

University of New Mexico

UNM Digital Repository

Mathematics & Statistics ETDs

Electronic Theses and Dissertations

5-28-1951

The Diophantine Equation

Frederic C. Barnett

Follow this and additional works at: https://digitalrepository.unm.edu/math_etds



Part of the [Mathematics Commons](#)

Recommended Citation

Barnett, Frederic C.. "The Diophantine Equation." (1951). https://digitalrepository.unm.edu/math_etds/83

This Thesis is brought to you for free and open access by the Electronic Theses and Dissertations at UNM Digital Repository. It has been accepted for inclusion in Mathematics & Statistics ETDs by an authorized administrator of UNM Digital Repository. For more information, please contact disc@unm.edu.

378.789

Un 3 Obar

1951

cop. 2

$$u = u_1 + u_2 + u_3$$

$$u = u_1 + u_2 + u_3$$

$$u = u_1 + u_2 + u_3$$

$$u = u_1 + u_2 + u_3$$

THE LIBRARY
UNIVERSITY OF NEW MEXICO



Call No.
378.789
Un30bar
1951
cop.2

Accession
Number
165275

A14400 955389

REC'D UNIV APR 20 '84

DATE DUE

MAR 13 '85

REC'D UNIV APR 15 '85

APR 10 '87

REC'D UNIV APR 10 '87

APR 9 '88

REC'D UNIV MAY -6 '88

DEMCO 38-297

UNIVERSITY OF NEW MEXICO LIBRARY

MANUSCRIPT THESES

Unpublished theses submitted for the Master's and Doctor's degrees and deposited in the University of New Mexico Library are open for inspection, but are to be used only with due regard to the rights of the authors. Bibliographical references may be noted, but passages may be copied only with the permission of the authors, and proper credit must be given in subsequent written or published work. Extensive copying or publication of the thesis in whole or in part requires also the consent of the Dean of the Graduate School of the University of New Mexico.

This thesis by Frederic C. Barnett
has been used by the following persons, whose signatures attest their acceptance of the above restrictions.

A Library which borrows this thesis for use by its patrons is expected to secure the signature of each user.

NAME AND ADDRESS

DATE

MANUSCRIPT NOTES

Unpublished notes submitted to the Master and Doctor are
 given and deposited in the University of New Mexico Library and
 open for inspection, but are to be used only with due regard to the
 rights of the authors. Bibliographical references may be noted and
 passages may be copied only with the permission of the author, and
 proper credit must be given in subsequent written or published
 work. Extensive copying or publication of the notes in whole or in
 part requires also the consent of the Dean of the Graduate School
 of the University of New Mexico.

This thesis by Frederick A. Barnett
 has been read by the following persons, whose signatures attest to the
 acceptance of the above statement.

A Library which borrows this thesis for use by its patrons is
 expected to secure the signature of each user.

NAME AND ADDRESS _____
 DATE _____

THE DIOPHANTINE EQUATION $x^n + y^n = z^n$

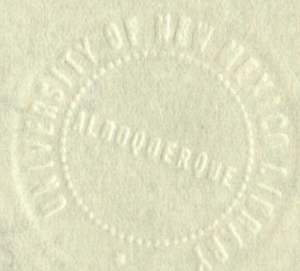
By

Frederic C. Barnett

A Thesis

In partial fulfillment of the
Requirements for the Degree of
Master of Science in Mathematics

The University of New Mexico
1951





Barnett

This thesis, directed and approved by the candidate's committee, has been accepted by the Graduate Committee of the University of New Mexico in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

E. F. Castetter

DEAN

5/28/51

DATE

Thesis committee

Lincoln La Paz

CHAIRMAN

C. E. Buell

Richard C. Hildner

This thesis directed and approved by the candidate's committee has been accepted by the Graduate Committee of the University of New Mexico in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

E. F. Anderson

1937

5/28/37

Date

Thesis Committee

James H. Taylor
W. B. Brown

Robert C. Anderson

378.789
Un30 Lav
1951
Cop.2

TABLE OF CONTENTS

	PAGE
INTRODUCTION	iv
CHAPTER	
I. ALGEBRAIC ATTACKS ON FERMAT'S LAST THEOREM	1
1. Relevant History	1
1.1 The man, Fermat	1
1.2 Definition of Diophantine Problems	1
1.3 Fermat's Statement	2
1.4 Scope of Investigations	3
1.5 Paul Wolfskehl's Prize	4
2. The Direct Attack	5
2.1 Fermat's Method of "infinite descent" . . .	5
2.2 General Solution of $x^2 + y^2 = z^2$	6
2.3 Impossibility of $x^4 + y^4 = z^4$	7
2.4 The Case $(xyz, n) = 1$	10
2.5 Conclusion	12
3. Indirect Algebraic Attacks	13
3.1 Purpose of this Section	13
3.2 Reduction of the Problem	14
3.3 Implications of the Existence of Solutions	14
3.4 Implications if No Solutions Exist	16
3.5 Absence of Indirect Geometric Attacks . . .	17

165275

378.789
 1951
 1951
 1951

TABLE OF CONTENTS

PAGE	
iv	INTRODUCTION
	CHAPTER
1	1. ALGEBRAIC ATTACKS ON FERMAT'S LAST THEOREM
1	1.1 Relevant History
1	1.1.1 The man, Fermat
1	1.2 Definition of Diophantine Problems
1	1.3 Fermat's statement
3	1.4 Scope of investigations
4	1.5 Paul Welfshelm's Prize
5	2. The Direct Attack
5	2.1 Fermat's Method of "infinite descent"
5	2.2 General Solution of $x^2 + y^2 = z^2$
7	2.3 Impossibility of $x^4 + y^4 = z^4$
10	2.4 The Case $(xyz, n) = 1$
13	2.5 Conclusion
13	3. Indirect Algebraic Attacks
13	3.1 Purpose of this Section
14	3.2 Reduction of the Problem
14	3.3 Implications of the Existence of Solutions
18	3.4 Implications if No Solutions Exist
19	3.5 Absence of Indirect Algebraic Attacks

CHAPTER

PAGE

II. GEOMETRIC ATTACK ON FERMAT'S LAST THEOREM	18
1. Analytic Geometry of F_n	18
1.1 F_n a Conical Surface	18
1.2 Contour Lines of F_n	18
1.3 Lemmas from the Theory of Real Variables .	23
1.4 Limiting Fermat Surfaces	24
1.5 Existence of Rational Points on S_E	26
2. Differential Geometry of F_n	30
2.1 Parameterizations of F_n	30
2.1.1 $Y(u, v_1) = uX(v_1)$, v_1 arc length . .	30
2.1.2 $Y(u, v_2) = uX(v_2)$, v_2 not arc length	30
2.1.3 Explicit Expression for X in Parameterization 2.1.1	31
2.1.4 $Y(u, v_3): [\bar{u}, v_3, (\bar{u}^n + v_3^n)^{1/n}]$. . .	33
2.2 The Fundamental Surface Quantities	34
2.2.1 Parameterization 2.1.1	34
2.2.2 Parameterization 2.1.2	34
2.2.3 Parameterization 2.1.3	37
2.3 Implied Differential Geometric Properties of F_n	38
2.3.1 Parameterizations 2.1.1 and 2.1.2 .	38
2.3.2 Parameterization 2.1.3	40
BIBLIOGRAPHY	44

11	11. GEOMETRIC ATTACK ON KEMER'S LAST THEOREM
12	1. Analytic Geometry of F_n
13	1.1 F_n a Conical Surface
14	1.2 Contour Lines of F_n
15	1.3 Lemmas from the Theory of Real Variables
16	1.4 Limiting Point Curves
17	1.5 Existence of Rational Points on F_n
18	2. Differential Geometry of F_n
19	2.1 Parametrizations of F_n
20	2.1.1 $Y(u, v_1) = X(v_1), v_1$ arc length
21	2.1.2 $Y(u, v_2) = X(v_2), v_2$ not arc length
22	2.1.3 Explicit expression for X in
23	2.1.4 $Y(u, v_2) = [X(v_2), (v_2^n + v_2^{n-1})^{1/n}]$
24	2.2 The Fundamental Surface Quantities
25	2.2.1 Parametrization 2.1.1
26	2.2.2 Parametrization 2.1.2
27	2.2.3 Parametrization 2.1.3
28	2.3 Implied Differential Geometric Properties
29	2.3.1 Parametrizations 2.1.1 and 2.1.2
30	2.3.2 Parametrization 2.1.3
31	BIBLIOGRAPHY

LIST OF FIGURES

FIGURE	PAGE
1. Contour Lines of F_n in the Plane $z = 1$: $n = 2m$. . .	21
2. Contour Lines of F_n in the Plane $z = 1$: $n = 2m + 1$. .	22
3. Fermat Surface S_E : $z \geq 0$	27
4. Fermat Surface S_0 : $z \geq 0$	28

FIGURE

1. Contour lines of P_1 in the $x-y$ plane
2. Contour lines of P_2 in the $x-y$ plane
3. Point surface P_1 at $x = 0$
4. Point surface P_2 at $x = 0$

INTRODUCTION

In any list of famous unsolved problems of mathematics, one must surely include Fermat's last theorem. It deserves this acclaim not only for the long list of great mathematicians who have been concerned with its proof over the past three centuries, which is indicative of its charm; but also for the importance of the mathematical developments adduced in the process of its attempted proof, which is indicative of its subtlety. For example, Dickson¹ states that Kummer held "always before himself as goal the complete proof of Fermat's last theorem and the general reciprocity law", and declares that "he would probably have abandoned his theory of ideal numbers, in spite of its success, if he had known another method of proving that theorem and law".

Perhaps the most fascinating aspect of this theorem is the ease with which it can be stated and grasped. It is a familiar fact that there exist triplets of integers such that the squares of two of them add up to the square of the third. It is then simplicity itself to grasp the meaning of the problem to find a triplet of integers such that the sum of the n th powers of two of them is equal to the n th power of the third. Fermat stated definitely that he had

¹L. E. Dickson, Annals of Mathematics, Series 2, 18:161.

INTRODUCTION

In any list of famous unsolved problems of mathematics, one must surely include Fermat's last theorem. It deserves this position not only for the long list of great mathematicians who have been concerned with its proof over the past three centuries, which is indicative of its status; but also for the importance of the mathematical developments advanced in the process of its attempted proof, which is indicative of its subtlety. For example, Dickson¹ states that Kummer held "always before himself as goal the complete proof of Fermat's last theorem and the general reciprocity law", and declares that "he would probably have abandoned his theory of ideal numbers, in spite of its success, if he had known another method of proving that theorem and law".

Perhaps the most fascinating aspect of this theorem is the ease with which it can be stated and grasped. It is a familiar fact that there exist triplets of integers such that the squares of two of them add up to the square of the third. It is then attempted to grasp the meaning of the problem to find a triplet of integers such that the sum of the n th powers of two of them is equal to the n th power of the third. Fermat stated definitely that he had

¹L. E. Dickson, History of Mathematics, Series 2, 1919.

found a "truly wonderful" proof of this proposition, which has become known as "Fermat's Last Theorem". This, then, is the problem with which we are concerned in this paper.

Propositions of such simplicity are often easily discovered by induction, and yet are often of so recondite a character that a satisfactory proof remains hidden for many years. Accordingly, it might be suspected that Fermat had found, but not proved, his last theorem. But as we have shown in the first chapter, Fermat was not only a mathematician of supreme ability in number theory, but was also a mathematician of peerless accuracy - he never claimed to have a proof where later the conclusion reached was shown to be false.

Though Fermat's last theorem has been proved for many particular values of n , the proofs in question have not been generalized to arbitrary n . The next step taken by mathematicians has then been to try to find implications in the field of algebra of the hypothesis that Fermat's relation has solutions. By this means, certain tests have been obtained which for particular values of n provide a ready verification, and others have been obtained that are of theoretical interest only. But it is important to note that even in this direction no published proof has been given of Fermat's "conjecture" for arbitrary n .

found a "truly wonderful" proof of this proposition, which has become known as "Fermat's Last Theorem". This, then, is the problem with which we are concerned in this paper. Propositions of such simplicity are often easily discovered by induction, and yet are often of no real value as a character that a satisfactory proof remains hidden for many years. Accordingly, it might be suspected that Fermat had found, but not proved, his last theorem. But as we have shown in the first chapter, Fermat was not only a mathematician of supreme ability in number theory, but was also a mathematician of vastness of resources - he never failed to have a proof where later the conclusion seemed too obvious to be false.

Though Fermat's last theorem has been proved for many particular values of n , the proofs in question have not been generalized to arbitrary n . The next step taken by mathematicians has then been to try to find indications in the field of algebra of the hypothesis that Fermat's relation has solutions. By this means, certain results have been obtained which for particular values of n provide a ready verification, and others have been obtained that are of theoretical interest only. But it is important to note that even in this direction no published proof has been given of Fermat's "conjecture" for arbitrary n .

The indirect algebraic attack, as we may term the method referred to in the last paragraph, suggested the main problem attacked in this thesis - that of initiating an indirect geometric attack on the last theorem of Fermat. This is accomplished by noting that each triplet of non-zero integers satisfying the Fermat relation, if such triplets exist, is included among the set of all real number triplets which for integral n greater than 2 satisfy the equation $x^n + y^n = z^n$. But the latter equation defines for each value of n a surface F_n which can be investigated in various ways in the attempt to find implications either of the assumption that integral triads are not present or of the assumption that integral triads do occur on the surfaces in question.

In the first part of Chapter II of this thesis a study is made of these surfaces F_n . Such surfaces have many interesting analytical geometric properties, among which is that as n increases without bound through even and odd integral values, respectively, they approach definite limiting surfaces, S_E and S_O .

If a rational point (x, y, z) did exist on F_n , $xyz \neq 0$, $n > 2$, we would have a contradiction of Fermat's last theorem, as is shown in the second chapter. On the other hand, it is shown there that rational points exist, and in fact, form an everywhere dense set on the limiting surfaces.

The indirect algebraic method, as we have seen, is a method referred to in the first chapter, and is the problem attacked in this thesis - that of finding indirect geometrically a line on the line system of three. This is accomplished by noting that each crystal of two zero integers satisfying the Fermat relation, if such triplets exist, is included among the set of all numbers $x^2 + y^2$ which for integer x and y is greater than x^2 . The latter satisfies the equation $x^2 + y^2 = z^2$. The latter equation defines for each value of x a surface F_x which can be investigated in various ways in the attempt to find implications either of the assumption that integer triplets are not present or of the assumption that integer triplets do occur on the surfaces in question.

In the first part of Chapter II of this thesis a study is made of these surfaces F_x . Such surfaces have many interesting analytical geometric properties, among which is that as x increases without bound through even and odd integral values, respectively, they approach definite limiting surfaces, F_{∞} and G_{∞} .

If a rational point (x, y, z) lies on F_x , G_x or H_x , $x > 2$, we would have a contradiction of Fermat's last theorem, as is shown in the second chapter. On the other hand, it is shown that rational points exist, and in fact, form an everywhere dense set on the limiting surfaces.

Yet an attempt to use this fact to demonstrate the existence of rational points of F_n is shown to require a solution of the Fermat relation itself!

In the second part of Chapter II, several differential geometric properties of F_n are adduced, and again, an attack based on certain of these is shown to lead back to the very theorem we seek to prove.

Finally, we obtain three geometrical implications of the assumption that an integral triad exists on F_n suggesting new lines of attack on the theorem of Fermat. These implications must be evaluated as important only in so far as further development in this direction utilizes them in obtaining proofs of Fermat's theorem for particular values of n , or perhaps, if fortune prevails, in obtaining a proof for arbitrary n .

Yet an attempt to use this fact to demonstrate the existence of rational points of F_n is shown to require a solution of the Fermat relation itself.

In the second part of Chapter II, several differential geometric properties of F_n are addressed, and again, an attack based on certain of these is shown to lead back to the very theorem we seek to prove.

Finally, we obtain three geometrical implications of the assumption that an integral exists on F_n , suggesting new lines of attack on the theorem of Fermat. These implications must be evaluated as important only in so far as further development in this direction utilizes them in obtaining proofs of Fermat's theorem for particular values of n , or perhaps, if fortune prevails, in obtaining a proof for arbitrary n .

CHAPTER I

1. RELEVANT HISTORY

1.1 The man, Fermat. Having received a classical education, Pierre de Fermat (1608 - 1665) became at the age of 30 commissioner of requests at Toulouse and five years later, king's councillor in the parliament of Toulouse. It is thus at least unusual that he should have completed works in mathematics that have earned him the highest praise. M. Cantor¹ ranks Fermat and Descartes as the greatest mathematicians of the seventeenth century and implies that Fermat's was the greater fame. He concludes, however, that such considerations "hat für die Gesamtwürdigung beider Geisteshelden keine Bedeutung".

1.2 Definition of Diophantine problems. The Arithmetics of Diophantos (A. D. 250) require the reader to find rational numbers satisfying prescribed conditions. For example, problem 8 of book II requests that a given square number be decomposed into the sum of two square numbers. Thus all problems for which one is required to find rational solutions are called Diophantine problems.

¹M. Cantor, Vorlesungen über Geschichte Der Mathematik, 2:876.

1. GENERAL INTRODUCTION

1.1 The term "number" has received a classical education, having been used (1800 - 1850) to denote the age of 30 commission of reports of numbers and five years later, King's Council in the Parliament of London. It is thus at least unusual that he should have concluded with an enthusiasm that have earned him the highest praise. M. Cantor ranks Fermat and Descartes as the greatest mathematicians of the seventeenth century and implies that Fermat's was the greater taste. He concludes, however, that such considerations "but the the mathematical order of the sciences" is not the determining factor.

