\ \Rightarrow x &\equiv \sqrt{-a}\, y \pmod{p} \\ \Rightarrow x &\equiv zy \pmod{p} \end{aligned}$$

where $z^2 \equiv -a \pmod{p}$, or z is a solution of ((2)).

Let us say that these solutions (x,y) of ((1)) and z of ((2)) are associated solutions. Clearly one solution of ((2)) does not yield more than one associated solution from ((1)) with $x > 0$ and $y > 0$, for,

$$\begin{aligned} z_0 \equiv \frac{x_1}{y_1} &\equiv -\frac{x_2}{y_2} \pmod{p} \\ \Rightarrow x_1 y_2 &\equiv -x_2 y_1 \pmod{p}. \end{aligned}$$

Since each of x_1, x_2, y_1 and y_2 is smaller than $\sqrt{p}$, we have

$$x_1 y_2 = -x_2 y_1$$

from which, because $G(x_1, y_1) = 1 = G(x_2, y_2)$, we conclude that

$$|x_1| = |x_2| \quad \text{and} \quad |y_1| = |y_2|\,.$$

Thus the distinct solutions can differ only in their signs, and the corresponding solutions with only positive components have to be equal.

Again, if z_0 is a solution of ((2)), it is an easy exercise through the arguments relating to the Farey series of $\sqrt{p}$ that we can have integers P and Q, and a real number θ such that

$$\frac{z_0}{p} = \frac{P}{Q} + \frac{\theta}{Q\sqrt{p}}; \quad G(P,Q) = 1, \quad 0 < Q \le \sqrt{p} \quad \text{and} \quad |\theta| < 1,$$

implying

$$z_0 Q \equiv \theta\sqrt{p} \pmod{p}$$
$$\Rightarrow z_0 \equiv \frac{\tau}{Q} \pmod{p} \qquad ((\underline{3}))$$

where $\tau = \theta\sqrt{p}$ with $|\tau| < \sqrt{p}$.
Now,

$$((\underline{2})) \text{ and } ((\underline{3})) \Rightarrow \tau^2 + aQ^2 \equiv 0 \pmod{p}.$$
$$\text{But, } 0 < \tau^2 + aQ^2 < (1+a)p.$$

Therefore, for $a = 2$, we must have

$$\text{either } \tau^2 + 2Q^2 = p \qquad ((\underline{4}))$$

$$\text{or, } \tau^2 + 2Q^2 = 2p. \qquad ((\underline{5}))$$

If ((5)) is true then τ is even, and therefore if $\tau = 2r_1$, then

$$p = Q^2 + 2r_1^2.$$

Thus when $a = 2$, we have a solution to ((1)) which is $(x, y) = (\tau, Q)$ or (Q, r_1). And when $a = 3$, we must have

$$\tau^2 + 3Q^2 = p, \quad \text{or} \quad 2p, \quad \text{or} \quad 3p.$$

The second case is impossible since modulo 4 the left side is 1 or 0 whereas the right side is 2. And in the third case τ is a multiple of 3, say $|\tau| = 3r_1$, as a result of which we have

$$p = Q^2 + 3r_1^2.$$

Thus when $a = 3$, we have a solution of ((1)) which is $(x, y) = (\tau, Q)$ or (Q, r_1).

Also clearly for each solution of ((1)) there corresponds a solution of ((2)), and for no solution of ((1)) we can have two distinct solutions of ((2)), since in such a case we must have

$$\frac{x_1}{y_1} \equiv -\frac{x_1}{y_1} \pmod{p},$$

which is impossible alongwith $x_1 > 0$ and $y_1 > 0$.

Now with the above arguments, the proof of our lemma is complete. □

Now since -2 is a quadratic residue of p if and only if p is of the form $8m+1$ or $8m+3$, and for an H_+-solution of $px^2 - 2y^2 = z^2$, x must be 1, in view of the above lemma we have the following:

Proposition. *For an odd prime p, $px^2 - 2y^2 = z^2$ is solvable if and only if p is of the form $8m+1$ or $8m+3$. Moreover, when solvable it has exactly one PCM-ray, and this unique PCM-ray is a singleton.* □ (12)

Also note that when $(a, b, c) = (1, 3, -p)$ with p as an odd prime, in view of the Lemma(11) and the fact that -3 is a quadratic residue of p if and only if p is of the form $6m+1$, we have established the validity of the following:

Proposition. *For an odd prime p, $px^2 - 3y^2 = z^2$ is solvable if and only if p is of the form $6m + 1$, and moreover, when solvable, it has exactly one PCM-ray, and this unique PCM-ray is a singleton.* □ (13)

Now, in view of (8),(10) and (12) we have the following:

Theorem. *When $|a| = 2$, $|b|$ is an odd prime, and $ax^2 + by^2 = z^2$ is nontrivially solvable, there is exactly one H_+-solution yielding only one PCM-ray which therefore is a singleton. In fact given the same initial conditions, this equation is nontrivially slovable if and only if*

either (i) $a = 2$ and $|b|$ is of the form $8m + 1$ or $8m - 1$;
or (ii) $a = -2$, $b > 0$ and is of the form $8m + 1$ or $8m + 3$. □ (14)

CASE-VII: $(a, b, c) = (p, q, -r)$, where p, q and r are distinct primes. In this case we claim the following:

Theorem. *If a, b and c are distinct primes, then the equation:*

$$ax^2 + by^2 = cz^2 \qquad ((1))$$

could have at most four PCM-rays. (15)

Proof: With no loss of generality, let us assume $a < b$. Now

$$\begin{aligned} & ax^2 + by^2 = cz^2 \\ \Rightarrow \quad & \sqrt{c}\, z \equiv \sqrt{a}\, x \pmod{b} \end{aligned}$$

where each of $\sqrt{c}$ and $\sqrt{a}$ has two values. Invoking the logic in the proof of our Primal-Ray-Theorem-(7), and observing that there are four pairs of possible values for (x, z), each of which could yield a ray if the corresponding y-values given by ((1)) are also integers, we infer that the maximum number of PCM-rays could be four. □

6.4 In Search of The CM-rays: Composite Coefficients

Now, given the equation: $ax^2 + by^2 + cz^2 = 0$, with abc square-free, let the coefficients a, b and c be composites. Let m_1, m_2 and m_3 be the numbers of distinct odd prime divisors of a, b and c respectively, and without any loss of generality let us assume that $m_1 \leq m_2 \leq m_3$.

