Texas Southern University
Digital Scholarship @ Texas Southern University

Theses (Pre-2016) Theses

7-1993

# Pythagorean Triples and Fermatis Last Theorem

Melanie L. "Goldie" Davis

Follow this and additional works at: https://digitalscholarship.tsu.edu/pre-2016_theses

Recommended Citation
Davis, Melanie L. "Goldie", "Pythagorean Triples and Fermatis Last Theorem" (1993). *Theses (Pre-2016)*. 150.
https://digitalscholarship.tsu.edu/pre-2016_theses/150

This Thesis is brought to you for free and open access by the Theses at Digital Scholarship @ Texas Southern University. It has been accepted for inclusion in Theses (Pre-2016) by an authorized administrator of Digital Scholarship @ Texas Southern University. For more information, please contact haiying.li@tsu.edu.

# PYTHAGOREAN TRIPLES AND FERMAT'S LAST THEOREM

THESIS

BY

MELANIE L. "GOLDIE" DAVIS

1993

ROBERT J TERRY LIBRARY
TEXAS SOUTHERN UNIVERSITY

# PYTHAGOREAN TRIPLES AND FERMAT'S LAST THEOREM

THESIS

Presented in Partial Fulfillment of the Requirements for the Degree Master of Science in the Graduate School of Texas Southern University

By

Melanie L. "Goldie" Davis, B.A.

Texas Southern University

1993

Approved by

Robert M. Nelms

Chairperson, Thesis Committee

Dean, The Graduate School

## ABSTRACT

## PYTHAGOREAN TRIPLES AND FERMAT'S LAST THEOREM

By

Melanie L. "Goldie" Davis, M. S.

Texas Southern University, 1993

Professor Robert Nehs, Advisor

This is the study of the Diophantine equations, in particular, Pythagorean Triples and Fermant's Last Theorem.

The main objective of this survey is to show the nonexistence of a solution to prove or disprove the equation for all n where n is a natural number larger than 2.

**Approved by:**

Robert M. Nehs — 8-20-99

**Chairperson, Thesis Committee** — **Date**
**Robert Nehs, Ph.D.**
**Department of Mathematics**

James E. Ginn — 8-20-99

**Thesis Committee** — **Date**
**James E. Ginn, Ph.D.**
**Department of Mathematics**

John B. Sapp — 8/20/99

**Thesis Committee** — **Date**
**(Representing Graduate School)**
**John B. Sapp, Jr., Ph. D.**
**Department of Science**

Willie E. Taylor, Jr. — 8-20-99

**Thesis Committee** — **Date**
**Willie E. Taylor, Jr., Ph.D.**
**Department of Mathematics**

# TABLE OF CONTENTS


| | Page |
|---|---|
| VITA | iv |
| DEDICATION | v |
| ACKNOWLEDGEMENTS | vi |
| CHAPTER | |
| 1. INTRODUCTION | 1 |
| 2. BASIC PROPERTIES OF THE INTEGERS | 6 |
| 3. PYTHAGOREAN TRIPLES | 26 |
| 4. FERMAT'S THEOREM FOR n = 3 AND 4 | 36 |
| 5. SUMMARY | 45 |
| REFERENCES | 46 |

VITA

August 24, 1955 ..... Born: Houston, Texas

1988-1992 ..... TEXAS SOUTHERN UNIVERSITY

Major Field ..... Mathematics

## DEDICATION

I dedicate this thesis to my darling daughter, Melandrea. All things are possible through Christ who strengthens us.

## ACKNOWLEDGEMENTS

I would like to express my appreciation to Professor Robert Nehs for his guidance, encouragement and contribution of knowledge and time during this research and my entire graduate study. Thanks go to Professor Williams for the encouragement on the study of number theory and to Professor Ginn for the motivation that helped to lead to my graduate study in mathematics. I give thanks to my committee members, Drs. Willie Taylor and John Sapp for their time and advice, to the entire staff of the Math Department whom all are giants that allowed me to stand on their shoulders. Also, I give thanks to the members of my family whose chain was so strong they didn't even know when I was pulling on them. Thank you. To my daughter, Melandrea, whom I love so dearly I thank you for allowing me to complete my education and for your outstanding patience, at the age of two, while attending the library and school. For if you were not working on your thesis, I could not have finished mine. May GOD continue to bless you. Most of all, I give thanks to GOD for without him nothing would have been possible.

# CHAPTER I

## INTRODUCTION

Of all the branches of mathematics, the one that seems to appeal most to our esthetic feelings is number theory, considered by many to be the queen of mathematics. Why is that so? Some people believe that this strong esthetic appeal is due to the very limited practical usefulness of number theory. However, there is another reason. In hardly any other branch of mathematics is it possible to ask really significant, non-trivial questions without preceding them by an annoyingly long list of definitions. In number theory, on the other hand, one can ask many questions in such simple terms that the famous "man in the street" can immediately understand but may not be able to answer them. The answers to some of these "simple to ask" questions are so difficult that nobody has yet found them. In particular, one of these questions is known as Fermat's Last Theorem.

Fermat's problem, also called Fermat's Last Theorem, has attracted the attention of mathematicians for more than three centuries. Many clever methods have been devised to attack the problem, and many beautiful theories have been created with the aim of proving the theorem. Yet, despite all the attempts, the question remains unanswered.

Pierre de Fermat (1601-1665) was a French judge who lived in Toulouse. He was a universal spirit, cultivating poetry, Greek philology, law but mainly mathematics. His special interest concerned the solutions of equations in integers known as Diophantine equations.