1.2 Definition of Number. The Arithmetic of Numbers (A. N. 1800) results in the number to find rational numbers satisfying prescribed conditions. For example, problem 2 of book II requires that a given square number be decomposed into the sum of two square numbers. Thus all problems for which an is required to find rational solutions are called Diophantine problems.

M. Cantor, *Vorlesungen über Zahlentheorie*, Leipzig, 1892.

The particular Diophantine problem alluded to above inspired an attempted generalization by Fermat.

1.3 Fermat's statement. Fermat's copy of Bachet's translation of Diophantos (1621) contains a marginal comment opposite problem 8 of book II: "On the other hand it is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or generally any power except a square into two powers with the same exponent. I have discovered a truly remarkable proof of this, which, however, the margin is not large enough to contain." Since the time of Fermat, mathematicians have been divided on the question of whether he really possessed a proof, since no proof has been found, though the greatest of them have used subtle tools of great power unknown to Fermat, in a futile attempt to find one. On the other hand, Fermat often made such claims, and with this one exception his proofs have since been rediscovered by other investigators. For example, in a letter to the French mathematician Roberval, he states that he had found by use of his favorite method of infinite descent a proof that positive integers can be written as the sum of at most four squares. "I confess openly that in the theory of numbers I have found nothing which I have enjoyed more than the proof of this theorem, and I should be pleased if you would attempt to find it. . . ." Although Euler himself

The particular Diophantine problem alluded to above is treated
in an attempted generalization by Fermat.

1.3 Fermat's statement. Fermat's copy of Bachet's
translation of Diophantus (1621) contains a marginal note
opposite problem 8 of book II: "On the other hand it is im-
possible to separate a cube into two cubes, or a biquadrate
into two biquadrates, or generally any power except a square
into two powers with the same exponent. I have discovered
a truly remarkable proof of this, which, however, the margin
is not large enough to contain." Since the time of Fermat,
mathematicians have been divided on the question of whether
he really possessed a proof, since no proof has been found,
though the greatest of them have used subtle tools of great
power unknown to Fermat, in a futile attempt to find one.
On the other hand, Fermat often made such claims, and with
this one exception his proofs have since been rediscovered
by other investigators. For example, in a letter to the
French mathematician Roberval, he stated that he had found
by use of his favorite method of infinite descent a proof
that positive integers can be written as the sum of at most
four squares. "I confess openly that in the theory of
numbers I have found nothing which I have enjoyed more than
the proof of this theorem, and I would be pleased if you
would attempt to find it." Although Euler himself

attacked this problem for many years, a proof was not found until J. L. Lagrange obtained one in 1770. Similarly, as is stated above, although Fermat was concerned with deep-lying properties of numbers, proofs have been found for each of his theorems but the one considered in this paper.

1.4 Scope of investigations devoted to Fermat's Theorem. Some idea can be obtained of the diversity of the mathematical investigations devoted to Fermat's last theorem from a comment made by Vandiver.² "Efforts on my part to clear up the question have led me into the following topics: Bernoulli numbers and polynomials and generalizations; Euler and Genocchi numbers; Euler and Mirimanoff polynomials; partitions modulo m ; finite fields and rings, including a great many types of congruences; the Dirichlet Zeta function and the related Dedekind function; the Lagrange resolvent and Jacobi ϕ -numbers and various generalizations including generalized Gauss sums; theory of Kummer fields, class numbers, class fields, power characters and laws of reciprocity in the theory of algebraic fields; transformations of Elliptic functions and complex multiplication; Fermat's quotient and other arithmetic quotient forms; congruence

²H. S. Vandiver, American Mathematical Monthly,
53:555-78, 1946
mm

attached this problem for many years, a great deal of work
 until J. A. Lagarias obtained one in 1977. Although
 in stated above, although I have not been able to
 living properties of numbers, which have been known for
 each of his theorems and the one considered in this paper.

1.4 Section of Investigations devoted to

Theorem. Some idea can be obtained of the difficulty of the
 mathematical investigations devoted to this problem from
 from a comment made by Van der Waerden. In "Efforts on the way to
 clear up the question have had me into the following questions:
 Harmonic numbers and polynomials and generalizations;
 Euler and Generalized numbers; Euler and Dirichlet's theorem on
 partitions modulo m ; finite fields and rings; Lagrange's
 great many types of representations; the partitions into squares
 and the related problems; the partitions into squares
 and Jacobsthal's numbers and various generalizations; the
 Generalized Gauss sums; theory of linear forms; class
 numbers, class fields, power characters and law of reciprocity
 precisely in the theory of algebraic fields; representations
 of elliptic functions and complex multiplication; formal
 quotient and other arithmetic questions; congruences

theories as applied to power series; abstract algebra including, particularly, group theory and semi-groups; and many types of Diophantine equations aside from the Fermat relation itself."

1.5 Paul Wolfskehl's prize. Adding not an iota to the mathematical interest of Fermat's Theorem, but a great deal to public curiosity concerning it has been the prize of 100,000 marks offered by the German mathematician Paul Wolfskehl for a proof of it, or for a complete determination of the values of n for which it is true, in case it is not universally true. The conditions were first outlined in the Jahresbericht der Deutschen Mathematiker-Vereinigung, June 1908, p. 111. Some of these are³ that "no manuscripts will be considered, but only printed articles or monographs. These articles or monographs must have appeared in regular periodicals or they must have been for sale in the open market. The prize will not be awarded for articles or monographs which have been before the public less than two years: the latest date for awarding the prize being September 13, 2007."

³G. A. Miller, Historical Introduction to Mathematical Literature, p. 156.

theories as applied to some social sciences; including, particularly, group theory and social psychology; and many types of theoretical relations which have been developed in the field of social psychology itself."

1.6 Final Selection of Papers. Nothing has as yet to the mathematical interest of the author, but a great deal of public interest concerning it has been the prize of 100,000 marks offered by the German Mathematical Society for a proof of it, or for a complete determination of the values of n for which it is true, in case it is not universally true. The conditions were first outlined in the Jahresbericht der Deutschen Mathematiker-Vereinigung, June 1908, p. 111. Some of these are "no manuscript will be considered, but only printed articles or monographs. These articles or monographs must have appeared in regular periodicals or they must have been for sale in the open market. The prize will not be awarded for articles or monographs which have been before the public less than two years: the latest date for awarding the prize being September 15, 1909."

Dr. A. Miller, Historical Information in Mathematics
Lecture 2. 1909.

2. THE DIRECT ATTACK

2.1 Fermat's method of "infinite descent". To students of beginning algebra is presented the method of proof by induction which is used to establish the truth of an infinite sequence of propositions, $P_1, P_2, \dots, P_n, \dots$. This method is based on an assumption that if for every positive integer k , P_k implies P_{k+1} , and P_1 is known to be true, then all of the propositions P_k , $k = 1, 2, 3, \dots$ are true. The closely analogous principle of infinite descent may be phrased as follows: if the assumption that a problem can be solved in positive integers (proposition P_{a_k}) can be shown to imply there is a solution to that problem in smaller positive integers (proposition $P_{a_{k+1}}$, $a_{k+1} < a_k$), then an infinity of propositions P_{a_k} are true, each successive proposition referring to smaller positive integers than does its predecessor. But in this case a contradiction is obtained which denies the truth of P_{a_k} for any set of integers; for although the set of positive integers is not bounded above, it is certainly bounded below. Just as the difficulty in any proof by induction usually lies in the proof that P_k implies P_{k+1} , so the difficulty in the infinite descent proof lies in the demonstration that P_{a_k} implies $P_{a_{k+1}}$. We may conjecture that Fermat was actually able to show this for the general Fermat

Theorem. After obtaining the general solution of $x^2 + y^2 = z^2$ in positive integers we shall indicate how he actually did carry through such a demonstration for the equation $x^4 - y^4 = z^2$, and how this result immediately implies the impossibility of $x^4 + y^4 = z^4$.⁴

2.2 General solution of $x^2 + y^2 = z^2$. The following chain of reasoning⁵ gives us the general solution of $x^2 + y^2 = z^2$ in positive integers. We first observe that $(x,y) = (x,z) = (y,z)$, and that this implies that all solutions can be expressed as multiples of the solutions of the primitive equation $x^2 + y^2 = z^2$, where $(x,y) = 1$. Accordingly, we assume that $(x,y) = 1$, from which it follows that z is odd. (For, if z were even, both of x and y would have to be odd. But if they were both odd, z^2 would be divisible by 2 but not by 4, which is impossible.) Thus, in the primitive equation, one of x and y is odd, the other even. Since x and y enter symmetrically, there is no loss in generality in taking x even. We may now state and prove: "The necessary and sufficient condition that

⁴Fermat's copy of Bachet, Diophantos, problem 26, book VI.

⁵Edmund Landau, Vorlesungen über Zahlentheorie, 3:204-5.

Theorem. After obtaining the general solution of the equation $x^2 + y^2 = z^2$ in positive integers, we can actually add every other such solution to the equation $x^2 - y^2 = z^2$, and the resulting solutions implies the impossibility of $x^2 + y^2 = z^2$.

2.2 General solution of $x^2 + y^2 = z^2$.
 chain of reasoning gives us the general solution of $x^2 + y^2 = z^2$ in positive integers. Let (x, y, z) be a solution of $x^2 + y^2 = z^2$ in positive integers, and let (x', y', z') be another solution. Then the solutions can be expressed as $x = kx'$, $y = ky'$, $z = kz'$ of the primitive solution $x'^2 + y'^2 = z'^2$. Accordingly, we assume that $(x, y, z) = (x', y', z')$. It follows that z is odd. If z were even, x and y would have to be odd, and z would be divisible by 2 but not by 4, which is impossible. Thus, in the primitive solution, one of x and y is even, the other even. Since x and y are either both even or both odd in general, in taking x even, y odd, we can prove: The necessary and sufficient condition for

$x^2 + y^2 = z^2$, $(x, y) = 1$, $x \equiv 0 \pmod{2}$ is that $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$, where u and v have relatively prime integral values such that $u > v > 0$ and $u + v \not\equiv 0 \pmod{2}$."

For, from $(y, z) = 1$, $\frac{z+y}{2} + \frac{z-y}{2} = z$, and

$\frac{z+y}{2} - \frac{z-y}{2} = y$, it is clear that $\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$.

Since $z > y$, it follows from $(\frac{1}{2}x)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2}$

that: $\frac{z+y}{2} = u^2$, $u > 0$, $\frac{z-y}{2} = v^2$, $v > 0$, where u and v

are integers such that $u > v$, $(u, v) = 1$ and

$(u + v)^2 \equiv u^2 + v^2 \not\equiv 0 \pmod{2}$, so that $u + v \not\equiv 0 \pmod{2}$.

Furthermore, $(\frac{1}{2}x)^2 = (uv)^2$ implies that $x = 2uv$.

Conversely, given $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$, where u and v are integers such that $u > v > 0$, $(u, v) = 1$, $(u + v) \not\equiv 0 \pmod{2}$, we have $x^2 + y^2 = (2uv)^2 + (u^2 - v^2)^2 = z^2$, where $xyz \neq 0$, $x \equiv 0 \pmod{2}$, $(x, y) = 1$, and x, y, z are all integers.

2.3 Impossibility of $x^4 + y^4 = z^4$. We are now prepared to follow an argument by infinite descent proving that both $x^4 - y^4 = z^2$ and $x^4 + y^4 = z^4$ are impossible in positive integers. To this end we define a primitive right triangle to be one whose sides have relatively prime integral lengths, and prove that the area of a primitive right triangle is never a square.

$x^2 + y^2 = z^2$, $(x, y) = 1$, $x \equiv 0 \pmod{2}$, is that $x = 2uv$,
 $y = u^2 - v^2$, $z = u^2 + v^2$, where u and v have relatively
 prime integral values such that $u > v > 0$ and

$$u + v \not\equiv 0 \pmod{2}.$$

For, from $(x, z) = 1$, $\frac{x+z}{2} + \frac{x-z}{2} = z$, and

$$\frac{x+z}{2} - \frac{x-z}{2} = y, \text{ it is clear that } \left(\frac{x+z}{2}, \frac{x-z}{2}\right) = 1.$$

Since $z > y$, it follows from $(\frac{x+z}{2}, \frac{x-z}{2}) = 1$ that

$$\frac{x+z}{2} = u^2, \frac{x-z}{2} = v^2, \text{ where } u \text{ and } v$$

are integers such that $u > v$, $(u, v) = 1$ and

$$(u+v)^2 \equiv u^2 + v^2 \not\equiv 0 \pmod{2}, \text{ so that } u + v \not\equiv 0 \pmod{2}.$$

Furthermore, $(\frac{x+z}{2})^2 = (u^2)^2 = u^4$, implies that $x = 2uv$.

Conversely, given $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$,

where u and v are integers such that $u > v > 0$, $(u, v) = 1$,

$$(u+v)^2 \not\equiv 0 \pmod{2}, \text{ we have } x^2 + y^2 = (2uv)^2 + (u^2 - v^2)^2 = z^2,$$

where $xyz \neq 0$, $x \equiv 0 \pmod{2}$, $(x, y) = 1$, and x, y, z are all

integers.

2.3 Impossibility of $x^4 + y^4 = z^4$ We are now

prepared to follow an argument by infinite descent proving

that both $x^4 - y^4 = z^4$ and $x^4 + y^4 = z^4$ are impossible in

positive integers. To this end we define a primitive right-

triangle to be one whose sides have relatively prime inte-

geral lengths, and prove that the area of a primitive right

triangle is never a square.

Since Pythagoras' Theorem assures us that the sides of a right triangle have the relation $x^2 + y^2 = z^2$, and in a primitive right triangle $(x,y) = 1$, the foregoing theorem gives us its area as $uv(u+v)(u-v)$, which is to be a perfect square. If the factors of this expression for the area were relatively prime, we would know thereby each of them to be a square. But they are relatively prime, the only pair for which this is not obvious being $u+v$, $u-v$. These are relatively prime, for any common factor would divide their sum and difference, $2u$ and $2v$. By the foregoing theorem u and v are relatively prime, and since $u+v$ and $u-v$ are odd, 2 could not be a common factor. Thus, $u = a^2$, $v = b^2$, $u-v = c^2$, $u+v = d^2$, where a, b, c, d are relatively prime in pairs.

By algebra,

$$(2.3.1) \quad 2a^2 = c^2 + d^2 \quad \text{and}$$

$$(2.3.2) \quad 2b^2 = (d+c)(d-c)$$

Since one of u and v is even and the other odd, a and b must have the same property. For the same reason c and d are both odd, so that both $d+c$ and $d-c$ are even.

Hence, from (2.3.2), b is even. Let $b = 2b_1$ and therefore

$$(2.3.3) \quad 2b_1^2 = \frac{d-c}{2} \cdot \frac{d+c}{2}, \quad \text{where} \quad \left(\frac{d-c}{2}, \frac{d+c}{2} \right) = 1,$$

Since Pythagoras' theorem assumes no limit the sides of a right triangle have the relation $x^2 + y^2 = z^2$, and in a primitive right triangle $(x, y) = 1$, the foregoing theorem gives us the area as $xy/2 + y/2(n - v)$, which is to be a perfect square. If the factors of this expression for the area were relatively prime, we would know thereby each of them to be a square. But they are relatively prime, the only pair for which this is not obvious being $n + v, n - v$. These are relatively prime, for any common factor would divide their sum and difference, $2n$ and $2v$. By the foregoing theorem n and v are relatively prime, and since $n + v$ and $n - v$ are odd, 2 could not be a common factor. Thus, $n = a^2, v = b^2, n - v = c^2, n + v = d^2$, where a, b, c, d are relatively prime in pairs.

By algebra,

$$(2.2.1) \quad 2a^2 = c^2 + d^2 \quad \text{and}$$

$$(2.2.2) \quad 2b^2 = (d + a)(d - a)$$

Since one of n and v is even and the other odd, a and b must have the same parity. For the same reason c and d are both odd, so that both $d + a$ and $d - a$ are even. Hence, from (2.2.2), b is even. Let $b = 2b_1$ and therefore

$$(2.2.3) \quad 2b_1^2 = \frac{d-a}{2} \cdot \frac{d+a}{2}, \quad \text{where} \quad \left(\frac{d-a}{2}, \frac{d+a}{2} \right) = 1.$$

their sum and difference being relatively prime. From (2.3.3) one of $\frac{d-c}{2}$, $\frac{d+c}{2}$ is even. Suppose in particular that $\frac{d-c}{2} = 2k^2$, $\frac{d+c}{2} = j^2$. This implies that $b_1^2 = k^2 j^2$. If on the other hand $\frac{d+c}{2}$ is even, say $\frac{d+c}{2} = 2k^2$, and $\frac{d-c}{2} = j^2$, we still have $b_1^2 = k^2 j^2$. Thus, from (2.3.1)

$$(2.3.4) \quad a^2 = (j^2)^2 + (2k^2)^2$$

We have so far proved that the assumption that there exists a primitive right triangle with area $uv(u^2 - v^2) > \frac{V}{4}$ implies the existence of another with area $b_1^2 = \frac{V}{4}$. This solution in turn assures us of another yet smaller, etc. So that we have proved there is an infinity of primitive right triangles with areas perfect squares, each less than that of the preceding. But this is impossible, and we know thereby that no primitive right triangle has an area equal to a perfect square.

We can conclude from this almost immediately that there exist no integers p, q, r , with $pqr \neq 0$ such that $p^4 - q^4 = r^2$. For, this equation implies that $(p^4 - q^4)p^2q^2 = r^2p^2q^2$, where $(2p^2q^2)^2 + (p^4 - q^4)^2 = (p^4 + q^4)^2$: that is, that a primitive right triangle does

their own and differences between them.