Here we need the following:

Lemma. *Given $G(a,m) = 1$, and*

$$m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

as the prime factorization of m with the p_i's as distinct primes, the necessary conditions for the solvability of the congruence:

$$x^2 \equiv a \pmod{m}$$

are:

$$(i) \quad a \equiv \begin{cases} 1 \pmod 4 & \text{for } \alpha = 2 \\ 1 \pmod 8 & \text{for } \alpha \geq 3; \end{cases}$$

and, $$(ii) \quad \left\| \frac{a}{p_i} \right| = 1 \quad \vdash \quad i = 1, 2, \ldots, k\,.$$

Moreover, if these conditions are satisfied, then the number of solutions for the above congruence is:

$$\begin{array}{ll} 2^k & \text{for } \alpha = 0 \text{ or } 1, \\ 2^{k+1} & \text{for } \alpha = 2, \text{ and} \\ 2^{k+2} & \text{for } \alpha \geq 3. \end{array} \qquad (1)$$

Proof: *Refer (13).* □

In view of this lemma, the arguments in the Primal-Ray-Theorem-(7) and the Theorem-(9) immediately yield the following:

Proposition. *If m_2 and m_3 are the numbers of distinct odd prime divisors of b and c respectively with bc square-free and $m_2 \leq m_3$, then the equation $x^2 + by^2 + cz^2 = 0$ has at most 2^{m_3} PCM-rays.* □ (2)

Now when $1 \leq m_1 \leq m_2 \leq m_3$, by using the Lemma-(1), from $ax^2 + by^2 + cz^2 = 0$ we deduce that the numbers of solutions for the congruences:

$$\frac{x^2}{y^2} \equiv -\frac{b}{a} \pmod{c},$$

and

$$\frac{x^2}{z^2} \equiv -\frac{c}{a} \pmod{b}$$

are 2^{m_3} and 2^{m_2} respectively.

Therefore, since each distinct pair of values for

$$\frac{x}{y} \pmod{c} \quad \text{and} \quad \frac{x}{z} \pmod{b}$$

could yield a distinct PCM-ray, in the light of the arguments in the Primal-Ray-Theorem, we conclude that the number of PCM-rays could be as high as $2^{m_2}.2^{m_3}$ or $2^{m_2+m_3}$. Thus, in view of (2), we have the following:

The Composite Ray Theorem. *If a, b, c are integers with abc square-free, and m_1, m_2 and m_3 are the numbers of distinct odd prime factors of a, b and c respectively with $m_1 \leq m_2 \leq m_3$, then the number of PCM-rays for the equation $ax^2+by^2+cz^2 = 0$ is at most $2^{m_2+m_3}$ when $m_1 > 0$ and 2^{m_3} when $a = 1$.* (3)

Let us now devise an algorithm for detecting these PCM-rays.

6.5 An Algorithm For Finding The PCM-rays of: $ax^2 + by^2 + cz^2 = 0$

Let us assume the conditions on a, b, c as described in the beginning of the previous section, i.e., m_1, m_2 and m_3 are the numbers of distinct odd prime factors of a, b and c respectively with $m_1 \leq m_2 \leq m_3$.

Let

$$S = \left\{ s \mid s^2 \equiv -\frac{c}{a} \pmod{|b|} \right\},$$

and

$$Z = \left\{ z \mid z \in \mathbb{Z}, \quad 1 \leq z \leq \sqrt{|ab|} \right\}.$$

Now, for $s \in S$ and $z \in Z$, let

$$zs \equiv x \pmod{|b|} \qquad \text{with} \quad 0 < x < |b|.$$

If $x \leq \sqrt{|bc|}$, then collect all the triples (x_i, y_i, z) where

$$x_i = x + |b|\, i \qquad \text{with} \quad 0 \leq i \leq \left\lfloor \frac{\sqrt{|bc|} - x}{|b|} \right\rfloor,$$

and

$$y_i = \sqrt{-\frac{ax_i^2 + cz^2}{b}}$$

is an integer such that $G(x_i, y_i, z) = 1$. Let $C_{(s,z)}$ denote this collection for the fixed pair (s, z), and let

$$\mathbf{C} = \bigcup_{\substack{s \in S, \\ z \in Z}} C_{(s,z)}.$$

Now this **C** is the collection of the bottommost H_+-solutions along the PCM-rays of

$$ax^2 + by^2 + cz^2 = 0, \qquad (\underline{1})$$

and its cardinality, i.e., $\#\mathbf{C}$, represents the number of PCM-rays of (1).

6.6 PCM-rays of: $ax^2+by^2+cz^2+dxy+exz+fyz = 0$

As described in the algorithm of §5.5, starting with

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0, \qquad (\underline{1})$$

after getting the reduced diagonalized equation

$$ku'^2 + lv'^2 + mw'^2 = 0 \qquad (\underline{2})$$

we should collect its PCM-rays in the form of a set **C** as outlined in the previous section.

Now each solution in **C** being an H_+-solution of (2), we can apply on it the algorithm of §5.5 to get a CM-solution of (1). Thus eventually **C** produces a collection of CM-solutions for (1), say **C'**, each element of which is the bottom-most lattice-point along a CM-ray of (1). Note that eventhough the nontrivial solvability of (1) assures the existence of at least one CM-ray, the existence of any PCM-ray is by no means guaranteed.

6.7 An Inequality

Thus in this chapter we saw that the H-solutions of a nontrivially solvable Legendre's equation: $ax^2 + by^2 + cz^2 = 0$, (with abc square-free), lie along some CM-rays, and the number of these CM-rays is bounded by $8 \times 2^{m_2+m_3}$ or $2^{3+m_2+m_3}$ where m_2 and m_3 are as described in §6.4. Moreover, when $a = 1$, this bound is reduced to 2^{3+m_3}.

Now let us synthesize this finding in the form of an inequality. First let us define a function $C: \mathbb{Z}_*^3 \longrightarrow \mathbb{Z}_+$ as follows:

For a nonzero integer n, let $P(n)$ denote the number of distinct odd prime divisors of n. And, given three integers a, b and c, let

$$\begin{aligned} m_3 &= \max(P(a), P(b), P(c)), \\ m_1 &= \min(P(a), P(b), P(c)), \quad \text{and} \\ m_2 &= P(a).P(b).P(c) \div (m_1.m_3). \end{aligned}$$

(Note that here a, b and c are integers in any order and are also with any sign.) Then we define the function $C: \mathbb{Z}_*^3 \longrightarrow \mathbb{Z}_+$ by

$$C(a,b,c) = \begin{cases} 0 & \text{if } S(a) = S(b) = S(c), \\ 2^{m_3} & \text{when } 1 \in \{|a|, |b|, |c|\}, \\ 2^{m_2+m_3} & \text{when } 1 \notin \{|a|, |b|, |c|\}. \end{cases}$$

Note that each of $C(a,b,c)$, $C(a,c,b)$, $C(b,a,c)$, $C(b,c,a)$, $C(c,a,b)$ and $C(c,b,a)$ has the same value.