(2.3.3) one of $\frac{1}{2} - \epsilon$, $\frac{1}{2} + \epsilon$ and $\frac{1}{2}$.

particular that $\frac{1}{2} - \epsilon = \frac{1}{2} - \frac{1}{2} = 0$, $\frac{1}{2} + \epsilon = \frac{1}{2} + \frac{1}{2} = 1$.

that $\frac{1}{2} - \epsilon = \frac{1}{2}$. It is the same as $\frac{1}{2}$.

say $\frac{1}{2} - \epsilon = \frac{1}{2}$, and $\frac{1}{2} + \epsilon = \frac{1}{2}$.

Thus, from (2.3.1)

$$(2.3.4) \quad a^2 = (1^2)^2 + (0^2)^2$$

we have as far as the first two terms are concerned

there exists a primitive right triangle

$$uv(u^2 - v^2) > \frac{1}{2} \text{ (Lambert's and Legendre's theorem)}$$

and $\frac{1}{2} - \epsilon = \frac{1}{2}$. This relation is satisfied by

another yet smaller, and so on, to infinity.

is an infinity of primitive right triangles

periodic squares, each less than the last.

But this is impossible, and we have

primitive right triangles are an infinity of

squares.

It can conclude from this that

there exist no isosceles right triangles

$$p^2 - q^2 = r^2, \text{ for this is impossible}$$

$$(p^2 - q^2)p^2 = r^2p^2, \text{ where } (p^2 - q^2) = 1$$

$$(p^2 + q^2)^2 = r^2, \text{ where } (p^2 + q^2) = r$$

exist whose area is a square. Since no true proposition can imply a false one, we have proved that $p^4 - q^4 = r^2$ is impossible with p, q, r integers such that $pqr \neq 0$.

Finally, there exists no integers x, y, z with $xyz \neq 0$ such that $x^4 + y^4 = z^4$, for this is an obvious special case of the preceding result that none exist such that $p^4 - q^4 = r^2$, where $p = z$, $q = x$ and $r = y^2$.

2.4 The case $(xyz, n) = 1$. Restricting the integers that enter into the Fermat equation so that $(xyz, n) = 1$, we are able to obtain⁶ a particularly elegant proof that $x^n + y^n + z^n = 0$ is impossible⁷ for $n = 3$ and $n = 5$.

Let,

$$L = x + y + z$$

$$S_1 = x^1 + y^1 + z^1 .$$

Then, identically,

$$\begin{aligned} L^3 - S_3 &= 3(x+y)(y+z)(z+x) \\ (2.4.1) \quad L^5 - S_5 &= 5(x+y)(y+z)(z+x) \frac{L^2 + x^2 + y^2 + z^2}{2} \end{aligned}$$

⁶P. Bachman, Niedere Zahlentheorie, 2:461-63.

⁷Section 3.2 shows how $x^n + y^n = z^n$ may be reduced to $x^n + y^n + z^n = 0$.

exists whose area is a square. Since no true composition can imply a false one, we have proved that $x^4 - y^4 = z^2$ is impossible with x, y, z integers such that $xyz \neq 0$. Finally, there exists no integers x, y, z with $xyz \neq 0$ such that $x^4 + y^4 = z^4$, for this is an obvious special case of the preceding result that none exist such that $p^4 - q^4 = r^2$, where $p = x$, $q = y$ and $r = z$.

2.4 The case $(xyz, n) = 1$. Restricting the integers

that enter into the Fermat equation so that $(xyz, n) = 1$, we are able to obtain a particularly elegant proof that $x^n + y^n + z^n = 0$ is impossible for $n = 3$ and $n = 4$.

Let

$$I = x + y + z$$

$$S_1 = x^2 + y^2 + z^2$$

Then, identically,

$$I^3 - 3S_1 = 3(x + y)(y + z)(z + x)$$

(2.4.1)

$$I^5 - 5S_1I = 5(x + y)(y + z)(z + x) \frac{I^3 + x^3 + y^3 + z^3}{3}$$

² P. Bachman, Elementary Number Theory, 2:461-62.

³ Section 2.2 shows how $x^n + y^n = z^n$ may be reduced to $x^n + y^n + z^n = 0$.

Fermat's well-known "little theorem" implies that

$$S_p \equiv x + y + z \pmod{p}$$

for every prime p . Therefore, if x, y, z are solutions of (3.2.1),

$$x + y + z \equiv 0 \pmod{p}.$$

In particular, if

$$x^3 + y^3 + z^3 = 0$$

$$x^5 + y^5 + z^5 = 0$$

then,

$$x + y + z \equiv 0 \pmod{3}$$

$$x + y + z \equiv 0 \pmod{5}$$

and relations (2.4.1) yield

$$(2.4.2) \quad 3(x + y)(y + z)(z + x) \equiv 0 \pmod{3^3}$$

$$5(x + y)(y + z)(z + x) \cdot \frac{L^2 + x^2 + y^2 + z^2}{2} \equiv 0 \pmod{5^5}.$$

From the first of congruences (2.4.2) it follows that at least one of the factors $(x + y)$, $(y + z)$, $(z + x)$ is divisible by 3, and therefore, from $x + y + z \equiv 0 \pmod{3}$, that one of the numbers x, y, z is divisible by 3.

Forman's well-known "little theorem" implies that

$$a^p \equiv a + v + x \pmod{p}$$

for every prime p . Therefore, if x, y, z are solutions of (2.4.1),

$$x + y + z \equiv 0 \pmod{p}.$$

In particular, if

$$x^2 + y^2 + z^2 \equiv 0$$

$$x^2 + y^2 + z^2 \equiv 0$$

then,

$$x + y + z \equiv 0 \pmod{3}$$

$$x + y + z \equiv 0 \pmod{3}$$

and relations (2.4.1) yield

$$3(x + y)(y + z)(z + x) \equiv 0 \pmod{27}$$

(2.4.2)

$$3(x + y)(y + z)(z + x) \cdot \frac{x^2 + y^2 + z^2}{2} \equiv 0 \pmod{27}$$

From the first of congruences (2.4.2) it follows that

at least one of the factors $(x + y)(y + z)(z + x)$ is

divisible by 3, and therefore, from $x + y + z \equiv 0 \pmod{3}$,

that one of the numbers x, y, z is divisible by 3.

From the second congruence we infer either the divisibility of one of the three factors $(x + y)$, $(y + z)$, $(z + x)$, or of the expression $L^2 + x^2 + y^2 + z^2$, by 5.

As before, we infer that if one of the factors $(x + y)$, $(y + z)$, $(z + x)$ is divisible by 5, so is one of the numbers x, y, z , which is a contradiction of $(xyz, p) = 1$. If on the other hand it is $L^2 + x^2 + y^2 + z^2$ that is divisible by 5, then

$$x^2 + y^2 + z^2 \equiv 0 \pmod{5},$$

for $L \equiv 0 \pmod{5}$. But this too is impossible unless one of x, y, z is divisible by 5.⁸ Bachman concludes, however, that other methods must be developed to handle $x^n + y^n + z^n = 0$ for larger values of p .

2.5 Conclusion. Existing elementary direct proofs become more difficult with increasing prime n . Already with $n = 3$, Uspensky⁹ requires thirteen pages of preparatory development and four¹⁰ more of specific treatment to obtain such a proof. More discouraging, these ponderous proofs do

⁸ If no one of x, y, z is divisible by 5, then x, y, z are congruent to ± 1 or $\pm 2 \pmod{5}$ in some order; whence, $x^2 + y^2 + z^2 \equiv (\pm 1) + (\pm 1) + (\pm 1) \not\equiv 0 \pmod{5}$.

⁹ J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, p. 484.

¹⁰ Ibid., pp. 408-11.

From the second congruence we infer either the
 divisibility of one of the three factors $(x+y), (y+z),$
 $(z+x)$, or of the expression $x^2 + y^2 + z^2 + x^2 + y^2 + z^2$, by 3.
 As before, we infer that if one of the factors
 $(x+y), (y+z), (z+x)$ is divisible by 3, so is one of
 the numbers x, y, z , which is a contradiction of $(x, y, z) = 1$.
 If on the other hand it is $x^2 + y^2 + z^2 + x^2 + y^2 + z^2$ that is
 divisible by 3, then

$$x^2 + y^2 + z^2 \equiv 0 \pmod{3},$$

for $1 \equiv 0 \pmod{3}$. But this too is impossible unless one
 of x, y, z is divisible by 3. Another conclusion, however,
 that other methods must be developed to handle
 $x^2 + y^2 + z^2 \equiv 0$ for larger values of n .

2.5 Conclusion. Finding elementary divisors

become more difficult with increasing prime n . Already
 with $n = 5$, however, ⁹ tedious algebraic pages of preliminary
 development and four ¹⁰ more of equally tedious treatment to obtain
 such a proof. More interesting, these monstrous proofs are

⁹ If no one of x, y, z is divisible by 3, then x, y, z
 are congruent to ± 1 or $\pm 2 \pmod{3}$ in some order; whence
 $x^2 + y^2 + z^2 \equiv (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 \equiv 0 \pmod{3}$.

¹⁰ V. Uspensky and M. A. Heuley, Number Theory,
 Chapter IV, p. 184.

not seem to suggest a method which can be generalized to all values of n . In fact, as we shall discover in the next section, the indirect attack seems to be more productive of important results.

3. INDIRECT ALGEBRAIC ATTACKS

3.1 Purpose of this section. As a preface to the second and geometrical portion of this thesis we shall set forth in this section certain known implications of one or the other of the alternative assumptions,

- (a) that solutions do exist for the Fermat problem,
- (b) that such solutions do not exist.

Such implications are many and varied, and it is clearly impossible in the present brief review either to deal comprehensively with them or to go into complete detail in connection with the relatively few which we choose to present as examples. Our real purpose is to make clear that when the direct attack on the Fermat problem seemed unproductive, a variety of indirect algebraic attacks were discovered. This procedure motivated the present thesis which in the second chapter seeks to discover certain geometrical implications of the basic assumptions (a) and (b) to which we have alluded above.

not seen to suggest a method which can be generalized to all values of n . In fact, we shall discover in the next section, the indirect attack seems to be more productive of important results.

2. INDIRECT ATTACKS

2.1. FACTORS OF THIS SECTION. As a contrast to the second and geometrical content of this thesis we shall set forth in this section certain known implications of one or the other of the alternative assumptions.

(a) that solutions do exist for the Fermat problem.

(b) that such solutions do not exist.

Such implications are many and varied, and it is clearly impossible in the present brief review either to deal comprehensively with them or to go into complete detail in connection with the relatively few which we choose to present as examples. Our main purpose is to make clear that when the direct attack on the Fermat problem seemed unproductive, a variety of indirect algebraic attacks were discovered. This procedure motivated the present thesis which in the second chapter seeks to discover certain geometrical implications of the basic assumptions (a) and (b) to which we have alluded above.

3.2 Reduction of the problem. In discussing Fermat's equation $x^n + y^n = z^n$ it is sufficient to consider a solution in which $(x,y) = 1$. For if there exists a solution in integers (x,y,z) where $(x,y) = k > 1$, then $z = kZ$ and we may set $x = kX$, $y = kY$. On cancelling k^n we have the Fermat equation $X^n + Y^n = Z^n$ in which $(X,Y) = 1$. Furthermore, if Fermat's theorem is true for some n , it is true for any multiple m of n , for if $(x^m)^n + (y^m)^n = (z^m)^n$ were possible, so would be $x^n + y^n = z^n$. Thus, since every integer greater than 2 is divisible by 4 or by an odd prime, it suffices to prove the Fermat conjecture for $n = 4$ and for $n = p$, p being an odd prime. Having already proved it for $n = 4$, the only exponents for which we must prove it are odd primes. Since in the algebraic treatment negative integers are admissible values of (x,y,z) , we may clearly write the Fermat equation in the form:

$$(3.2.1) \quad x^p + y^p + z^p = 0, \quad p \text{ an odd prime.}$$

3.3 Implications of the existence of solutions.

In 1850, E. E. Kummer¹¹ proved that if (3.2.1) holds, then n divides at least one of the numerators of the Bernoulli numbers $B_1, B_2, \dots, B_{\frac{p-3}{2}}$.

¹¹L. E. Dickson, History of the Theory of Numbers, 2:742. For the definition of B_1 , see Niels Nielsen, Traite Elementaire Des Nombres De Bernoulli, p. 14.

3.2. Proof of the Theorem. In classical Fermat's equation $x^n + y^n = z^n$ it is sufficient to consider a solution in which $(x, y) = 1$. For if there exists a solution in integers (x, y, z) where $(x, y) = d > 1$, then $x = dx_1$ and $y = dy_1$ where $(x_1, y_1) = 1$. For simplicity we have the Fermat equation $x^n + y^n = z^n$ and write $(x, y) = 1$. Furthermore, if Fermat's Theorem is true for some n , it is true for any multiple m of n . For if $(x, y, z) = (x_1, y_1, z_1)$ is a solution, so could be $x_1^m + y_1^m = z_1^m$. Thus, since every integer greater than 2 is divisible by 2 and by an odd prime, it suffices to prove the Fermat conjecture for $n = 4$ and for $n = p$, p being an odd prime. Having already proved it for $n = 4$, we only have to prove it for odd primes p . In the algebraic treatment negative integers are inadmissible in the algebraic treatment. We may restrict the Fermat equation to the form

$$(3.2.1) \quad x^p + y^p = z^p, \quad p \text{ an odd prime.}$$

3.3. Factorization of the expression of solutions. In 1850, K. F. Gauss proved that if (3.2.1) holds, then z divides at least one of the numerators of the fractions

$$x_1^p, x_2^p, \dots, x_{p-1}^p, y_1^p, y_2^p, \dots, y_{p-1}^p, z^p.$$

11. K. F. Gauss, History of the Theory of Numbers, 2:740. For the details of the proof see Gauss, Disquisitiones Arithmeticae, p. 10.

A. Wieferich¹² proved that if equation (3.2.1) is possible in integers prime to p , where p is an odd prime, then $2^{p-1} - 1$ is divisible by p^2 . This criterion is satisfied only for $p = 1093$ and $p = 3511$ for $p < 16000$.

Under the same conditions, D. Mirimanoff¹³ showed that $3^{p-1} \equiv 1 \pmod{p^2}$. By combining criteria of this nature, the Lehmers¹⁴ established the case $(xyz, p) = 1$ of Fermat's Theorem for all p less than 253,747,889.

Let $L = x + y + z$, $M = xy + yz + zx$, $N = xyz$. Then (3.2.1) can be written in the form:

$$(3.3.1) \quad G_p(L, M, N) = 0^{15}$$

where x, y, z are roots of

$$(3.3.2) \quad t^3 - Lt^2 + Mt - N = 0.$$

(3.2.1) can have a rational solution only when all roots of (3.3.2) are rational, its coefficients being subject to criterion (3.3.1). This result is due to Mirimanoff¹⁶.

¹²Dickson, op. cit., p. 764.

¹³Ibid., p. 768.

¹⁴D. H. & Emma Lehmer, "On the First Case of Fermat's Last Theorem", Bulletin American Mathematical Society, 47:139-42.

¹⁵ $G_p(L, M, N)$ is the expression obtained on substituting the solution for x, y, z in terms of L, M, N into (3.2.1).

¹⁶Dickson, op. cit., p. 766.

A. Waterhouse¹² proved that if equation (3.2.1) is possible in integers prime to p , where p is an odd prime, then $2p-1$ is divisible by p . This assertion is satisfied only for $p = 1093$ and $p = 3511$ for $p < 10000$. Under the same conditions, D. Mirmanoff¹³ proved that $2p-1 \equiv 1 \pmod{p^2}$. By combining assertions of this nature, the authors¹⁴ established the case $(x, y, z) = 1$ of Fermat's Theorem for all p less than 223,747,283. Let $L = x + y + z$, $M = xy + yz + xz$, $N = xyz$. Then (3.2.1) can be written in the form:

$$(3.2.1) \quad G_p(L, M, N) = 0$$

where x, y, z are roots of

$$(3.2.2) \quad t^3 - Lt^2 + Mt - N = 0.$$

(3.2.1) can have a rational solution only when all roots of (3.2.2) are rational, its coefficients being subject to restriction (3.2.1). This result is due to Mirmanoff.¹⁵

¹² Jackson, op. cit., p. 784.

¹³ Ibid., p. 785.

¹⁴ D. H. & Emma Lehmer, "On the First Case of Fermat's Last Theorem", Bulletin American Mathematical Society, 47:132-40.

¹⁵ G. (L, M, N) is the expression obtained on substituting the solution for x, y, z in terms of L, M, N into (3.2.1).

¹⁶ Jackson, op. cit., p. 785.

3.4 Implications if no solutions exist. We now attempt to find solvable Diophantine implications of (3.2.1) with the hope of finding a contradiction to the conjecture that (3.2.1) is impossible.

V. A. Lebesgue¹⁷ stated in 1840, that if $x^n + y^n = z^n$ is impossible in integers, so is $x^{2n} + y^{2n} = z^2$. This result follows readily from the general solution of $x^2 + y^2 = z^2$. For if $(x^n)^2 + (y^n)^2 = z^2$ has solutions they are given by $x^n = u^2 - v^2$, $y^n = 2uv$ where $(u, v) = 1$. Thus,

$$\begin{aligned} u - v &= a^n \\ u + v &= b^n \\ u &= 2^{n-1} c^n \\ v &= d^n \end{aligned}$$

in some order. Hence,

$$a^n \pm b^n = (2c)^n ;$$

i.e., $x^n + y^n = z^n$ is possible.

J. Liouville¹⁸ noted a similar result in the same year. If $x^n + y^n = z^n$ is impossible in integers not zero, then so is $x^{2n} - y^{2n} = 2z^n$.

¹⁷Dickson, op. cit., p. 737.

¹⁸Ibid., p. 738.

3.4. Indistinguishability of no solution exists

attempt to find a suitable Diophantine implication of (3.2.1) with the hope of finding a contradiction to the conjecture that (3.2.1) is impossible.

V. A. Lebesgue¹⁷ stated in 1840, that if

$$x^n + y^n = z^n \text{ is impossible in integers, so is } x^{2n} + y^{2n} = z^{2n}.$$

This result follows readily from the general solution of

$$x^2 + y^2 = z^2. \text{ For if } (x^n)^2 + (y^n)^2 = z^{2n} \text{ has solutions}$$

they are given by $x^n = u^2 - v^2$, $y^n = 2uv$ where $(u, v) = 1$.

Thus,

$$u - v = x^n$$

$$u + v = y^n$$

$$u = \frac{y^n + x^n}{2}$$

$$v = \frac{y^n - x^n}{2}$$

in some order. Hence,

$$x^n \pm y^n = (2u)^n$$

i.e., $x^n + y^n = z^n$ is possible.

A. Lioville¹⁸ noted a similar result in the same

year. If $x^n + y^n = z^n$ is impossible in integers not

zero, then so is $x^{2n} + y^{2n} = z^{2n}$.

¹⁷ V. A. Lebesgue, *Ann. Chem. Phys.*, 3, 1840.

¹⁸ A. Lioville, *Bull. Soc. Math.*, 1840.

Finally, A. Hurwitz¹⁹ proved that if $x^k + y^k = z^k$ is impossible for every integer K , $K > 2$, then

$$u^m v^n + v^m w^n + w^m u^n = 0$$

is impossible for every pair of integral m and n except where $(u, v, w) = (1, 0, 0)$, $(0, 1, 0)$, or $(0, 0, 1)$.

3.5 Absence of indirect geometric attacks.

Although indirect algebraic attacks abound in the literature, I have been unable to locate any investigation giving geometric implications of the (a) existence, or (b) non-existence of solutions of the Fermat problem. If such could be found, the proof of Fermat's last theorem would become a problem of geometry.

It is not inconceivable that the assumed existence of a solution for the Fermat problem would imply a geometrical impossibility. It is in the desire to throw the problem into a geometrical one that we have developed in the next chapter the geometry of Fermat surfaces,

$$F_n : x^n + y^n = z^n$$

¹⁹Ibid., p. 764.

Finally, A. Hurwitz¹² proved that if $x^2 + y^2 = z^2$

is impossible for every integer z , $z > 2$, then

$$x^2 + y^2 + z^2 = 0$$

is impossible for every pair of integers x and y except

where $(x, y, z) = (1, 0, 0)$, $(0, 1, 0)$, or $(0, 0, 1)$.

3.3 Absence of indirect geometric attacks

Although indirect algebraic attacks abound in the literature,

I have been unable to locate any investigation giving

geometric implications of the (a) existence, or (b) non-

existence of solutions of the Fermat problem. If such

could be found, the proof of Fermat's last theorem would

become a problem of geometry.

It is not inconceivable that the assumed existence

of a solution for the Fermat problem would imply a

geometrical impossibility. It is in the desire to know

the problem into a geometrical one that we have developed

in the next chapter the geometry of Fermat surfaces.

$$x^2 + y^2 + z^2 = 1$$

CHAPTER II

1. ANALYTIC GEOMETRY OF F_n

1.1 F_n a conical surface. The intersections of the surfaces F_n and y ax have the equations

$$(1.1.1) \quad \frac{x}{(1+a^{-n})^{1/n}} = \frac{y}{(1+a^n)^{1/n}} = (\pm 1)^{n+1} \frac{z}{(a^n + a^{-n} + 2)^{1/n}}$$

and hence comprise a family of straight lines passing through $(0,0,0)$. For $x^n + y^n = z^n$ and $y^n = a^n x^n$ imply

$$\text{that } x = (\pm 1)^{n+1} \frac{z}{(1+a^n)^{1/n}}. \text{ But } x = \frac{y}{a} = \frac{x}{1}$$

$$\text{Hence } \frac{x}{1} = \frac{y}{a} = (\pm 1)^{n+1} \frac{z}{(1+a^n)^{1/n}} \text{ Multiplication by } \frac{1}{(1+a^{-n})^{1/n}}$$

gives (1.1.1). Thus, the Fermat surfaces are cones with vertices at the origin.

As is true with the familiar F_2 , all the surfaces F_n are symmetric with respect to the origin, which can be seen from equations (1.1.1). Hence, in the sequel we shall limit ourselves without loss of generality to the portions of these conical surfaces for which $z \geq 0$.

1.2 Contour lines of F_n . The contour lines of the Fermat cones fall into categories corresponding, respectively, to even or odd values of n .

1. ANALYTIC CONTINUITY OF F_n

1.1 F_n is meromorphic. The representations of

the surfaces F_n and \bar{F}_n all have the same form

$$(1.1.1) \quad \frac{x}{(1+\alpha^n)^{1/n}} = \frac{z}{(1+\alpha^n)^{1/n}} = (1 \pm i)^{n+1} \frac{z}{(\alpha^n + \alpha^{-n} + 2)^{1/n}}$$

and hence comprise a family of straight lines passing through $(0,0,0)$. For $x^2 + y^2 = z^2$ and $y^2 = x^2$ imply

$$\text{that } x = (1 \pm i)^{n+1} \frac{z}{(1+\alpha^n)^{1/n}} \quad \text{and } x = \frac{z}{\alpha} \quad \text{and } x = \frac{z}{\alpha}$$

$$\text{Hence } \frac{x}{z} = \frac{z}{x} = (1 \pm i)^{n+1} \frac{z}{(\alpha^n + \alpha^{-n} + 2)^{1/n}} \quad \text{multiplication by } \frac{1}{(1+\alpha^n)^{1/n}}$$

gives (1.1.1). Thus, the surfaces F_n are cones with

vertices at the origin.

As is true with the families F_n , all the surfaces

\bar{F}_n are symmetric with respect to the origin, which can

be seen from equations (1.1.1). Hence, in the sequel we

shall limit ourselves without loss of generality to the

portions of these conical surfaces for which $x \geq 0$.

1.2 Contour lines of F_n . The contour lines of

the Fermat cones fall into categories corresponding

respectively, to even or odd values of n .

Case I, $n = 2m$.

In case n is even, the contour lines are curves parallel to the x, y -plane whose projections on that plane are given by the equations $x^n + y^n = z_0^n$, where z_0 is their distance above that plane. We infer from the equations that x is defined only for $|y| \leq |z_0|$ and y for $|x| \leq |z_0|$, and hence, that no asymptote is possible.

From the fact that n is even we know that these contours are symmetric with respect to both the x - and y -axes. The intercepts are at $(0, \pm z_0)$ and $(\pm z_0, 0)$.

Case II, $n = 2m + 1$.

In case n is odd, the contour lines are again curves parallel to the x, y -plane whose projections on that plane are given by the equations $x^n + y^n = z_0^n$, where z_0 is their distance above that plane. These equations are unchanged when x is replaced by y and y by x , so that $y = x$ is a line of symmetry. The points $(z_0, 0)$ and $(0, z_0)$ are the only intercepts. We infer from the equations that points exist on these contours at every real value of x , so that we may profitably test for asymptotes.

Case I, $n = 2m$.

In case n is even, the boundary lines are curves parallel to the x, y -plane whose projections on that plane are given by the equations $x^2 + y^2 = a_0^2$, where a_0 is their distance above that plane. We infer from the equations that x is defined only for $|y| \leq |a_0|$ and y for $|x| \leq |a_0|$, and hence, that no asymptote is possible. From the fact that n is even we know that these contours are symmetric with respect to both the x - and y -axes. The intercepts are at $(0, \pm a_0)$ and $(\pm a_0, 0)$.

Case II, $n = 2m + 1$.

In case n is odd, the contour lines are again curves parallel to the x, y -plane whose projections on that plane are given by the equations $x^2 + y^2 = a_0^2$, where a_0 is their distance above that plane. These equations are satisfied when x is restricted by y and y by x , so that $y = x$ is a line of symmetry. The points $(a_0, 0)$ and $(0, a_0)$ are the only intercepts. We infer from the equations that points exist on these contours at every real value of x , so that no asymptote exists for asymptotes.

We have from $x^n + y^n = z_0^n$ that $y' = -x^{n-1}y^{1-n}$ and hence, the equation of the tangent at (x,y) is given by $y^{n-1}Y + x^{n-1}X = z_0^n$, where (X,Y) are the running coordinates. The intercepts of the tangent line are therefore, $\left(\frac{z_0^n}{x^{n-1}}, 0\right)$ and $\left(0, \frac{z_0^n}{y^{n-1}}\right)$. As (x,y) moves off to infinity these intercepts approach $(0,0)$ so that any asymptote of these contours will pass through the origin. We can find the slope of the asymptotes by considering $\lim_{x \rightarrow \infty} y'$. But $y' = -\left(\frac{z_0^n}{x^n} - 1\right)^{\frac{1-n}{n}}$ and $\lim_{x \rightarrow \infty} y' = -1$. Thus, there is a single asymptote whose equation is $y = -x$.

The following two pages contain sketches of the contour lines in the plane $z = z_0 = 1$ for even and odd n , respectively, and for several values of n in each case to show the manner in which for fixed z these contours approach limiting positions shown by the heavy lines.

To derive equations of limiting positions of $x^n + y^n = z^n$ for increasing even and odd values of n , respectively, we shall first consider two lemmas and a definition.

We have from $x^n + y^n = a^n$ that $y' = -\frac{x^{n-1}}{y^{n-1}}$ and hence, the equation of the tangent at (x, y) is given by $y^{n-1} + x^{n-1} = a^{n-1}$, where (x, y) are the running coordinates. The intercepts of the tangent are

$$\text{therefore, } \left(\frac{a^n}{x^{n-1}}, 0 \right) \text{ and } \left(0, \frac{a^n}{y^{n-1}} \right) \text{ as } (x, y) \text{ moves}$$

off to infinity these intercepts approach $(0, a)$ and $(a, 0)$ and any asymptote of these curves will pass through the origin. We can find the slope of the asymptote by

$$\text{considering } \lim_{x \rightarrow \infty} y' = -\frac{x^{n-1}}{y^{n-1}} = -1$$

and $\lim_{x \rightarrow \infty} y = -1$. Thus, there is a single asymptote

whose equation is $y = -x$.

The following two pages contain sketches of the contour lines in the plane $z = k$, $k = 1$ for even and odd n , respectively, and for several values of n in each case to show the manner in which for fixed z these contours approach limiting positions when n becomes large.

To derive equations of limiting positions of $x^n + y^n = z^n$ for increasing even and odd values of n , respectively, we shall first consider two forms and a definition.

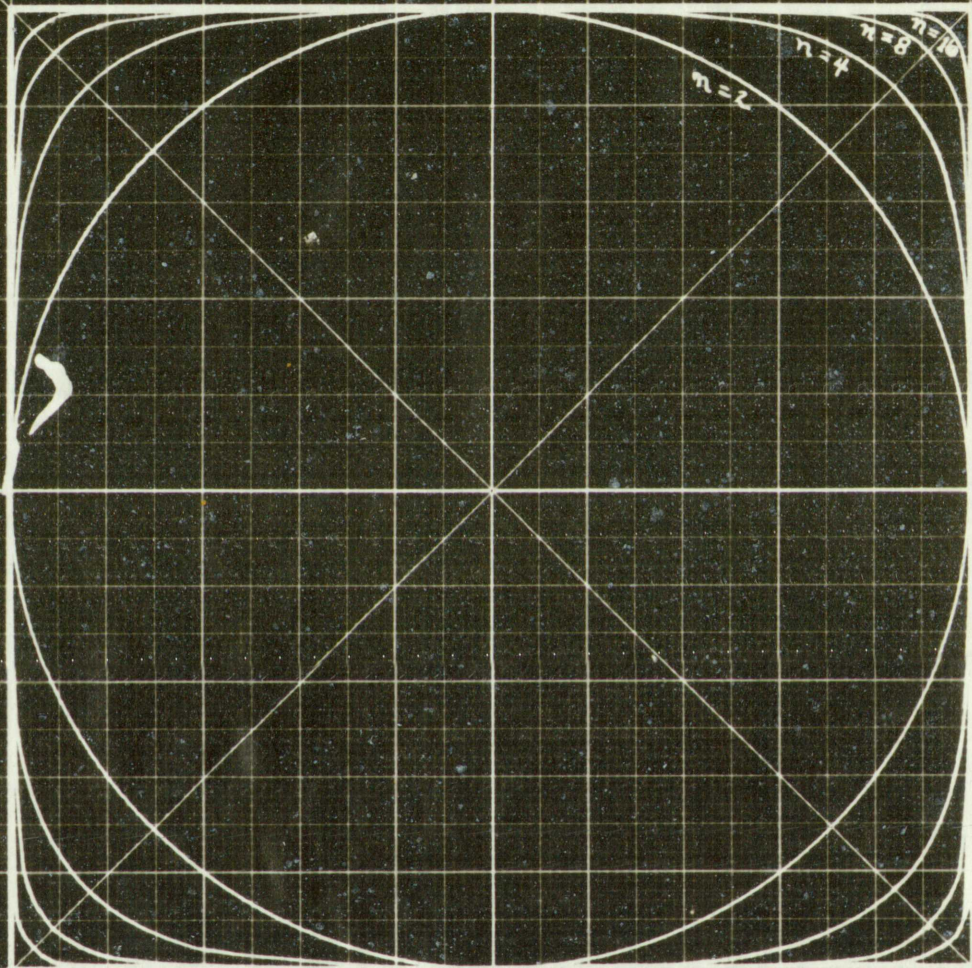
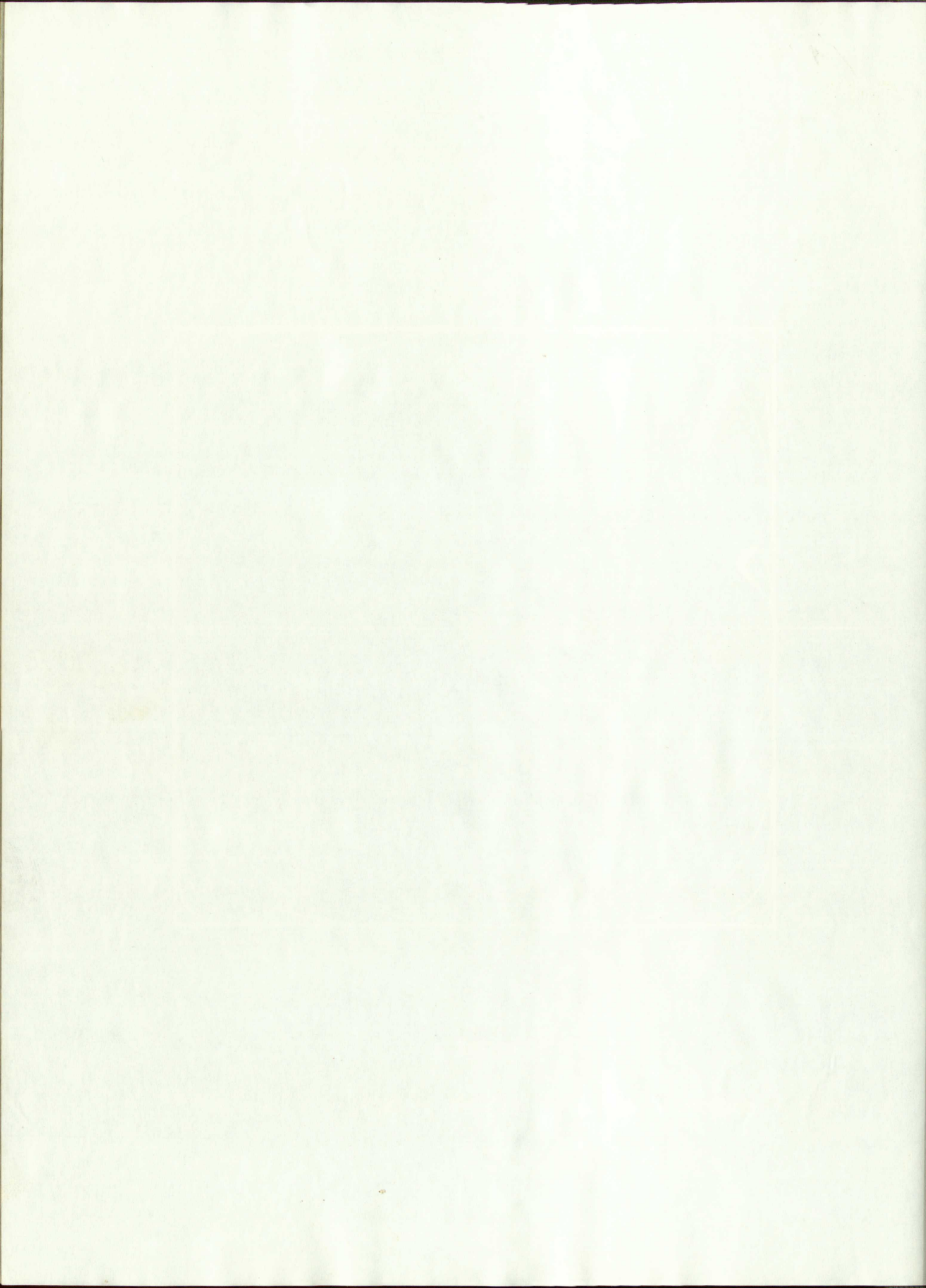