Now let us define another function:

$$PCM: \mathbb{Z}_*^3 \longrightarrow \mathbb{Z}_+$$

by setting the number of PCM-rays of the equation $ax^2 + by^2 + cz^2 = 0$ as the value of $PCM(a,b,c)$. We are going to call this number $PCM(a,b,c)$ as the *PCM-number* of the triple (a,b,c), as well as of the equation $ax^2 + by^2 + cz^2 = 0$.

It is now clear that when abc is square-free, what we have achieved in this chapter can be abbreviated to the inequality:

$$PCM(a,b,c) \leq C(a,b,c).$$

Here at this point we must expressly note that the above upper bound $C(a,b,c)$ is very rarely achieved by the Legendre's equations. After a large number of computations we have come across some few examples of Legendre's equations where

$$PCM(a,b,c) = C(a,b,c).$$

The next section is going to demonstrate some of these numerical examples.

6.8 Some Numerical Examples of The PCM-Rays

Here in this section we want to present a few tables of our computational results relating to the PCM-rays of some Legendre's equations. The letters p and c in the positions of the coefficients will denote that they are odd primes and composites respectively.

In any of the Tables, each row gives all the relevant information about one Legendre's Equation:

$$ax^2 + by^2 + cz^2 = 0 \qquad (1)$$

with its coefficients as a triple: (a,b,c) in the first column. If any of the coefficients is a composite integer, then its factorization is given just below this triple. The second column will give the Holzer's range as a triple of integers, which are the maximum integral values allowed for the corresponding components of any H-solution. The number of PCM-rays of (1) will be given in the third column. The next and the last column will present all the PCM-rays of (1) in the order of increasing heights of their bottom-most solutions so that the first ray contains the minimal solution of (1). Each PCM-ray is presented as a quadruple: $[x,y,z,n]$, in which (x,y,z) represents the bottom-most solution, and n is the number of H-solutions along that ray.

Table 6.3: PCM-Rays of: $(1, 1, -p)$

The Coefficients $(1, 1, -p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,1,-5)	(2,2,1)	2	[2,1,1,1], [1,2,1,1]
(1,1,-13)	(3,3,1)	2	[2,3,1,1], [3,2,1,1]
(1,1,-53)	(7,7,1)	2	[2,7,1,1], [7,2,1,1]
(1,1,-73)	(8,8,1)	2	[8,3,1,1], [3,8,1,1]
(1,1,-113)	(10,10,1)	2	[7,8,1,1], [8,7,1,1]
(1,1,-257)	(16,16,1)	2	[16,1,1,1], [1,16,1,1]

Table 6.4: PCM-Rays of: $(-1, 1, p)$

The Coefficients $(-1, 1, p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,1,5)	(2,2,1)	1	[1,1,0,2]
(-1,1,101)	(10,10,1)	1	[1,1,0,10]
(-1,1,139)	(11,11,1)	1	[1,1,0,11]
(-1,1,149)	(12,12,1)	1	[1,1,0,12]
(-1,1,953)	(30,30,1)	1	[1,1,0,30]
(-1,1,991)	(31,31,1)	1	[1,1,0,31]
(-1,1,997)	(31,31,1)	1	[1,1,0,31]

Table 6.5: PCM-Rays of: $(1, 2, -p)$

The Coefficients $(1, 2, -p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,2,-3)	(2,1,1)	1	[1,1,1,1]
(1,2,-17)	(5,4,1)	1	[3,2,1,1]
(1,2,-19)	(6,4,1)	1	[1,3,1,1]
(1,2,-41)	(9,6,1)	1	[3,4,1,1]
(1,2,-43)	(9,6,1)	1	[5,3,1,1]
(1,2,-73)	(12,8,1)	1	[1,6,1,1]
(1,2,-83)	(12,9,1)	1	[9,1,1,1]
(1,2,-107)	(14,10,1)	1	[3,7,1,1]
(1,2,-137)	(16,11,1)	1	[3,8,1,1]

Table 6.6: PCM-Rays of: $(1, -2, p)$

The Coefficients $(1, -2, p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,-2,7)	(3,2,1)	1	[1,2,1,1]
(1,-2,17)	(5,4,1)	1	[1,3,1,1]
(1,-2,31)	(7,5,1)	1	[1,4,1,1]
(1,-2,41)	(9,6,1)	1	[3,5,1,1]
(1,-2,47)	(9,6,1)	1	[5,6,1,1]
(1,-2,199)	(19,14,1)	1	[1,10,1,1]
(1,-2,977)	(44,31,1)	1	[9,23,1,1]

Table 6.7: PCM-Rays of: $(-1, 2, p)$

The Coefficients $(-1,2,p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,2,17)	(5,4,1)	1	[5,2,1,1]
(-1,2,71)	(11,8,1)	1	[11,5,1,1]
(-1,2,89)	(13,9,1)	1	[11,4,1,1]
(-1,2,103)	(14,10,1)	1	[11,3,1,1]
(-1,2,127)	(15,11,1)	1	[15,7,1,1]
(-1,2,137)	(16,11,1)	1	[13,4,1,1]
(-1,2,193)	(19,13,1)	1	[15,4,1,1]
(-1,2,257)	(22,16,1)	1	[17,4,1,1]
(-1,2,313)	(25,17,1)	1	[21,8,1,1]
(-1,2,991)	(44,31,1)	1	[33,7,1,1]
(-1,2,4567)	(95,67,1)	1	[75,23,1,1]

Table 6.8: PCM-Rays of: $(1, p, -p)$

The Coeffs. $(1,p,-p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,29,-1601)	(215,40,5)	2	[18,37,5,1], [53,20,3,1]
(1,73,-509)	(192,22,8)	2	[62,17,7,1], [157,2,7,1]
(1,83,-509)	(205,22,9)	2	[91,11,6,1], [129,10,7,1]
(1,167,-503)	(289,22,12)	2	[24,19,11,1], [63,13,8,1]
(1,197,-1601)	(561,40,14)	2	[242,19,9,1], [339,20,11,1]
(1,239,-509)	(348,22,12)	2	[65,17,12,1], [337,2,15,1]
(1,281,-509)	(378,22,16)	2	[183,10,11,1], [338,1,15,1]
(1,281,-929)	(510,30,16)	2	[3,20,11,1], [328,19,15,1]
(1,347,-503)	(417,22,18)	2	[246,1,11,1], [323,13,18,1]
(1,347,-1601)	(745,40,18)	2	[209,37,18,1], [363,20,13,1]
(1,353,-1601)	(751,40,18)	2	[492,25,17,1], [567,20,17,1]
(1,373,-1601)	(772,40,19)	2	[211,20,11,1], [386,29,17,1]
(1,431,-823)	(595,28,20)	2	[172,19,15,1], [373,21,20,1]
(1,439,-509)	(472,22,20)	2	[133,10,11,1], [277,17,20,1]
(1,863,-1601)	(1175,40,29)	2	[723,8,19,1], [949,5,24,1]