FIGURE 1

CONTOUR LINES OF F_n IN THE PLANE $z = 1$: $n = 2m$



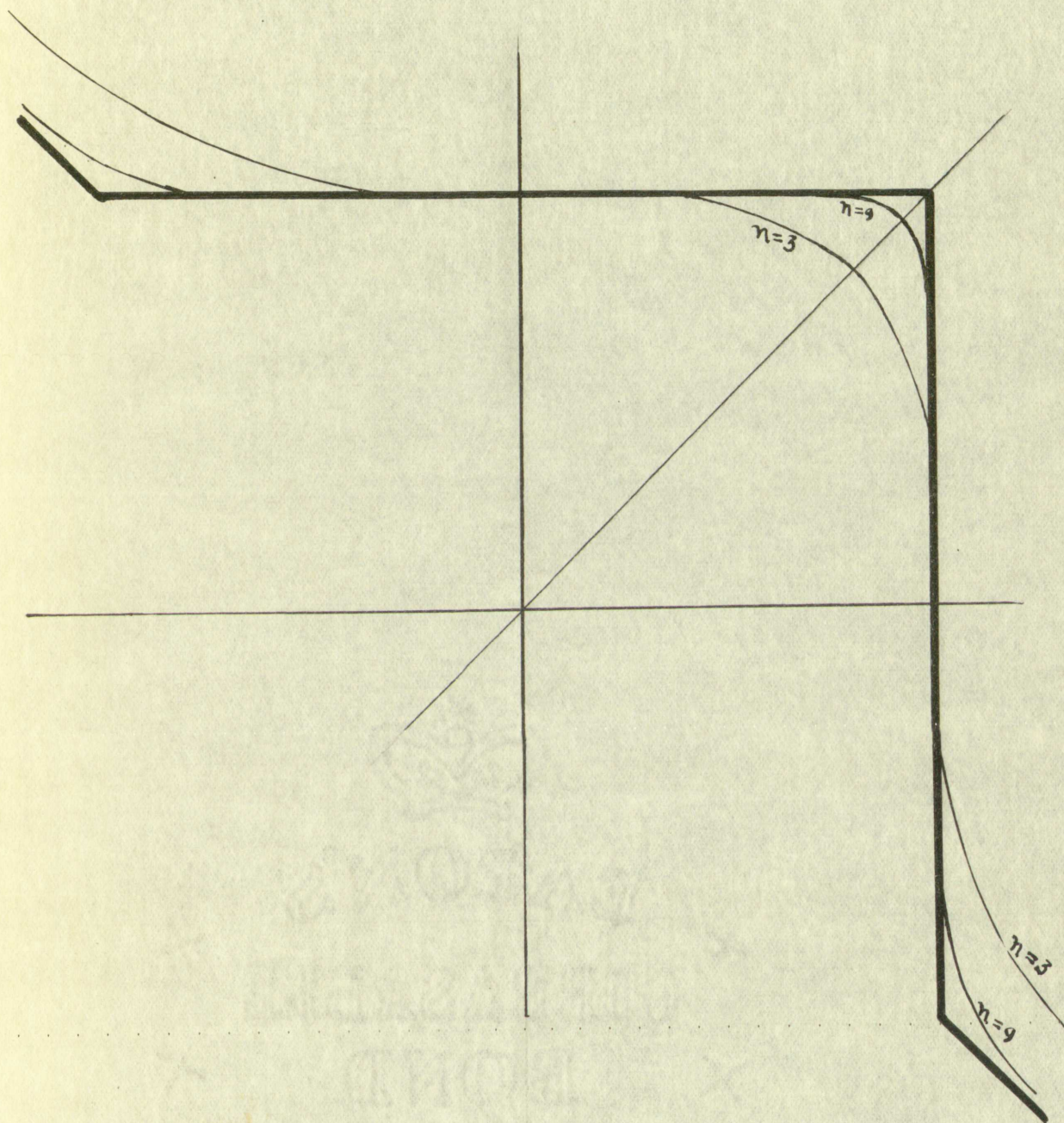
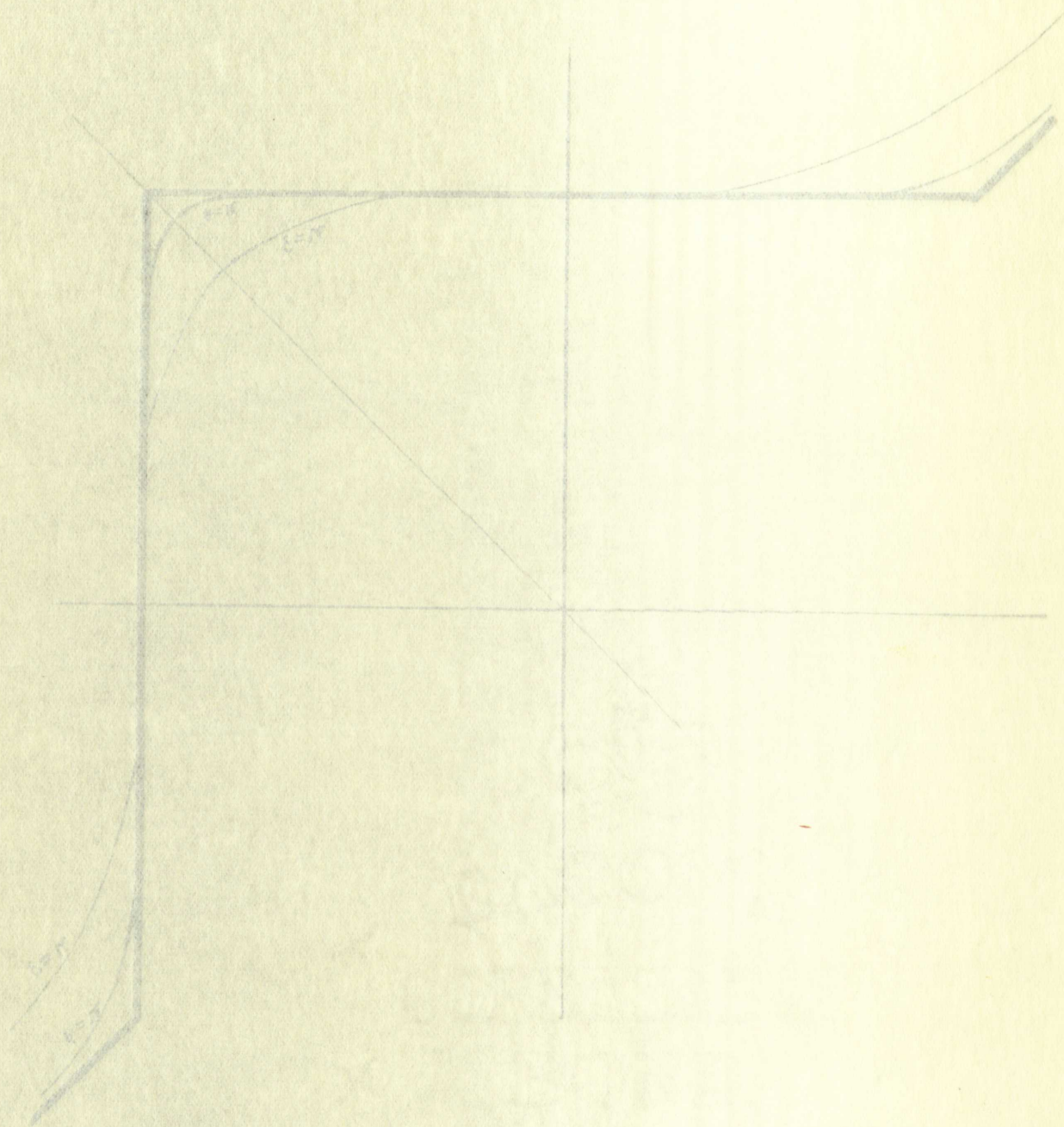


FIGURE 2

CONTOUR LINES OF F_n IN THE PLANE $z = 1$: $n = 2m + 1$

CONTOUR LINES OF R'' IN THE PLANE $z = 1$; $n = 2$ & 3

FIGURE 2



1.3 Lemmas from the theory of real variables.

Let a and b be any real numbers such that $a \geq b \geq 0$.

Then $a = tb \geq 0$, where t is a real number greater than or equal to 1. Whence, if we restrict attention to positive n th roots only,

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = \lim_{n \rightarrow \infty} (t^n b^n + b^n)^{1/n} = \lim_{n \rightarrow \infty} b (t^n + 1)^{1/n}.$$

But,

$$\lim_{n \rightarrow \infty} b (t^n)^{1/n} \leq \lim_{n \rightarrow \infty} b (t^n + 1)^{1/n} \leq \lim_{n \rightarrow \infty} b (t^n + t^n)^{1/n}.$$

So that,

$$bt \leq \lim_{n \rightarrow \infty} b (t^n + 1)^{1/n} \leq bt \lim_{n \rightarrow \infty} 2^{1/n} = bt.$$

Whence, $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = a.$

Similarly, if $0 \leq a \leq b$, $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = b.$

Consequently, if we define

$$M(a, b) = a \quad \text{if } |a| > |b|$$

$$M(a, b) = b \quad \text{if } |b| > |a|$$

$$M(a, b) = \frac{a + b}{2} \quad \text{if } |a| = |b|$$

we may state:

Lemma I. $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = M(a, b).$

1.3. Lemma on the limit of real variables.

Let a and b be any real numbers such that $a > b > 0$.
 Then $a > 0$, where b is a real number greater than
 or equal to 1. When, if we restrict attention to
 positive real numbers only,

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = \lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = \lim_{n \rightarrow \infty} a^n (1 + (b/a)^n)^{1/n} = a \lim_{n \rightarrow \infty} (1 + (b/a)^n)^{1/n}.$$

But,

$$\lim_{n \rightarrow \infty} (1 + (b/a)^n)^{1/n} \leq \lim_{n \rightarrow \infty} (1 + (b/a)^n)^{1/n} = 1.$$

So that,

$$a \leq \lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} \leq a \lim_{n \rightarrow \infty} (1 + (b/a)^n)^{1/n} = a.$$

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = a.$$

$$\text{Similarly, if } 0 < a < b, \lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = b.$$

Consequently, if we define

$$M(a, b) = a \quad \text{if } |a| > |b|$$

$$M(a, b) = b \quad \text{if } |b| > |a|$$

$$M(a, b) = \frac{a+b}{2} \quad \text{if } |a| = |b|$$

we may state:

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = M(a, b).$$

If a and b are any two real numbers such that $|b| < |a|$ and $n = 2m + 1$, then $a = tb$ where t is a real number such that $|t| > 1$. If $1 \leq t$, the theory of Lemma I carries over to this case. If, however, $t \leq -1$, consider

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = \lim_{n \rightarrow \infty} b(1 + t^n)^{1/n}.$$

Now,

$$\lim_{n \rightarrow \infty} b(t^n + t^n)^{1/n} \leq \lim_{n \rightarrow \infty} b(1 + t^n)^{1/n} \leq \lim_{n \rightarrow \infty} b(t^n)^{1/n} = bt.$$

so that,

$$bt = bt \lim_{n \rightarrow \infty} 2^{1/n} \leq \lim_{n \rightarrow \infty} b(1 + t^n)^{1/n} \leq bt.$$

whence, $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = a.$

Similarly, if

$$|a| < |b|, \quad \lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = b.$$

If $a = -b$, $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = 0 = \frac{a+b}{2}.$

Consequently, we may state:

Lemma II. $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = M(a, b).$

1.4 Limiting Fermat surfaces. Divide the family of surfaces $F_n: x^n + y^n = z^n$ where x, y, z are real, $z > 0$, $n > 0$, into the two subfamilies,

$$(1.4.1) \quad x^{2m} + y^{2m} = z^{2m}$$

$$(1.4.2) \quad x^{2m+1} + y^{2m+1} = z^{2m+1}.$$

It is easy to see that if a and b are two real numbers such that $|a| > |b|$ and $a = 2n + 1$, then $a = 2n + 1$ is a real number such that $|a| > 1$. If $1 \leq a$, the theory of Lemma I carried over to this case. If, however, $a \leq -1$, consider

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = \lim_{n \rightarrow \infty} b^n (1 + t^n)^{1/n}$$

$$\lim_{n \rightarrow \infty} b^n (1 + t^n)^{1/n} \leq \lim_{n \rightarrow \infty} b^n (1 + t^n)^{1/n} \leq \lim_{n \rightarrow \infty} b^n (1 + t^n)^{1/n} = b^n$$

$$b^n = b^n \lim_{n \rightarrow \infty} (1 + t^n)^{1/n} \leq \lim_{n \rightarrow \infty} b^n (1 + t^n)^{1/n} \leq b^n$$

$$\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = a$$

$$|a| < |b|, \lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = b$$

$$\text{If } a = -b, \lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = 0 = \frac{a+b}{2}$$

Consequently, we may state:
 Lemma II. $\lim_{n \rightarrow \infty} (a^n + b^n)^{1/n} = M(a, b)$

1.4 Limiting Process. Divide the family

of surfaces $F_n: x^n + y^n = z^n$ where x, y, z are real, $a > 0, n > 0$, into the two subfamilies

$$(1.4.1) \quad x^{2m} + y^{2m} = z^{2m}$$

$$(1.4.2) \quad x^{2m+1} + y^{2m+1} = z^{2m+1}$$

For any choice of x and y in (1.4.1) we have

$$\begin{aligned}\lim_{n \rightarrow \infty} z &= \lim_{n \rightarrow \infty} (x^n + y^n)^{1/n} \\ &= \lim_{n \rightarrow \infty} (|x|^{2m} + |y|^{2m})^{1/2m} \\ &= M(|x|, |y|), \text{ by Lemma I.}\end{aligned}$$

Define the surface $z = M(|x|, |y|)$ to be the limiting Fermat surface, S_E , in this case.

On the other hand, from (1.4.2) we have

$$\begin{aligned}z &= (x^{2m+1} + y^{2m+1})^{1/2m+1} \\ y &= (z^{2m+1} - x^{2m+1})^{1/2m+1} \\ x &= (z^{2m+1} - y^{2m+1})^{1/2m+1}.\end{aligned}$$

Whence by Lemma II

$$\lim_{m \rightarrow \infty} z = M(x, y)$$

$$\lim_{m \rightarrow \infty} y = M(z, -x)$$

$$\lim_{m \rightarrow \infty} x = M(z, -y)$$

We define the limiting surface S_0 to be the point set in space which consists of number triplets which satisfy one or more of the relations:

$$z = M(x, y)$$

$$y = M(z, -x)$$

$$x = M(z, -y)$$

For any choice of x and y in (1.4.1) we have

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log (x^n + y^n)^{1/n} = \lim_{n \rightarrow \infty} \frac{1}{n} \log (|x|^{2n} + |y|^{2n})^{1/2n}$$

$$= M(x, y), \text{ by Lemma I.}$$

Define the surface $z = M(x, y)$ to be the limit

surface, S_M , in this case.

On the other hand, from (1.4.2) we have

$$\begin{aligned} z &= (x^{2m+1} + y^{2m+1})^{1/(2m+1)} \\ y &= (z^{2m+1} - x^{2m+1})^{1/(2m+1)} \\ x &= (z^{2m+1} - y^{2m+1})^{1/(2m+1)} \end{aligned}$$

Whence by Lemma II

$$\lim_{n \rightarrow \infty} x = M(x, y)$$

$$\lim_{n \rightarrow \infty} y = M(x, y)$$

$$\lim_{n \rightarrow \infty} z = M(x, y)$$

We define the limit surface S_M to be the set

set in space which consists of number triplets which

satisfy one or more of the relations:

$$x = M(x, y)$$

$$y = M(x, y)$$

$$z = M(x, y)$$

While S_E is symmetric with respect to all three coordinate planes, S_O is symmetric with respect to the origin and the plane $y = x$. On the following two pages are three-dimensional sketches of S_E and S_O , respectively.

1.5 Existence of rational points on S_E . If there did exist a rational point on any Fermat surface F_n , $n > 2$,

say $\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3} \right)$, then Fermat's conjecture would be

disproved, for we would then have

$$(a_1 b_2 b_3)^n + (b_1 a_2 b_3)^n = (b_1 b_2 a_3)^n$$

for some n greater than 2, and obviously the quantities in parentheses are integers. For this reason, we should be happy to discover such a point, or to be able to prove that none exists, but up to the present no proof or disproof of the existence of such points has been discovered.

On the other hand, we shall see that such points do exist on the limiting Fermat surfaces, and in abundance, and it might seem that this fact would lead directly to an answer to the question proposed in the last paragraph. This is not true as we shall show below.

Consider the intersections of the planes $x = \frac{a_3}{a_4} y$

with the contour of S_E in the plane $z = \frac{a_1}{a_2}$, a_1 integers.

While \mathcal{E}_1 is symmetric with respect to all three coordinate planes, \mathcal{E}_2 is symmetric with respect to the origin and the plane $y = x$. On the following two pages are three-dimensional sketches of \mathcal{E}_1 and \mathcal{E}_2 , respectively.

1.6 Distance of rational points on \mathcal{E}_1 . It does not exist a rational point on any Fermat surface \mathcal{F}_n , $n \geq 5$.

say $\left(\frac{a}{d}, \frac{a_1}{d_1}, \frac{a_2}{d_2} \right)$, then Fermat's conjecture would be

disproved, for we would then have

$$(a, b_1 b_2)^n + (a, a_1 b_2)^n = (a, b_1 a_2)^n$$

for some n greater than 5, and obviously the quantities in parentheses are integers. For this reason, we should be

happy to discover such a point, or to be able to prove that none exists, but up to the present no proof or disproof of

the existence of such points has been discovered.

On the other hand, we shall see that such points do

exist on the limiting Fermat surfaces, and in particular, and

it might seem that this fact would lead directly to an answer

to the question proposed in the last paragraph. This is not

true as we shall show below.

Consider the intersection of the planes $x = \frac{a_1}{d_1}$ and

with the contour of \mathcal{E}_1 in the plane $y = \frac{a_2}{d_2}$, a_1, a_2 integers.