Table 6.9: PCM-Rays of: $(-1, p, p)$

The Coeffs. $(-1, p, p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,3,13)	(6,3,1)	2	[4,1,1,1], [5,2,1,1]
(-1,3,373)	(33,19,1)	2	[20,3,1,1], [31,14,1,1]
(-1,3,421)	(35,20,1)	2	[23,6,1,1], [28,11,1,1]
(-1,3,937)	(53,30,1)	2	[37,12,1,1], [38,13,1,1]
(-1,5,89)	(21,9,2)	2	[13,4,1,1], [19,1,2,1]
(-1,11,257)	(53,16,3)	2	[31,8,1,1], [46,13,1,1]
(-1,41,379)	(124,19,6)	2	[98,15,1,1], [105,11,4,1]
(-1,181,773)	(374,27,13)	2	[223,11,6,1], [327,22,5,1]
(-1,193,331)	(252,18,13)	2	[134,3,7,1], [239,7,12,1]
(-1,281,587)	(406,24,16)	2	[286,17,1,1], [301,17,4,1]
(-1,373,773)	(536,27,19)	2	[333,17,2,1], [433,22,3,1]
(-1,449,593)	(516,24,21)	2	[317,8,11,1], [497,23,4,1]
(-1,641,929)	(771,30,25)	2	[445,8,13,1], [685,19,16,1]
(-1,809,953)	(878,30,28)	2	[617,13,16,1], [797,28,1,1]

Table 6.10: PCM-Rays of: $(p, p, -p)$

The Coeffs. $(p, p, -p)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(23,431,-503)	(416,96,99)	4	[23,96,89,1], [183,64,71,1] [248,51,71,1], [408,19,89,1]
(79,383,-547)	(457,207,173)	4	[109,146,129,1], [190,119,123,1] [193,118,123,1], [274,91,129,1]
(811,953,-727)	(832,767,879)	4	[115,447,526,1], [425,371,618,1] [17,654,749,1], [625,438,829,1]

Table 6.11: PCM-Rays of: $(1, 1, -c)$

The Coeffs. $(1, 1, -c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,1,-65) $65 = 13.5$	(8,8,1)	4	[7,4,1,1], [4,7,1,1] [8,1,1,1], [1,8,1,1]
(1,1,-377) $377 = 13.29$	(19,19,1)	4	[16,11,1,1], [11,16,1,1] [19,4,1,1], [4,19,1,1]

Table 6.12: PCM-Rays of: $(-1, 1, c)$

The Coeffs. $(-1, 1, c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,1,105) 105 = 3.5.7	(10,10,1)	1	[1,1,0,10]
(-1,1,153) 153 = 3.3.17	(12,12,1)	1	[1,1,0,12]
(-1,1,231) 231 = 3.7.11	(15,15,1)	1	[1,1,0,15]
(-1,1,285) 285 = 3.5.19	(16,16,1)	1	[1,1,0,16]
(-1,1,555) 555 = 3.5.37	(23,23,1)	1	[1,1,0,23]
(-1,1,1000) 1000 = 2.2.2.5.5.5	(31,31,1)	1	[1,1,0,31]

Table 6.13: PCM-Rays of: $(1, 2, -c)$

The Coeffs. $(1, 2, -c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,2,-51) 51 = 3.17	(10,7,1)	2	[1,5,1,1], [7,1,1,1]
(1,2,-323) 323 = 17.19	(25,17,1)	2	[9,11,1,1], [15,7,1,1]
(1,2,-19393) 19393 = 11.41.43	(196,139,1)	4	[85,78,1,1], [95,72,1,1] [31,96,1,1], [139,6,1,1]
(1,2,-18791817) 18791817 = 3.11.17.19.41.43	(6130,4334,1)	32	[2435,2536,1,1], [2323,2588,1,1] [2657,2422,1,1], [2047,2702,1,1] [2015,2714,1,1], [1645,2836,1,1] [1603,2848,1,1], [1567,2858,1,1] [1345,2914,1,1], [1217,2942,1,1] [2947,2248,1,1], [637,3032,1,1] [577,3038,1,1] , [403,3052,1,1] [125,3064,1,1] , [3073,2162,1,1] [3233,2042,1,1], [3263,2018,1,1] [3347,1948,1,1], [3437,1868,1,1] [3517,1792,1,1], [3713,1582,1,1] [3907,1328,1,1], [3935,1286,1,1] [4115,964,1,1], [4127,938,1,1] [4193,778,1,1], [4225,686,1,1] [4243,628,1,1], [4255,586,1,1] [4285,464,1,1], [4333,92,1,1]

Table 6.14: PCM-Rays of: $(1, -2, c)$

The Coeffs. $(1, -2, c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,-2,119) 119 = 7.17	(15,10,1)	2	[3,8,1,1], [9,10,1,1]
(1,-2,161) 161 = 23.7	(17,12,1)	2	[1,9,1,1], [9,11,1,1]
(1,-2,697) 697 = 41.17	(37,26,1)	2	[5,19,1,1], [19,23,1,1]
(1,-2,12257) 12257 = 7.17.103	(156,110,1)	4	[15,79,1,1], [39,83,1,1] [71,93,1,1], [81,97,1,1]
(1,-2,33233) 33233 = 199.167	(257,182,1)	2	[7,129,1,1], [33,131,1,1]
(1,-2,3478727) 3478727 = 7.17.23.31.41	(2637,1865,1)	16	[129,1322,1,1], [165,1324,1,1] [319,1338,1,1], [351,1342,1,1] [481,1362,1,1], [545,1374,1,1] [555,1376,1,1], [789,1432,1,1] [859,1452,1,1], [1119,1538,1,1] [1215,1574,1,1], [1301,1608,1,1] [1345,1626,1,1], [1499,1692,1,1] [1579,1728,1,1], [1749,1808,1,1]

Table 6.15: PCM-Rays of: $(-1, 2, c)$

The Coeffs. $(-1, 2, c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,2,161) 161 = 7.23	(17,12,1)	2	[13,2,1,1], [17,8,1,1]
(-1,2,12257) 12257 = 7.17.103	(156,110,1)	4	[113,16,1,1], [115,22,1,1] [127,44,1,1], [143,64,1,1]
(-1,2,84847) 84847 = 7.17.23.31	(411,291,1)	8	[295,33,1,1], [297,41,1,1] [303,59,1,1], [313,81,1,1] [335,117,1,1], [353,141,1,1] [375,167,1,1], [407,201,1,1]

Table 6.16: PCM-Rays of: $(1, p, -c)$

The Coeffs. $(1, p, -c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,7,-22) $22 = 2.11$	(12,4,2)	2	[5,3,2,1], [9,1,2,1]
(1,7,-46) $46 = 2.23$	(17,6,2)	2	[3,5,2,1], [11,3,2,1]
(1,29,-1329) $1329 = 3.443$	(196,36,5)	4	[19,20,3,1], [94,29,5,1] [106,5,3,1], [181,4,5,1]
(1,887,-2457886) $2457886 =$ 2.1228943	(46692,1567,29)	2	[941,947,18,1], [16931,1245,26,1]

Table 6.17: PCM-Rays of: $(1, -p, c)$

The Coeffs. $(1, -p, c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,-17,461422) $461422 = 2.13.17747$	(2800,679,4)	4	[5,659,4,1], [703,371,2,1] [805,383,2,1], [2267,641,2,1]
(1,-17,251987) $251987 = 67.3761$	(2069,501,4)	4	[9,487,4,1], [485,501,4,1] [1545,394,1,1], [1991,498,1,1]

Table 6.18: PCM-Rays of: $(-1, p, c)$

The Coeffs. $(-1, p, c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,3,22) 22 = 2.11	(8,4,1)	2	[5,1,1,1], [7,3,1,1]
(-1,3,1261) 1261 = 13.97	(61,35,1)	4	[37,6,1,1], [43,14,1,1] [44,15,1,1], [56,25,1,1]
(-1,3,1969) 1969 = 11.179	(76,44,1)	4	[46,7,1,1], [49,12,1,1] [62,25,1,1], [71,32,1,1]
(-1,3,4393) 4393 = 23.191	(114,66,1)	4	[70,13,1,1], [74,19,1,1] [91,36,1,1], [101,44,1,1]
(-1,3,4654) 4654 = 2.13.179	(118,68,1)	4	[73,15,1,1], [79,23,1,1] [89,33,1,1], [101,43,1,1]
(-1,3,6313) 6313 = 59.107	(137,79,1)	4	[86,19,1,1], [94,29,1,1] [101,36,1,1], [115,48,1,1]
(-1,3,6526) 6526 = 2.13.251	(139,80,1)	4	[83,11,1,1], [97,31,1,1] [101,35,1,1], [133,61,1,1]
(-1,3,9694) 9694 = 2.37.131	(170,98,1)	4	[101,13,1,1], [109,27,1,1] [137,55,1,1], [163,75,1,1]
(-1,3,57937) 57937 = 11.23.229	(416,240,1)	8	[247,32,1,1], [250,39,1,1] [257,52,1,1], [265,64,1,1] [338,137,1,1], [358,153,1,1] [383,172,1,1], [398,183,1,1]
(-1,3,63349) 63349 = 11.13.443	(435,251,1)	8	[256,27,1,1], [257,30,1,1] [271,58,1,1], [289,82,1,1] [332,125,1,1], [368,155,1,1] [424,197,1,1], [431,202,1,1]
(-1,5,209) 209 = 11.19	(32,14,2)	4	[17,4,1,1], [23,8,1,1] [29,1,2,1], [31,5,2,1]
(-1,5,2519) 2519 = 11.229	(112,50,2)	4	[58,13,1,1], [82,29,1,1] [101,5,2,1], [109,19,2,1]
(-1,5,3421) 3421 = 11.311	(130,58,2)	4	[71,18,1,1], [89,30,1,1] [117,1,2,1], [123,17,2,1]
(-1,5,6821) 6821 = 19.359	(184,82,2)	4	[101,26,1,1], [139,50,1,1] [167,11,2,1], [173,23,2,1]
(-1,13,129) 129 = 3.43	(40,11,3)	4	[23,1,2,1], [29,5,2,1] [31,8,1,1], [37,4,3,1]
(-1,13,1257) 1257 = 3.419	(127,35,3)	4	[71,1,2,1], [85,13,2,1] [107,28,1,1], [121,16,3,1]
(-1,31,66) 66 = 2.3.11	(45,8,5)	4	[25,1,3,1], [29,5,1,1] [37,5,3,1], [41,1,5,1]

Table 6.19: PCM-Rays of: $(1, c, -c)$

The Coeffs. $(1, c, -c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(1,132326,-105) $105 = 3.5.7$ $132326 = 2.109.607$	(257,34,14)	8	[1,2,71,5], [173,4,143,2] [733,4,159,2], [1079,2,127,2] [1639,2,175,2], [1859,8,337,1] [1861,2,195,1], [1867,4,231,1]
(1,5207,-579) $5207 = 41.127$ $579 = 3.193$	(1736,24,72)	4	[2,1,3,24], [569,5,28,2] [806,17,61,1], [931,17,64,1]

Table 6.20: PCM-Rays of: $(-1, c, c)$

The Coeffs. $(-1, c, c)$	Holzer's Range	# of PCM-Rays	All the PCM-Rays
(-1,15,4081) 15 = 3.5 4081 = 7.11.53	(247,63,3)	8	[64,1,1,3], [71,8,1,3] [79,12,1,3], [89,16,1,2] [116,25,1,2], [136,31,1,1] [164,39,1,1], [241,60,1,1]
(-1,15,41701) 15 = 3.5 41701 = 11.17.223	(790,204,3)	8	[206,7,1,3], [226,25,1,3] [254,39,1,3], [271,46,1,2] [394,87,1,2], [431,98,1,1] [529,126,1,1], [719,178,1,1]
(-1,15,54961) 15 = 3.5 54961 = 17.53.61	(907,234,3)	8	[236,7,1,3], [239,12,1,3] [281,40,1,3], [344,65,1,2] [401,84,1,2], [524,121,1,1] [776,191,1,1], [839,208,1,1]
(-1,15,64801) 15 = 3.5 64801 = 11.43.137	(985,254,3)	8	[256,7,1,3], [271,24,1,3] [296,39,1,3], [401,80,1,2] [404,81,1,2], [599,140,1,1] [724,175,1,1], [919,228,1,1]
(-1,15,145189) 15 = 3.5 145189 = 11.67.197	(1475,381,3)	8	[382,7,1,3], [383,10,1,3] [527,94,1,2], [598,119,1,2] [607,122,1,2], [698,151,1,2] [1382,343,1,1], [1423,354,1,1]
(-1,15,263461) 15 = 3.5	(1987,513,3)	8	[514,7,1,3], [586,73,1,3] [614,87,1,2], [719,130,1,2] [926,199,1,2], [1151,266,1,1] [1249,294,1,1], [1951,486,1,1]