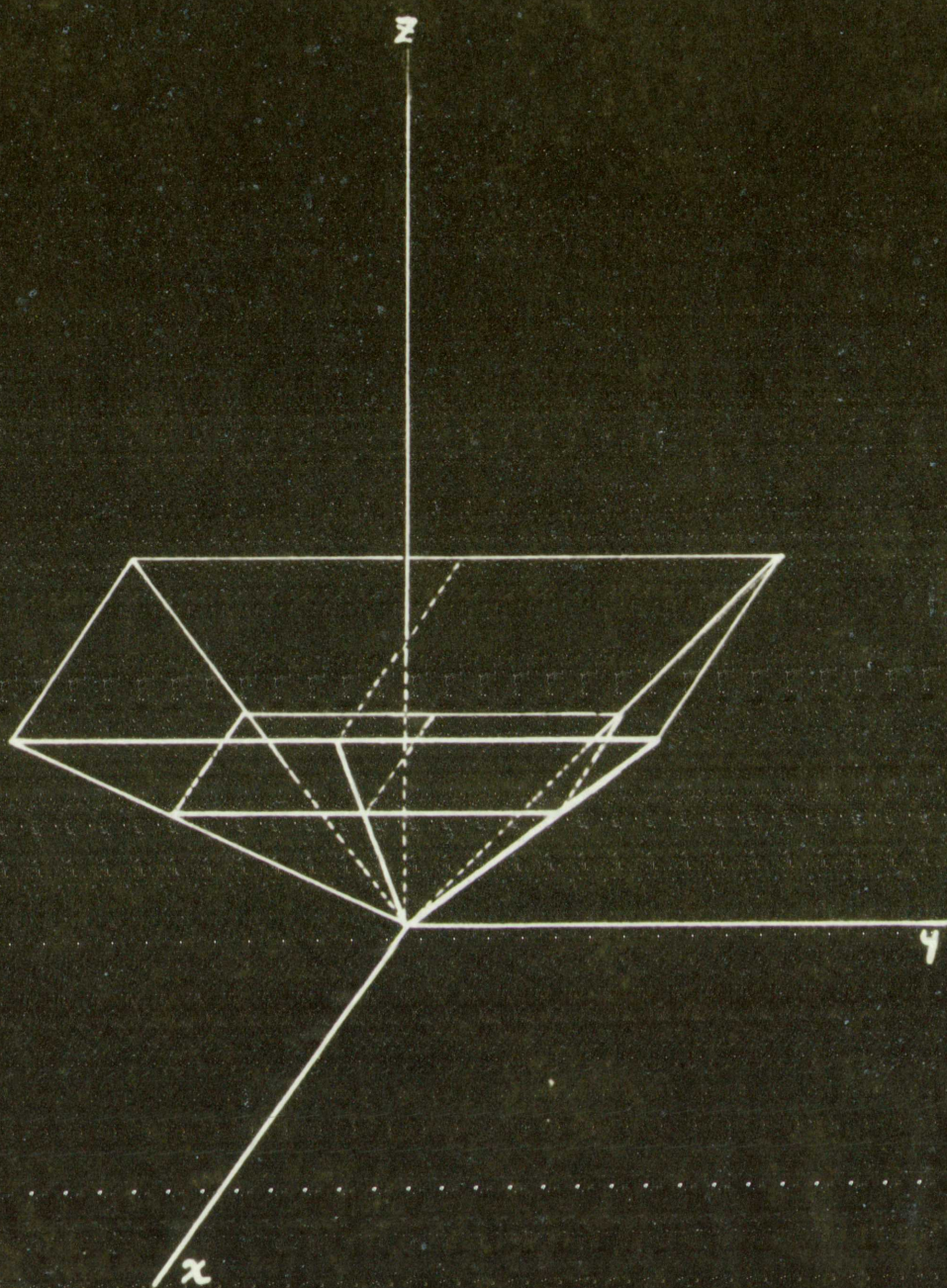
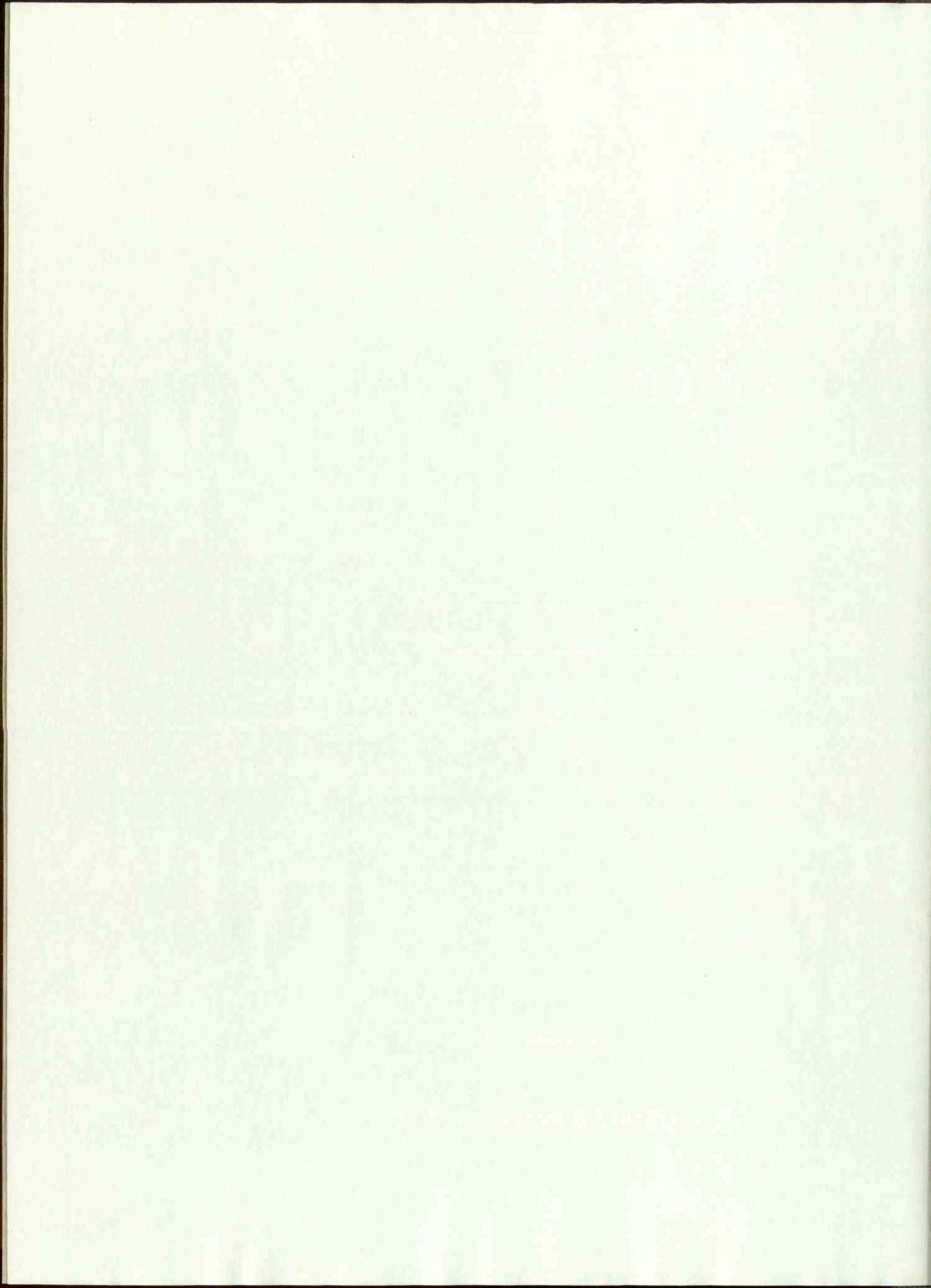


FIGURE 3

FERMAT SURFACE S_E : $z \geq 0$



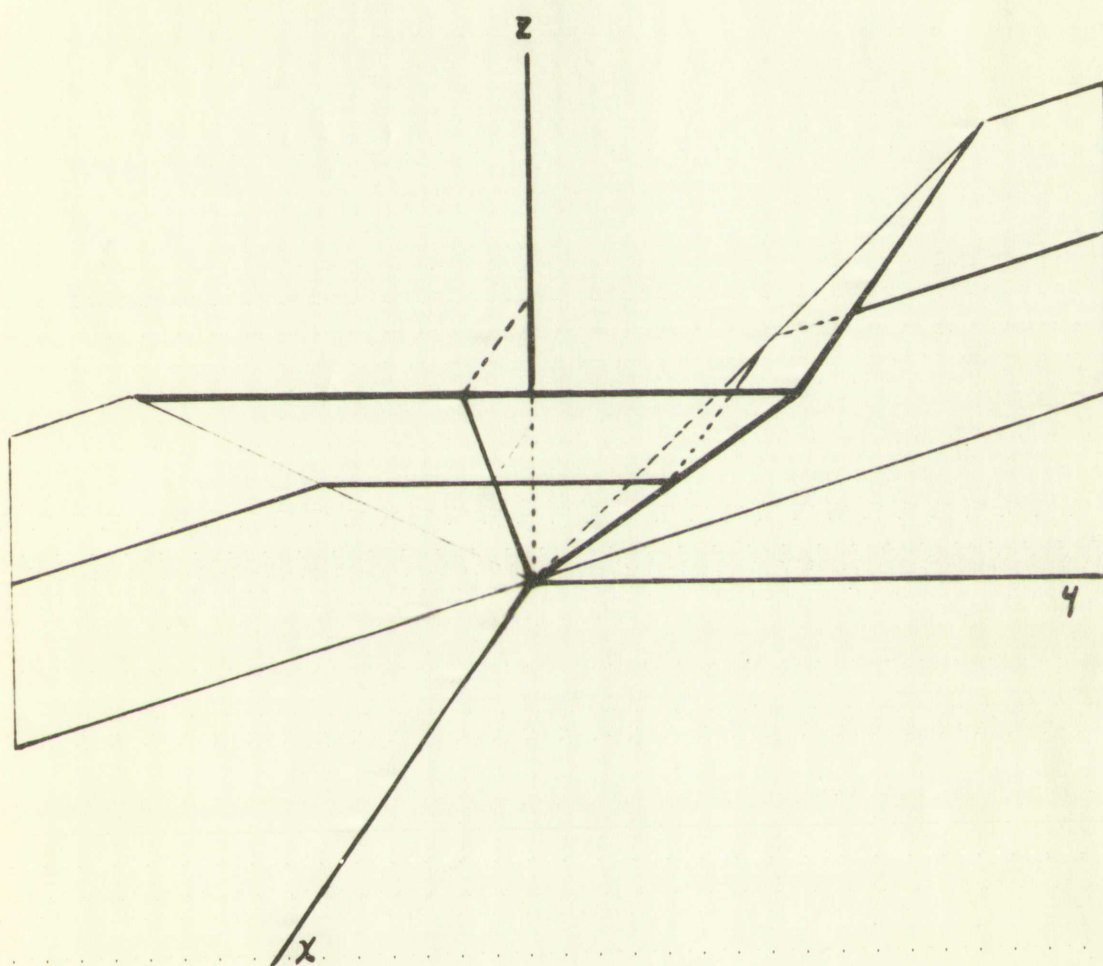


FIGURE 4

FERMAT SURFACE $S_0: z \geq 0$



The intersections are rational points, and in fact, all rational points on S_E may be obtained this way. The points in question constitute an everywhere dense set on F_n .

But consider the intersections with the surfaces F_n of the lines $x = \frac{a_3}{a_4} y$, $z = \frac{a_1}{a_2}$ used to determine the rational points on S_E . These intersections are

$$a_2^n y^n (a_3^n + a_4^n) = a_1^n a_4^n.$$

From this we see that y is rational if and only if

$a_3^n + a_4^n$ is a perfect n th power, which is the very issue at question in our investigation.

The intersection of the line $x = \frac{a_1}{a_2}$ with the line $y = \frac{b_1}{b_2}$ is the point $(\frac{a_1}{a_2}, \frac{b_1}{b_2})$. But consider the line $x = \frac{a_1}{a_2}$ and the line $y = \frac{b_1}{b_2}$.

of the line $x = \frac{a_1}{a_2}$ and the line $y = \frac{b_1}{b_2}$ is the point $(\frac{a_1}{a_2}, \frac{b_1}{b_2})$. From this we see that the intersection of the line $x = \frac{a_1}{a_2}$ and the line $y = \frac{b_1}{b_2}$ is the point $(\frac{a_1}{a_2}, \frac{b_1}{b_2})$.

From this we see that the intersection of the line $x = \frac{a_1}{a_2}$ and the line $y = \frac{b_1}{b_2}$ is the point $(\frac{a_1}{a_2}, \frac{b_1}{b_2})$. The intersection of the line $x = \frac{a_1}{a_2}$ and the line $y = \frac{b_1}{b_2}$ is the point $(\frac{a_1}{a_2}, \frac{b_1}{b_2})$.

2. DIFFERENTIAL GEOMETRY OF F_n

2.1 PARAMETERIZATIONS OF F_n

2.1.1 $Y(u, v_1) = uX(v_1)$, v_1 arc length. The search for the most useful parameterization of F_n first yielded the following. We consider the curve C_n of intersection of F_n with the unit sphere whose center is at $(0,0,0)$. Points P_{v_1} on this curve are uniquely determined in position by their arc length distance v_1 measured along C_n from an arbitrary point on C_n corresponding to arc length distance 0. Let $X(v_1)$ be the unit vector¹ emanating from the origin with terminal point at P_{v_1} . Let u be a scalar, so that for fixed v_1 and variable u , $uX(v_1)$ is the vector representation of the line through the origin and P_{v_1} . Using C as directrix and $uX(v_1)$ as generator, we have one simple representation of F_n .

2.1.2 $Y(u, v_2) = uX(v_2)$, v_2 not arc length. One such representation may be obtained as follows. We again let $X(v_2)$ be the unit vector emanating from the origin and terminating on C_n , where this time v_2 is the tangent of the angle made with the positive x-axis by the projection of $X(v_2)$ on the x,y-plane. There results a representation of

¹Here and elsewhere in this section, the capital letters X , Y , N , will be used to denote three-dimensional vectors.

2. REPRESENTATION OF A CURVE OF F_n

2.1. PARAMETRIZATION OF F_n

2.1.1. $X(v_1) = (x_1, y_1, z_1)$ AND $X(v_2)$. THE SCALAR

for the case under consideration of F_n is defined as follows. We consider the curve C_n of F_n in the F_n space whose center is at $(0, 0, 0)$. Let v_1 on this curve be arbitrarily determined in position by their arc length distance s_1 measured along C_n from an arbitrary point on C_n corresponding to the length distance s_1 . Let $X(v_1)$ be the unit vector emanating from the origin with terminal point at P_1 . Let v be a vector, as shown in Fig. 1, and variable v , $X(v)$ is the vector representation of the line through the origin and P_1 . Using θ as direction and $X(v_1)$ as generator, we have the plane representation of F_n .

2.1.2. $X(v_2) = (x_2, y_2, z_2)$ AND $X(v_3)$. THE SCALAR

representation may be obtained as follows. We again let $X(v_2)$ be the unit vector emanating from the origin and terminating on C_n , where this time v_2 is the tangent of the angle made with the positive x -axis by the projection of $X(v_2)$ on the xy -plane. There results a representation of

¹ Here and elsewhere in this section, the capital letters X, Y, Z will be used to denote three-dimensional vectors.

F_n as $uX(v_2)$, where $X(v_2)$ can be written explicitly:

$$(2.1.2.1) \quad X(v_2) : \left[\frac{1}{w^{1/2}}, \frac{v_2}{w^{1/2}}, \frac{(1+v_2^n)^{1/n}}{w^{1/2}} \right]$$

where $w = 1 + v_2^2 + (1 + v_2^n)^{2/n}$.

2.1.3 Explicit expression for X in parameterization

2.1.1. While in parameterization (2.1.2) we have an explicit expression for $X(v_2)$, the vector $X(v_1)$ has not been given explicitly in (2.1.1); although such an explicit expression possibly would have been of great value in the sequel. In this section we justify our omission by carrying through the explicit determination of $X(v_1)$ in the special case $n = 2$ and showing that an attempt to generalize this to arbitrary n would only lead us into hopeless complexities. Several indirect attempts to obtain $S(v_1)$ explicitly were also unsuccessful.

Using parameterization 2.1.2, arc length along C_n from $v_2 = 0$ to $v_2 = v_2$ is given by $v_1 = \int_0^{v_2} \sqrt{\dot{X}(v_2) | \dot{X}(v_2)} dv_2$, where

$$(2.1.3.1) \quad \dot{X}(v_2) | \dot{X}(v_2) = \frac{1 + (1 + v_2^n)^{\frac{2-2n}{n}} + v_2^{2n-2} (1 + v_2^n)^{\frac{2-2n}{n}}}{w^2}$$

We interrupt our development to show on the following page how (2.1.3.1) was derived from (2.1.2.1).

$\dot{X}(v_2)$ as $\dot{X}(v_2)$, where $\dot{X}(v_2)$ can be written explicitly:

$$(2.1.2.1) \quad \dot{X}(v_2) = \left[\frac{1}{W^{v_2}} : \frac{v_2}{W^{v_2}} : \frac{(1+v_2^{2n})}{W^{v_2}} \right]$$

where $W = 1 + v_2^2 + (1+v_2^{2n})^{2n}$.

2.1.3. Explicit expression for \dot{X} in parameterization

2.1.1. While in parameterization (2.1.2) we have an explicit

expression for $\dot{X}(v_2)$, the vector $\dot{X}(v_1)$ has not been given

explicitly in (2.1.1); although such an explicit expression

possibly would have been of great value in the sequel, in

this section we justify our omission by arguing through

the explicit determination of $\dot{X}(v_1)$ in the special case

2 and showing that an attempt to generalize this to

arbitrary n would only lead us into hopeless complications.