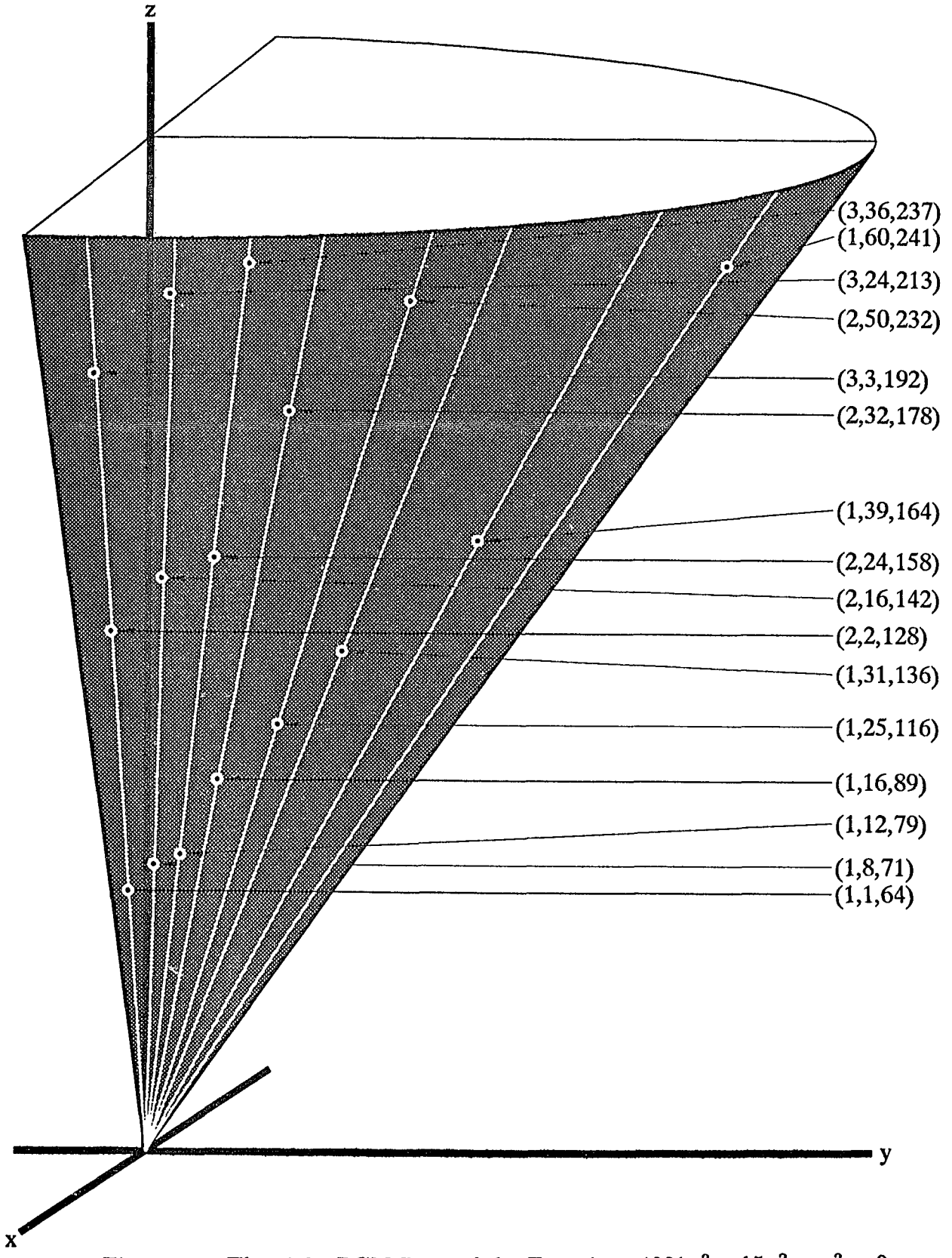

Figure 6.5: The eight PCM-Rays of the Equation: $4081x^2 + 15y^2 - z^2 = 0$

Table 6.21: PCM-Rays of: $(c, c, -c)$

The Coeffs. $(c, c, -c)$	Holz. Range	# of PCM-Rays	All the PCM-Rays
(16241,1517,-12673) 16241 = 109.149 1517 = 37.41 12673 = 19.23.29	(4384, 14346, 4963)	31	[2,37,13,381], [278,773,413,12] [707,188,803,6], [1190,671,1367,3] [250,1493,589,8], [1367,712,1567,3] [1301,1724,1589,3], [245,1804,683,7] [295,2456,913,5], [857,2488,1297,3] [797,2612,1277,3], [1175,2728,1631,3] [2395,2252,2821,1], [2443,1828,2837,1] [2435,2896,2933,1], [329,3056,1121,4] [2995,2932,3539,1], [2065,3968,2711,1] [791,4376,1759,2], [3037,4492,3773,1] [1195,4616,2093,2], [3946,4139,4691,1] [1819,4724,2629,1], [977,4792,1993,2] [3550,5027,4379,1], [2221,5036,3059,1] [3418,6193,4423,1], [1930,7691,3443,1] [119,8804,3049,1], [1706,10391,4081,1] [1834,12991,4951,1].

Chapter 7

FUTURE ANTICIPATIONS

7.1 In This Concluding Chapter

While struggling wth some of the reasonings and then their confirming numerical verifications, or sometimes the vice versa, some general observations and guidelines for future investigations, mathematical or otherwise, have come up on our way. We want to devote this conluding chapter to outline some of these desirable objectives.

7.2 Some Mathematical Problems

Conjecture 1. *If $ax^2 + by^2 = z^2$, with $|a|$ and $|b|$ as primes, has two PCM-rays, then each of them has to be a singleton.*

Conjecture 2. *IF m_2 and m_3 are the numbers of distinct odd prime divisors of a and b respectively with $m_2 \leq m_3$, then the number of PCM-rays for $ax^2 + by^2 = 2z^2$ is less than or equal to 2^{m_3}*

Conjecture 3. *After getting one nontrivial solution X_0 of a Legendre's equation, all of its H-solutions and consequently all of its CM-rays can possibly be detected by means of the solution-generating-formula (5.2.2) alone, by varying $\underline{R}$ over the lattice points on the six HF_i's and the three LHS_i's of the corresponding H-box. (This in fact is a very conservative expectation, which potentially could be much more refinable.)*

SUGGESTION.1: It may be hard, but probably possible to characterize some classes of nonH-solutions, such that from any solution in these classes one can reach a solution within the Holzer's range by a single application of the Mordell's reduction-algorithm of §5.3.

SUGGESTION.2: If we call the CM-rays of equations with only prime coefficients, or with at least one composite coefficient as the primal- and composite- rays respectively, there should be a natural way of linking the primal rays with some corresponding composite rays. This may demand some sort of composition of the

primal rays leading to some composite rays. This in fact could lead to a very new and interesting theory.

SUGGESTION.3: One could possibly try to generalize the idea of CM-rays to homogeneous quadratic equations in more than three variables. Also the idea could be developed in the context of nonhomogeneous equations whose graphs are nothing other than cross-sections of some corresponding generalized cones by planes parallel to the coordinate-planes at integral distances from the origin.

SUGGESTION.4: One could also think of pursuing a somewhat more difficult direction by generalizing this concept of CM-rays to the case of higher-degree equations.

7.3 A Philosophical Comment

In the light of the abundant role of the quadratics or equivalently the cones and the conic sections in both the living and the inanimate universe from the subatomic to the cosmic scale, could one not possibly identify these CM-rays as at least some few concrete phenomena, (however rare they may be), in the unceasing and continuously changing scenes of nature which at least could be in some partial conformity with the Kroneckerian comment about the role of natural numbers in the Creation of God !

Appendix A

AN AUTOBIOGRAPHICAL NOTE: THE GENESIS OF THIS COMPUTATIONAL INVOLVEMENT

Here I want to scrutinize some incidents of my past which led to the present involvement in computational number theory.

The earliest incident that I can recollect which could be pertinent to the growth of my computational interest is my elder brother Sj. Dibakar Mishra's teaching me, during my toddling years, such concepts as $7 - 11 = -4$, and, when one subtracts $7x$ from $5x$ the result is $-2x$, where x could be replaced by any conceivable symbol. Both the concrete and abstract computation was thrilling for him in his high-school algebra at that point of time, (who of course now is a Professor in Physics), and I can imagine why he might have felt overly excited when I, his three-year-old student, could surprise some of his high-school class-mates by giving the correct answer even though the concepts might have been just settling in their mind as some fascinating new things.

One of my brother's class-mates eventually became my first teacher in arithmetic in my 'Shishu Shreni', the year before my first grade. Once he asked essentially the following question:

> *There were five crows on a tree. A hunter shot at them with a gun and two of them died and fell down. How many of them remained on the tree ?*

I was quick to give the answer as zero, telling that the other three would fly away, upon which he came and embraced me with high appreciation. I would say my love for arithmetic was born sometime around that.

Most probably the next arithmetical problem about which I thought with some keen interest that I can recollect now, was asked about a year from then, in my first grade, by my brother Sj. Nishakar Mishra, now a successful engineer in northern India, but then only in his seventh grade. The problem was the following:

There were four poles each having a hole at its base, from and into which mice come out and enter freely. A cat ate some of the mice which came out from the first hole, and some escaped. From the second hole came out twice the number of mice that escaped at the first hole. Again the cat ate some mice and some mice escaped. Three times the number of mice which escaped at the second hole came out from the third hole. Again the cat ate some of those mice. Whatever escaped at the third hole, four times that number came out from the fourth hole. This time the experienced cat finished all of them. If each time the cat ate the same number of mice, what was the number of mice which came out from the first hole, and how many mice the cat was eating each time ?

For some reason, thinking that the question must be with insufficient information, I refused to think about it. I remember my brother, at my submissive challenge, telling me the answer to be 41 and 24. But what amused me about a month later was my finding that the answer was not unique, but any of (82,48), (123,72), or in general $(41m, 24m)$ with m as an arbitrary positive integer, could also constitute a solution. The problem definitely was simple — but at the school when I started asking the same question to some of my competitive class-mates, I had to face some embarrassment when it was passed on to my teacher for whom it was not a very pleasant thing to face. But anyway, the incident increased my confidence.

About two years later I came across a police officer who was very fond of arithmetic and various tricky games with playing cards. I am very sorry to admit that I don't remember his name, but I remember his face very clearly, and more clearly the calf in one of his legs, which, by a bullet during some war, was disfigured into a bundle of rope-like muscles, which his regular uniform, a khaki half-pant could not cover. With due apology, let me call him X.

Mr. X started liking me very much because I could answer most of his tricky arithmetical problems — one among which I remember even till to-day, which actually involves playing-cards. My experience with this tricky game could be described as follows:

The juggler X puts all the thirteen cards of hearts with face down, and asks a naive person Y, just like me at that point, who knows how to count, to think of one of the cards in hearts. Assuming the Ace to be one, and etc., Jack to be eleven, Queen to be 12 and King to be 13, if m is the number of the card Y has thought of, after asking Y to start counting silently in the head from $m+1$ with each tapping over the cards and instructing to indicate by saying 'YES' only when he or she, (i.e., Y), reaches 20, the juggler starts tapping the cards randomly. At that age of around seven, it was very surprising for me to see that whenever I thought of a card, without asking me anything, and only with my counting in the head, each time with my 'YES', the tapping fore-finger of Mr. X stopped over the card I thought of. It seemed as if he was controlling my past thinking !

He offered to tell me the method only after I admit my failure — but somehow by that time I had already grown a certain amount of personal ego — and I persisted in thinking out the mathematical reasoning behind the magic.

About three days later, when Mr. X was playing cards with some of his coleagues, I told him that one does not have to stop at 20 — it could be any number larger than 13, the only restriction being that this final stopping number had to be agreed upon before the tapping starts. In fact I played the role of the juggler, and with his 'YES' at the agreed-upon number, whatever it was, my fore-finger was over the card which he had thought of. — I think by this time I already had grown a fascination for arithmetic.

To speak a little more about the growth of my feeling for mathematics in general, I could say that my vision of mathematics as equivalent to, or even better than any other artistic discipline was enkindled mainly by two teachers of my pre-college years. The first of them was my fifth-grade teacher, Headmaster Bhasker Chandra Raut of the Practicing Upper Primary School at Baripada in India, who, while explaining the arithmetic of trains moving in opposite directions would whistle and walk like a train, or while explaining the problems relating to monkeys climbing slippery poles, or boats sailing along or against the current in a river, would physically demonstrate the problems like an actor on the stage, even though I would think he was well into his fifties at that time. And the second person, who inspired a certain amount of rigour in my mathematical thinking alongwith his imparting an impression in my mind how mathematics could be felt as a very artistic discipline, was my tenth-grade teacher Sj. Madan Mohan Panda, who, among many other things, would demand each mathematics problem to be treated just like an essay — no comma or full-stop should be missed — and no discrete phrases without the proper punctuations should be inserted within the body of a mathematical presentation. I don't know how many mathematical presentations could survive his strict scrutiny. However, even though my conscience acknowledges that it is quite hard a standard to maintain in hundred percent of the cases, while delivering the same preaching to most of my enthusiastic students, I do remember my revered teacher Mr. Panda with heartiest gratitude, and I think that so will he be in my mind for the rest of my life.