Several indirect attempts to obtain $\dot{X}(v_1)$ explicitly were

also unsuccessful.

Using parameterization 2.1.2, we found along the

line $v_2 = 0$ to $v_2 = v_2$ is given by $v_1 = \int_0^{v_2} \sqrt{\dot{X}(v_2) \dot{X}(v_2)} dv_2$

where

$$(2.1.3.1) \quad \dot{X}(v_2) \dot{X}(v_2) = \frac{1 + (1+v_2^{2n})^{\frac{2n-2}{2n-1}} + v_2^{\frac{2n-2}{2n-1}} (1+v_2^{2n})^{\frac{2n-2}{2n-1}}}{W^{\frac{2n-2}{2n-1}}}$$

We interrupt our development to show on the following

page how (2.1.3.1) was derived from (2.1.2.1).

Given The vector $X(v_2)$ as in (2.1.2.1), we find that $\dot{X}_1 = -[v_2 + v_2^{n-1}(1+v_2^n)^{\frac{2-n}{n}}] W^{\frac{3-n}{2}}$

\dot{X}_2 and \dot{X}_3 can be given in terms of \dot{X}_1 as: $\dot{X}_2 = v_2 \dot{X}_1 + X_1$, $\dot{X}_3 = (1+v_2^n)^{\frac{4n}{n}} \dot{X}_1 + v_2^{n-1}(1+v_2^n)^{\frac{4n}{n}} \dot{X}_1$

Hence, $\dot{X}|\dot{X} = \dot{X}_1^2 + v_2^2 \dot{X}_1^2 + 2v_2 \dot{X}_1 X_1 + X_1^2 + (1+v_2^n)^{\frac{2-n}{n}} v_2^{2n-2} \dot{X}_1^2 + 2(1+v_2^n)^{\frac{2-n}{n}} v_2^{n-1} X_1 \dot{X}_1 + (1+v_2^n)^{\frac{2n}{n}} \dot{X}_1^2$

and $W^2 \dot{X}|\dot{X}$ is given by each of the following expressions:

$$\begin{aligned} & \left[v_2 + (1+v_2^n)^{\frac{2-n}{n}} v_2^{n-1} \right]^2 - 2 \left[v_2 + (1+v_2^n)^{\frac{2-n}{n}} v_2^{n-1} \right]^2 + \left[1 + v_2^{2n-2} (1+v_2^n)^{\frac{2-2n}{n}} \right] W \\ & - v_2^2 - 2v_2^n (1+v_2^n)^{\frac{2-n}{n}} - v_2^{2n-2} (1+v_2^n)^{\frac{4-2n}{n}} + 1 + v_2^2 + (1+v_2^n)^{\frac{2n}{n}} + v_2^{2n-2} (1+v_2^n)^{\frac{2-2n}{n}} + v_2^{2n-2} (1+v_2^n)^{\frac{4-2n}{n}} \\ & - 2v_2^n (1+v_2^n)^{\frac{2-2n}{n}} - 2v_2^{2n} (1+v_2^n)^{\frac{2-2n}{n}} + 1 + (1+v_2^n)^2 (1+v_2^n)^{\frac{2-2n}{n}} + v_2^{2n-2} (1+v_2^n)^{\frac{2-2n}{n}} + v_2^{2n} (1+v_2^n)^{\frac{2-2n}{n}} \\ & - 2v_2^n (1+v_2^n)^{\frac{2-2n}{n}} - 2v_2^{2n} (1+v_2^n)^{\frac{2-2n}{n}} + 1 + (1+v_2^n)^{\frac{2n}{n}} + 2v_2^n (1+v_2^n)^{\frac{2-2n}{n}} + v_2^{2n-2} (1+v_2^n)^{\frac{2-2n}{n}} + v_2^{2n} (1+v_2^n)^{\frac{2-2n}{n}} \end{aligned}$$

Hence, $W^2 \dot{X}|\dot{X} = 1 + (1+v_2^n)^{\frac{2-2n}{n}} + v_2^{2n-2} (1+v_2^n)^{\frac{2-2n}{n}}$

Divide both sides of The last equation by W^2 to obtain (2.1.3.1).

The right member of (2.1.3.1) is essentially bulky, for $\frac{2-2n}{n}$ is not an integer except for $n = 1$ or $n = 2$, as may be seen from the congruence $2 - 2n \equiv 0 \pmod{n}$, which is true if and only if $2(1 - n) \equiv 0 \pmod{n}$. Since $1 - n$ is never divisible by integral n except for $n = 1$, it follows that $2(1 - n) \equiv 0 \pmod{n}$ only for $n = 1$ or $n = 2$.

In case $n = 2$, the right member of (2.1.3.1) reduces

$$\text{to } \frac{1}{2(1+v_2^2)^2} \quad \text{and} \quad v_1 = \frac{\sqrt{2}}{2} \int_0^{v_2} \frac{dv_2}{1+v_2^2} = \frac{\sqrt{2}}{2} \tan^{-1} v_2.$$

Thus, when $n = 2$, $X(v_1)$ is given explicitly by

$$(2.1.3.2) \quad \left[\frac{\cos(\sqrt{2} v_1)}{\sqrt{2}}, \frac{\sin(\sqrt{2} v_1)}{\sqrt{2}}, \frac{1}{2} \right].$$

However, inspection of the general formula (2.1.3.1) from whence this explicit result was derived by integration in the special case $n = 2$ will convince the reader that this direct procedure is not feasible for general n .

2.1.4 $Y(\bar{u}, v_3): \left[\bar{u}, v_3, \frac{(\bar{u}^n + v_3^n)^{1/n}}{n} \right]$. This vector representation of F_n is obtained immediately from $x^n + y^n = z^n$ on setting $x = \bar{u}$, $y = v_3$, $z = (\bar{u}^n + v_3^n)^{1/n}$.

The right member of (2.1.3.1) is essentially unity,

for $\frac{2-2n}{n}$ is not an integer except for $n = 1$ or $n = 2$, as may be seen from the congruence $2 - 2n \equiv 0 \pmod{n}$, which is true if and only if $2(1-n) \equiv 0 \pmod{n}$. Since $1-n$ is never divisible by integer n except for $n = 1$, it follows that $2(1-n) \equiv 0 \pmod{n}$ only for $n = 1$ or $n = 2$. In case $n = 2$, the right member of (2.1.3.1) reduces

$$\text{to } \frac{1}{2(1+v^2)^{1/2}} \quad \text{and } v' = \frac{v}{1+v^2} \quad \text{and } v'' = \frac{2v}{1+v^2}.$$

Thus, when $n = 2$, $X(v')$ is given explicitly by

$$(2.1.3.2) \quad \left[\frac{\cos(\sqrt{2}v')}{\sqrt{2}}, \frac{\sin(\sqrt{2}v')}{\sqrt{2}}, \frac{1}{2} \right].$$

However, inspection of the general formula (2.1.3.1) from whence this explicit result was derived by integration in the special case $n = 2$ will convince the reader that this direct procedure is not feasible for general n .

2.1.4 $X(\bar{u}, \bar{v})$: $\left[\bar{u}, \bar{v}, \frac{(\bar{u}^2 + \bar{v}^2)^{1/2}}{2} \right]$. This vector representation of \bar{u} is obtained immediately from $\bar{x} + \bar{y} = \bar{u}$ on setting $\bar{x} = \bar{u}$, $\bar{y} = \bar{v}$, $\bar{z} = (\bar{u}^2 + \bar{v}^2)^{1/2}$.

2.2 THE FUNDAMENTAL SURFACE QUANTITIES

2.2.1 Parameterization 2.1.1. Since $X(v_1)$ is a unit vector defining C_n , along which v_1 is arc length, we have the relations $X|X = 1$, $X|\dot{X} = 0$, $\dot{X}|\dot{X} = 1$, and $\dot{X}|\ddot{X} = 0$. Hence, $Y_u = X$, $Y_{v_1} = u\dot{X}$, $Y_{uu} = 0$, $Y_{uv_1} = \dot{X}$, and $Y_{v_1v_1} = u\ddot{X}$.

It follows that

$$(2.2.1.1) \quad E = 1, F = 0, G = u^2, D^2 = u^2 \text{ and}$$

$$(2.2.1.2) \quad e = 0, f = 0, g = u(X\ddot{X}), d^2 = 0.$$

Furthermore, if f is the unit normal at the point $Y(u, v_1)$ on F_n , $f = \hat{X} \times \dot{X}$, $f_u = 0$, $f_{v_1} = \hat{X} \times \ddot{X}$, so that

$$(2.2.1.3) \quad \mathcal{E} = 0, \mathcal{F} = 0, \mathcal{G} = \ddot{X}|X - u^2 \text{ and } \mathcal{D}^2 = 0.$$

It is clearly remarkable that these comprehensive results could have been obtained without an explicit expression for $X(v_1)$.

2.2.2 Parameterization 2.1.2. From expression (2.1.2.1) for $X(v_2)$ and $Y = uX$, we have $Y_u = X$ and

$$Y_{v_2} : \left[u \frac{-v_2 - v_2^{n-1}(1+v_2^n)^{\frac{2-n}{n}}}{W^{3/2}}, \mu \frac{1+(1+v_2^n)^{\frac{2}{n}} - v_2^n(1+v_2^n)^{\frac{2-n}{n}}}{W^{3/2}}, \mu \frac{(1+v_2^n)^{\frac{1}{n}} \{-v_2 + (1+v_2^2)(1+v_2^n)^{-1} v_2^{n-1}\}}{W^{3/2}} \right]$$

We interrupt 2.2.2 to show how the components of Y_{v_2} were derived from the results on page 32.

From P.32, $X_{v_2} : \left[u \frac{-v_2 - v_2^{n-1}(1+v_2^n)^{\frac{2-n}{n}}}{W^{3/2}}, u(v_2 \dot{X}_1 + X_1), u \left\{ (1+v_2^n)^{1/n} \dot{X} + v_2^{n-1}(1+v_2^n)^{\frac{1-n}{n}} X \right\} \right]$

$$\begin{aligned} \text{But, } v_2 \dot{X}_1 + X_1 &= \frac{-v_2 [v_2 + v_2^{n-1}(1+v_2^n)^{\frac{2-n}{n}}]}{W^{3/2}} + \frac{W}{W^{3/2}} \\ &= \frac{-\cancel{v_2} - v_2^n (1+v_2^n)^{\frac{2-n}{n}} + 1 + \cancel{v_2} + (1+v_2^n)^{2/n}}{W^{3/2}} \\ &= \frac{1}{u} [\text{component 2 of } X_{v_2}] . \end{aligned}$$

$(1+v_2^n)^{1/n} \dot{X}_1 + v_2^{n-1}(1+v_2^n)^{\frac{1-n}{n}} X_1$ is given by each of :

$$\begin{aligned} &\frac{-(1+v_2^n)^{1/n} [v_2 + v_2^{n-1}(1+v_2^n)^{\frac{2-n}{n}}]}{W^{3/2}} + \frac{v_2^{n-1}(1+v_2^n)^{\frac{1-n}{n}} W}{W^{3/2}} \\ &= \frac{-v_2(1+v_2^n)^{1/n} - \cancel{v_2^{n-1}}(1+v_2^n)^{\frac{3-n}{n}} + v_2^{n-1}(1+v_2^n)^{\frac{1-n}{n}} + v_2^{n+1}(1+v_2^n)^{\frac{1-n}{n}} + \cancel{v_2^{n-1}}(1+v_2^n)^{\frac{3-n}{n}}}{W^{3/2}} \\ &= \frac{(1+v_2^n)^{1/n} [-v_2 + v_2^{n-1}(1+v_2^n)^{-1} + v_2^{n+1}(1+v_2^n)^{-1}]}{W^{3/2}} \\ &= \frac{(1+v_2^n)^{1/n} [-v_2 + v_2^{n-1}(1+v_2^n)^{-1}(1+v_2^2)]}{W^{3/2}} \\ &= \frac{1}{u} [\text{component 3 of } X_{v_2}] . \end{aligned}$$

$$\text{But } \sqrt{2}x + x = \frac{-(-2\sqrt{2} + 2) \pm \sqrt{(-2\sqrt{2} + 2)^2 - 4(1)(1)}}{2(1)}$$

$$= \frac{-(-2\sqrt{2} + 2) \pm \sqrt{8 - 8}}{2} = \frac{2\sqrt{2} - 2}{2} = \sqrt{2} - 1$$

$$= \frac{1}{2} [\text{Component of } \sqrt{2}]$$

$$= \frac{1}{2} \left[\frac{(1+\sqrt{2})^n}{2} + \frac{(1-\sqrt{2})^n}{2} \right] \quad \text{for each of } x^1 + x^0(1+\sqrt{2})^n + x^0(1-\sqrt{2})^n$$

$$= \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2} \quad \text{from P. 20}$$

$$= \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2} \quad \text{from P. 20}$$

$$= \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}$$

$$= \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2} \quad \text{from P. 20}$$

$$= \frac{1}{2} [\text{Component of } \sqrt{2}]$$

It follows that

$$(2.2.2.1) \quad E = 1, \quad F = 0, \quad G = u^2 \left[\frac{(1 + (1 + v_2^n)^{\frac{2-2n}{n}} + v_2^{2n-2} (1 + v_2^n)^{\frac{2-2n}{n}})}{\{1 + v_2^2 + (1 + v_2^n)^{2/n}\}^2} \right]$$

and

$$(2.2.2.2) \quad e = 0, \quad f = 0, \quad g = \frac{(Y_{v_2 v_2} \times Y_{v_2})}{\sqrt{G}}$$

In this case, an explicit expression could be obtained for g by dint of considerable effort. However, we have found in the sequel no use for this result, and consequently, have not obtained it.

It follows that

$$(2.2.2.1) \quad E = 1, \quad F = 0, \quad C = \frac{1}{2} \left[\frac{(1 + \sqrt{2})^n}{(1 + \sqrt{2})^n + (1 + \sqrt{2})^n} \right]$$

and

$$(2.2.2.2) \quad e = 0, \quad f = 0, \quad \frac{(X_1 X_2)}{\sqrt{e}} = \frac{1}{2}$$

In this case, an explicit expression could be obtained for a by hand of considerable effort. However, we have found in the sequel no use for this result, and consequently, have not obtained it.

2.2.3 Parameterization 2.1.3. We obtain from expression (2.1.4) for $Y(u, v_3)$ that

$$(2.2.3.1) \quad \begin{cases} E = 1 + x^{2n-2} (x^n + y^n)^{\frac{2-2n}{n}} \\ F = x^{n-1} y^{n-1} (x^n + y^n)^{\frac{2-2n}{n}} \\ G = 1 + y^{2n-2} (x^n + y^n)^{\frac{2-2n}{n}} \end{cases}$$

and

$$(2.2.3.2) \quad \begin{cases} e = \frac{(n-1) x^{n-2} y^n (x^n + y^n)^{\frac{1-2n}{n}}}{V} \\ f = \frac{(1-n) x^{n-1} y^{n-1} (x^n + y^n)^{\frac{1-2n}{n}}}{V} \\ g = \frac{(n-1) x^n y^{n-2} (x^n + y^n)^{\frac{1-2n}{n}}}{V} \end{cases}$$

where $V = \left[1 + x^{2n-2} (x^n + y^n)^{\frac{2-2n}{n}} + y^{2n-2} (x^n + y^n)^{\frac{2-2n}{n}} \right]^{1/2}$.

Furthermore,

$$(2.2.3.3) \quad f: \left[\frac{-x^{n-1} (x^n + y^n)^{\frac{1-n}{n}}}{V}, \frac{-y^{n-1} (x^n + y^n)^{\frac{1-n}{n}}}{V}, \frac{1}{V} \right].$$

2.2.2 Parameterization 2.1.2. We obtain from

expression (2.1.4) for $Y(u, v)$ that

$$(2.2.2.1) \quad \begin{cases} E = 1 + x^{2N-2} (x^n + y^n) \frac{2-2N}{N} \\ F = x^{n-1} y^{N-1} (x^n + y^n) \frac{N-2}{N} \\ G = 1 + y^{2N-2} (x^n + y^n) \frac{2-2N}{N} \end{cases}$$

and

$$(2.2.2.2) \quad \begin{cases} a = \frac{(n-1) x^{n-2} y^{2-n} (x^n + y^n) \frac{2-2N}{N}}{V} \\ b = \frac{(1-n) x^{n-1} y^{1-n} (x^n + y^n) \frac{2-2N}{N}}{V} \\ c = \frac{(n-1) x^n y^{n-2} (x^n + y^n) \frac{2-2N}{N}}{V} \end{cases}$$

where $V = [1 + x^{2N-2} (x^n + y^n) \frac{2-2N}{N} + y^{2N-2} (x^n + y^n) \frac{2-2N}{N}]^{1/2}$.

Furthermore,

$$(2.2.2.3) \quad \begin{cases} \frac{1}{V} \left[\frac{-x^{n-1} (x^n + y^n) \frac{2-2N}{N}}{V} \right] \\ \frac{1}{V} \left[\frac{-y^{n-1} (x^n + y^n) \frac{2-2N}{N}}{V} \right] \end{cases}$$

2.3 IMPLIED DIFFERENTIAL GEOMETRIC PROPERTIES OF F_n

2.31 Parameterizations 2.11 and 2.12. We first obtain the differential equations of the geodesics on F_n . These equations have the form²

$$(2.3.1.1) \quad \begin{cases} \frac{d^2 u}{ds^2} + C_{11}' \left(\frac{du}{ds} \right)^2 + 2 C_{12}' \frac{du}{ds} \frac{dv}{ds} + C_{22}' \left(\frac{dv}{ds} \right)^2 = 0 \\ \frac{d^2 v}{ds^2} + C_{11}'' \left(\frac{du}{ds} \right)^2 + 2 C_{12}'' \frac{du}{ds} \frac{dv}{ds} + C_{22}'' \left(\frac{dv}{ds} \right)^2 = 0 \end{cases}$$

But from parameterization 2.1.1, we have

$$C_{11}' = 0, \quad C_{12}' = 0, \quad C_{22}' = u(\ddot{X}|X) = -u$$

$$C_{11}'' = 0, \quad C_{12}'' = \frac{1}{u}, \quad C_{22}'' = \dot{X}|\ddot{X} = 0$$

Hence, for F_n , (2.3.1.1) reduces to

$$(2.3.1.2) \quad \begin{cases} \frac{d^2 u}{ds^2} - u \left(\frac{dv}{ds} \right)^2 = 0 \\ \frac{d^2 v}{ds^2} + \frac{2}{u} \left(\frac{du}{ds} \right) \left(\frac{dv}{ds} \right) = 0 \end{cases}$$

We immediately verify that the u -curves are geodesics.

²W. C. Graustein, Differential Geometry, p. 155.

2.2. IMPLICIT DIFFERENTIAL GEOMETRY: PROPERTIES OF \mathcal{M}

2.2.1 Parameterizations 2.1.1 and 2.1.2. We first

obtain the differential equations of the geodesics on \mathcal{M} .

These equations have the form

$$(2.2.1.1) \quad \begin{cases} \frac{d^2 u}{ds^2} + C_{11}^1 \left(\frac{du}{ds} \right)^2 + 2 C_{12}^1 \frac{du}{ds} \frac{dv}{ds} + C_{22}^1 \left(\frac{dv}{ds} \right)^2 = 0 \\ \frac{d^2 v}{ds^2} + C_{11}^2 \left(\frac{du}{ds} \right)^2 + 2 C_{12}^2 \frac{du}{ds} \frac{dv}{ds} + C_{22}^2 \left(\frac{dv}{ds} \right)^2 = 0 \end{cases}$$

But from parameterization 2.1.1, we have

$$C_{11}^1 = 0, \quad C_{12}^1 = 0, \quad C_{22}^1 = \omega(\dot{X}|\dot{X}) = -\omega$$

$$C_{11}^2 = 0, \quad C_{12}^2 = \frac{1}{\omega}, \quad C_{22}^2 = \dot{X}|\ddot{X} = 0$$

Hence, for \mathcal{M} (2.2.1.1) reduces to

$$(2.2.1.2) \quad \begin{cases} \frac{d^2 u}{ds^2} - \omega \left(\frac{dv}{ds} \right)^2 = 0 \\ \frac{d^2 v}{ds^2} + \frac{1}{\omega} \left(\frac{du}{ds} \right) \left(\frac{dv}{ds} \right) = 0 \end{cases}$$

We immediately verify that the α -curves are geodesics.

To obtain other important systems of curves on F_n we turn to the equation of the lines of curvature³

$$(2.3.1.3) \quad (Ef - Fe) du^2 + (Eg - Ge) du dv + (Fg - GF) dv^2 = 0$$

and that of the asymptotic lines⁴

$$(2.3.1.4) \quad e du^2 + 2f du dv + g dv^2 = 0.$$

Using parameterization 2.1.1,

$$e = f = F = 0, \quad E = 1, \quad G = u^2, \quad g = u(x \ddot{x})$$

so that (2.3.1.3) and (2.3.1.4) reduce to

$$(2.3.1.5) \quad u(x \ddot{x}) du dv = 0$$

and

$$(2.3.1.6) \quad u(x \ddot{x}) dv^2 = 0$$

respectively. Because $e = f = 0$, we could not have also $g = 0$, since this would imply that F_n is a plane. Hence, for parameterizations 2.1.1 and 2.1.2 the parametric curves are the lines of curvature, while the u -curves are the asymptotic lines.

³Ibid., p. 111.

⁴Ibid., p. 127.

To obtain other important systems of curves on V

we turn to the equation of the lines of curvature

$$(2.2.1.2) \quad (E_f - Fg) dx^2 + (Eg - Gf) dx dy + (Fg - Gf) dy^2 = 0$$

and that of the asymptotic lines

$$(2.2.1.4) \quad e dx^2 + 2f dx dy + g dy^2 = 0$$

Using parametrization (2.1.1)

$$e = f = 0, \quad E = 1, \quad G = u^2, \quad f = u(x \times X)$$

so that (2.2.1.2) and (2.2.1.4) reduce to

$$(2.2.1.5) \quad u(x \times X) dx dy = 0$$

and

$$(2.2.1.6) \quad u(x \times X) dx^2 = 0$$

respectively. Because $e = f = 0$, we could not have also $E = 0$, since this would imply that V is a plane. Hence, for parametrizations (2.1.1) and (2.1.2) the parametric curves are the lines of curvature, while the u -curves are the asymptotic lines.

²Imb., p. 111.
⁴Imb., p. 127.

2.3.2 Parameterization 2.1.3. The angle between the directed u - and v -curves is given by

$$\cos \omega = \frac{x^{n-1} y^{n-1} (x^n + y^n)^{\frac{2-2n}{n}}}{\left\{ [1 + x^{2n-2} (x^n + y^n)^{\frac{2-2n}{n}}] [1 + y^{2n-2} (x^n + y^n)^{\frac{2-2n}{n}}] \right\}^{1/2}},$$

since along the curves $v = \text{constant}$, the direction of the tangent is X_u ; along $u = \text{constant}$, it is X_v . Thus,

$$\cos \omega = \frac{X_u | X_v}{\sqrt{E} \sqrt{G}},$$

which reduces to the value given above.

Let $S: x^2 + y^2 + z^2 - r^2 = 0$ intersect F_n at (x, y, z) . The normal N to S at this point has direction components x, y, z . From (2.2.3.3), direction components of the normal N_n to F_n at this point are

$$\left[-x^{n-1} (x^n + y^n)^{\frac{1-n}{n}}, -y^{n-1} (x^n + y^n)^{\frac{1-n}{n}}, 1 \right].$$

Hence, $N | N_n = 0$, and the normals intersect orthogonally at each point of their curve of intersection. This result verifies the famous theorem of Joachimsthal⁵, that if a curve of intersection of two surfaces is a line of curvature on both, the surfaces intersect at the same angle along the curve. This is the situation obtaining in our case, since as is well known, every curve on a sphere is a line of

⁵ Graustein, op. cit., p. 121.

as is well known, every curve on a sphere is a line of

curve. This is the situation obtaining in our case, since

on both, the surfaces intersect at the same angle along the

curve of intersection of two surfaces is a line of curvature

verifies the famous theorem of Joachimsthal. And if a

each point of their curve of intersection. This result

Hence, $W_{12} = 0$, and the normals intersect orthogonally at

$$[-x^{n-1}(x^n+y^n)^{\frac{1-n}{2}}, -y^{n-1}(x^n+y^n)^{\frac{1-n}{2}}, 1]$$

the normal N_1 to S_1 at this point are

components x, y, z . From (2.2.3), direction components of

(x, y, z) . The normal N_2 to S_2 at this point has direction

$$\text{Let } S: x^2 + y^2 + z^2 = 1 \text{ intersect } S_1 \text{ at}$$

which reduces to the value given above.

$$\cos \omega = \frac{x_1/x_2}{\sqrt{E} \sqrt{E}}$$

tangent to S_1 ; along u = constant, it is A_1 . Thus,

along the curve v = constant, the direction of the

$$\cos \omega = \frac{x^{n-1}y^{n-1}(x^n+y^n)^{\frac{1-n}{2}}}{\left\{ [1+x^{2n-2}(x^n+y^n)^{\frac{1-n}{2}}] + [1+y^{2n-2}(x^n+y^n)^{\frac{1-n}{2}}] \right\}^{\frac{1}{2}}}$$

directed u - and v -curves is given by

2.2.3 Intersection 2.2.3. The angle between the

curvature, and we have found above that C_n is also a line of curvature on F_n .

Following an attack suggested by this result, let S_P denote the sphere passing through the point P on F_n . Direction numbers of the normal to the sphere are (x, y, z) . If P is an integral point, these direction numbers (A, B, C) are integers. Let (a, b, c) be the set of direction numbers of the normal to F_n at P given by

$$a = -x^{n-1}(x^n + y^n)^{\frac{1-n}{n}}, \quad b = -y^{n-1}(x^n + y^n)^{\frac{1-n}{n}}, \quad c = 1.$$

The orthogonality property implies that $Aa + Bb = C$ or $[A^n + B^n]^{\frac{1}{n}} = C$. We do not attain a contradiction of our assumption that an integral point does exist on F_n unless it is impossible that $A^n + B^n = C^n$. Thus again, as in section 1.5, our indirect attack has led back to the very theorem we seek to prove.

Finally, from parameterization 2.1.4 we obtain three heuristic geometric implications of Fermat's last theorem:

Theorem I. If there exists an integral triad on F_n , where these surfaces are represented parametrically in terms of x and y , then the coefficients, E, F, G , of the first fundamental differential quadratic form of F_n are integers.

consequence, and we have found above that G is also a line

of curvature on V_n .

Following an attack suggested by this result, let

P denote the sphere passing through the point P on V_n .

Direction numbers of the normal to the sphere are (x, y, z) .

If P is an integral point, these direction numbers (x, y, z)

are integers. Let (a, b, c) be the set of direction numbers

of the normal to V_n at P given by

$$a = -x^{n-1}(x'' + y''), \quad b = -y^{n-1}(x'' + y''), \quad c = 1 - \frac{1}{n} \frac{(x'')^2}{x^{n-2}} - \frac{1}{n} \frac{(y'')^2}{y^{n-2}}$$

The orthogonality property implies that $Aa + Bb = C$ or

$$[A'' + B'']^n = C. \quad \text{We do not obtain a contradiction of}$$

our assumption that an integral point does exist on V_n .

unless it is impossible that $A'' + B'' = C''$. Thus again,

as in section 1.5, our indirect attack has led back to the

very theorem we seek to prove.

Finally, from generalization 3.1.4 we obtain three

interesting geometric implications of Fermat's last theorem:

Theorem I. If there exists an integral point on V_n , where

these surfaces are represented parametrically in terms of

x and y , then the coefficients E, F, G of the first

fundamental differential quadratic form of V_n are integers.

Theorem II. If when F_n is represented parametrically in terms of x and y there exists on the surface F an integral triad (x, y, z) such that $x^n + y^n = (z^{1/2})^n$, then the coefficients of the first fundamental differential quadratic form of F_n are integers.

Theorem III. If there exists an integral triad on F_n , where these surfaces are represented parametrically in terms of x and y , then the quotients, obtained by dividing the coefficients e, f, g , of the second fundamental differential quadratic form of F_n by the corresponding components of the unit normal, are rational numbers.

The first two theorems derive from inspection of the coefficients of the first fundamental form, while the divisions mentioned in the third theorem yield

$$\frac{e}{f_1} = \frac{(1-n)y^n}{x(x^n+y^n)} \quad , \quad \frac{f}{f_2} = \frac{(n-1)x^{n-1}}{x^n+y^n} \quad , \quad \frac{g}{f_3} = \frac{(n-1)x^n y^{n-2}(x^n+y^n)^{1/n}}{(x^n+y^n)^2}$$

which are seen to be rational numbers if $x^n + y^n = z^n$,
 x, y, z , integers.

Theorem II. If F_n is a homogeneous polynomial of degree n in x and y which satisfies the condition that $F_n(x, y) = 0$ is a factor of the first fundamental differential equation of the first kind, then the quotient is a form of F_n of the form

Theorem III. If there exists an integral curve of the form $y = vx$ where v is a function of x and y , then the quotient, obtained by dividing the coefficients a, b, c of the second fundamental differential equation of the first kind by the corresponding components of the unit normal, are rational functions.

The third and fourth theorems derive from the condition of the coefficients of the first fundamental form, while the divisions mentioned in the fifth theorem yield

$$\frac{a}{b} = \frac{(1-v^2)y^2}{x(x^2+y^2)}, \quad \frac{c}{b} = \frac{(1-v^2)x^2}{x^2+y^2}, \quad \frac{c}{a} = \frac{(1-v^2)x^2}{(x^2+y^2)^2} = \frac{(1-v^2)x^2}{(x^2+y^2)^2}$$

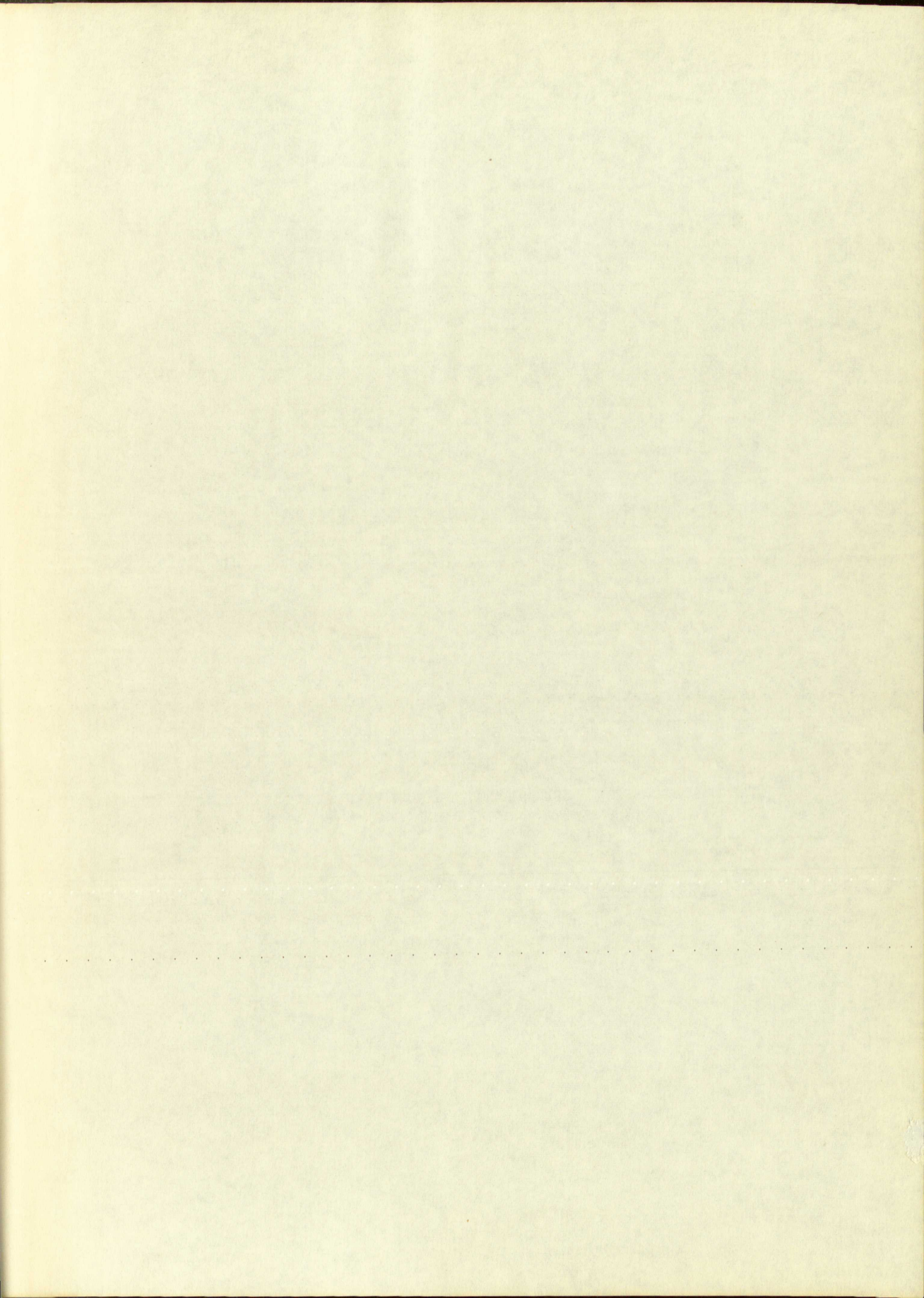
which are seen to be rational functions if $m + n = 0$, a, b, c integers.

CONFIDENTIAL
BOND

BIBLIOGRAPHY

STENOGRAPHY

- Bachman, P., Niedere Zahlentheorie. 2 vols.;
Leipzig: B. G. Teubner, 1910.
- Cantor, M., Vorlesungen über Geschichte Der Mathematik.
3 vols.; Leipzig: B. G. Teubner, 1900.
- Dickson, L. E., History of the Theory of Numbers. 3 vols.;
Washington: Carnegie Institution, 1920. ✓
- _____, "Fermat's Last Theorem and the Origin and Nature of
the Theory of Algebraic Numbers", Annals of Mathematics,
Series 2, Vol. XVIII, 1917., pp. 161-76.
- Graustein, W. C., Differential Geometry. New York: The
Macmillan Company, 1949. 230 pp.
- Landau, E., Vorlesungen über Zahlentheorie. 3 vols.;
New York: Chelsea Publishing Company, 1947.
- LaPaz, Lincoln, Lecture Notes on Number Theory, Ohio State
University, 1934-1941.
- Miller, G. A., Historical Introduction to Mathematical
Literature. New York: The Macmillan Co., 1916. 302 pp.
- Nielsen, N., Traite Elementaire Des Nombres De Bernoulli.
Paris: Gauthier-Villars, 1923. 398 pp.
- Uspensky, J. V. and Heaslet, M. A., Elementary Number Theory. ✓
New York: McGraw-Hill Book Company, 1939. 484 pp.
- Vandiver, H. S., "Fermat's Last Theorem, Its History, and
the Nature of the Known Results Concerning It", American
Mathematical Monthly, Vol. 53, 1946. pp. 555-78. ✓



IMPORTANT!

Special care should be taken to prevent loss or damage of this volume. If lost or damaged, it must be paid for at the current rate of typing.

PR 6-100-9 63