There were many encounters of similar nature which gradually built into my faculty: a fascination for computation, which gradually evolved into, may be via the rationals and the reals, to the realms of geometry and the broad discipline of mathematics in general. Here I must digress a little and give one comment about the position of mathematics in the contemporary society I grew in. Unfortunately when I was intellectually growing in India during my high-school years, which in my view is the most pregnant period of a man's life, even though only good students were supposed to do well in mathematics, the profession of a mathematician was not regarded as a very prestigious one. It is a rather complex observation which I should avoid discussing here. — However, with indirect and sometimes direct pressure of the environment, my interests trailed along some zigzag paths.

But finally during my M. Sc. years I met a personality, Dr. Siba Prasad Misra, now at the Institute of Physics at Bhubaneswar in India, (a former Director of

the same Institute), who was then the Head of the Department of Mathematics in Regional Engineering College, my *alma mater*, in the City of Rourkela in India. There, Dr. Misra's influence revived my genuine interest in computations and mathematics in general, and being himself one of the finest gentlemen I have seen in my life, he aroused in my heart the highest reverence for him and thereby also for the Discipline of Mathematics.

Since there have been so many people in my life who have directly or indirectly influenced me in a positive or negative manner to get involved in computations or mathematics in general, if I continue in this style, I am afraid I may elongate this note into a big autobiographical novel. Therefore let me try to conclude soon by coming straight to the right point.

After all the impressions about mathematics I have had through various people or books, I have come to a very personal conclusion that: computations, whenever I have faced them, all along have stood before me as interesting challenges — no matter in what context. I think it is not appropriate to cite here the indivisual computational problems which interested me at various points of my life. However, through my involvements in a large number of discrete mathematical problems, gradually I have come to realize that whenever, either in its developmental stage or in its resolution, a problem gets into an engaging numerical computation, that phase of the problem becomes highly intriguing for me.

While dealing with algebraic topology, starting with the elementary number theoretic argument establishing the five platonic solids as the only possible regular polyhedra, up to again the number theoretic reasoning to substantiate Adam's theorem stating a map α: $S^{2n-1} \longrightarrow S^n$ to be of Hopf-invariant one only when $n = 2, 4,$ or 8, I have found that whenever some tricky computational difficulty arises, something like a genuinely innate instinct simultaneously rises within me, to struggle with that problem with an intrinsic captivating desire.

That is why, when an occasion came up to choose something very distinctly as a primal project of my life, after making a brief review of the status of the computational number theory, I thought of picking up this computational problem of solving the quadratic equations as the central theme. Out of that struggle has come up this thesis: *Rays of Small Integer Solutions of Homogeneous Ternary Quadratic Equations.* And, if anybody is reading this autobiographical note as the first thing from this thesis, after finishing this appendix, he or she could safely continue reading the Introduction in Chapter-1 in order to have a fuller glimpse of the genesis of this work. In that sense, this autobiographical note could be regarded as the genetic introduction to this dissertation.

While concluding, I want to disclose a personal secret. It is regarding some of the names I have used for the rays of solutions we discovered, and also for some of the related concepts we have developed in this work. At certain point after their discovery, I realized that we have something very precious in our hand. I personally wanted to commemorate this collaboration with Professor Harvey Cohn by naming these rays as the *Cohn-Mishra rays*, or the *CM-rays*. It is my very personal and emotional way of expressing the true gratitude to my mentor, Professor Harvey Cohn, who taught

me a very unique method of doing work in computational number theory.

Wishing the Best of Luck to the CM-rays, I conclude this work by quoting a thought which has played a very important role in the development of an attitude in my education almost since the beginning days of my intellectual awakening:

> *I do not know what I may appear to the world, but to myself I seem to have been only like a boy playing on the sea-shore, and diverting myself every now and then finding a smooth pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me.*
>
> — *Sir Isaac Newton* —

Bibliography

[1] Harvey Cohn. *Advanced Number Theory.* Dover Publications Inc., New York. (1980). (First published by John Wiley & Sons. Inc. in 1962 under the title: *A Second Course in Number Theory*).

[2] A. Desboves. *Ref.* [3]. Nouv. Ann. Math., (3),3,(1884), 225-239.

[3] L. E. Dickson. *History of the Theory of Numbers, Vol. 2.* Chelsea Pub. Co., New York. (1952).

[4] Carl Friedrich Gauss. *Disquisitiones Arithmeticæ.*(English Translation by A. A. Clarke,S. J.) Yale University Press, New Haven. (1966).

[5] L. Holzer. *Minimal Solutions of Diophantine Equations.* Can. J. Math., **11** (1950), 238–244.

[6] Adrien-Marie Legendre. *Recherches d' Analyse Indeterminée* in: Histoire de l'Académie Royale des Sciences, Année *M.DCCLXXXV.*

[7] A. Meyer. *His publications around the period 1770-1785*

[8] L. J. Mordell. *The Representation of Numbers by Some Quaternary Quadratic Forms.* Acta Arithmetica,**XII** (1966), 47–54.

[9] L. J. Mordell. *On the Magnitude of the Integer Solutions of the Equation* $ax^2 + by^2 + cz^2 = 0$. J. Number Theory, **I** (1968), 1–3.

[10] L. J. Mordell. *Diophantine Equations.* Vol. 30 in Pure And Applied Mathematics, Academic Press, London and New York. (1969).

[11] J. C. Owings, Jr. *An Elementary Approach to Diophantine Equations of the Second Degree.* Duke Mathematical J., Vol.**37**, (1970), 261–273.

[12] S. Perlis. *Theory of Matrices.* Addison-Wesley Pub. Co.,Reading, Massachusetts. (1952).

[13] I. M. Vinogradov. *Elements of Number Theory.* (English Translation of the Fifth Russian Edition of 1949). Dover Publications, Inc. (1954)

[14] André Weil. *Number Theory.* Birkhäuser, Boston. (1984).

[15] K. S. Williams. *On the Size of a Solution of Legendre's Equation.* Utilitas Mathematica **34** (1988), 65–72.