For example, Fermat studied equations of the type $X^2 - dy^2 = \pm 1$, where d is a positive square-free integer (that is without square factors different from 1), and he discovered the existence of infinitely many solutions. He has also discovered which natural numbers n may be written as the sum of two squares, namely, those with the following property: every prime factor p of n which is congruent to 3 modulo 4 must divide n to an even power.

[Fermat wrote: It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into powers of like degree; I have discovered a truly remarkable proof.](13 Lectures on Fermat's Last Theorem.) In modern language, Fermat's statement means: The equation $X^n + Y^n = Z^n$, where n is a natural number larger than 2, has no solution in integers all different from 0.

No proof of this statement was ever found among Fermat's papers. He seldom published his work and often the only records of what he did are statements of theorems he discovered, usually given without proofs, in letters to his friends, in notebooks, in margins of books that he read and so

on. However, he did write a proof that the equations $X^4 - Y^4 = Z^2$ and $X^4 + Y^4 = Z^2$ have no solutions in integers all different from 0.

With very few exceptions, all Fermat's other assertions have now been confirmed. So this problem is usually called Fermat's Last Theorem, despite the fact that it has never been proved.

Fermat's most notable erroneous belief concerns the numbers $F_n = 2^{2^n}+1$, which he thought were always prime. But Euler showed that 641 is a factor of $f_5 = 2^{32} + 1$. Sierpinski and Schinzel pointed out some other false assertions made by Fermat.

In trying to prove Fermat's theorem for every positive integer $n \geq 3$, Gauss made the following observation. If the theorem holds for an integer m and $n = tm$ is a multiple of m, then it holds also for n. For, if x,y,z are nonzero integers and $x^n + y^n = z^n$ then $(x^t)^m + (y^t)^m = (z^t)^m$, contradicting the hypothesis. Since every integer $n \geq 3$ is a multiple of 4 or of a prime $p \neq 2$, it suffices to prove Fermat's conjecture for $n = 4$ and for every prime $p \neq 2$.

The statement of Fermat's Last Theorem is often subdivided further into two cases:

The first case holds for the exponent p when there do not exist integers x,y,z such that $p \nmid xyz$ and $x^p + y^p = z^p$.

The second case holds for the exponent p when there

do not exist integers x,y,z, all different from 0, such that $p|xyz$, $\gcd(x,y,z) = 1$ and $x^p + y^p = z^p$.

If one could find a set of numbers that do not fit into either of the two cases then maybe one could disprove his theorem.

It was already known in antiquity that a sum of two squares of integers may well be the square of another integer. Pythagoras was supposed to have proven that the lengths a,b,c of the sides of a right-angle triangle satisfy the relation

$$a^2 + b^2 = c^2;$$

so the above fact just means the existence of such triangles with sides measured by integers.

But the situation is already very different for cubes, biquadrates and so on. Fermat's proof for the case of biquadrates involved the use of a method for which he is credited for inventing known as "infinite descent." This method of infinite descent is nothing but the well-ordering principle of the natural numbers.

Fermat's Last Theorem aroused the interest of mathematicians and some of the best minds turned to it. Euler considered the case where $n = 3$. He was led to studying odd cubes $a^2 + 3b^2$ (with a,b relatively prime), and forms of their divisors; he concluded the proof by the method of infinite descent.

Gauss gave another proof for the case of cubes. His proof was not "rational" since it involved complex numbers.

This proof was an early incursion into the realm of number fields, i.e., those sets of complex numbers obtained from the roots of polynomials by the operations of addition, subtraction, multiplication, and division.

In 1825, Dirichlet attempted to prove the theorem for the case n = 5. In fact his proof was incomplete, which was pointed out by Legendre, who provided an independent and complete proof. Dirichlet then completed his own proof in 1828.

In Chapter 2, the basic properties of the integers and important theorems needed to solve Fermat's Last Theorem for n = 3 and 4 are discussed. In Chapter 3, the Pythagorean triples and some new ways of finding the Pythagorean triples are covered. Chapter 4 is devoted to proving Fermat's Theorem for n = 3 and 4.

# CHAPTER 2

## BASIC PROPERTIES OF THE INTEGERS

The first three sections of this chapter are devoted to divisibility and prime numbers, as well as to the information about integers that the concept of division can provide. Given any two integers, one can always add, subtract, or multiply them, and again obtain an integer. This is no longer the case with the operation of division. All the sections in this chapter are useful in studying Fermat's Theorems. Let Z denote the set of integers and N denote the set of natural numbers.

### 2.1. Divisibility

Definition 2.1.1. If a and b are in Z and $a \neq 0$, then a divides b means that there is an integer c such that $b = ac$. We write this as $a|b$.

If $a|b$ we say that a is a factor of b or that b is a multiple of a. As an example, $3|6$, because $6 = 3 \cdot 2$. If a does not divide b, we write $a \nmid b$. As an example, $2 \nmid 3$, since there is no integer which when multiplied by 2 gives 3. It is true that $c = 3/2$ makes the statement $3 = 2c$ true, but 3/2 is not an integer.

The following theorem follows from the definition of divisibility.

Theorem 2.1.2

(1) $a|a$ for any $a \neq 0$ in Z.

(2) If $a|b$ and $b|a$, then $b = \pm a$.

(3) If $a|b$, then $a|bc$ for any c in Z.

(4) If $a|b$ and $b|c$, then $a|c$.

(5) If $a|b$ and a,b are both positive, then $a \leq b$.

(6) If $d|a$ and $d|b$, then $d|(ax + by)$ for any pair of integers x and y. In particular, $d|0$ for any nonzero integer d.

Lemma 2.1.3. If $u, v_1, v_2, \ldots, v_n$ are in Z and $u|v_1$, $u|v_2, \ldots, u|v_n$, then $u|(v_1 + v_2 + \ldots + v_n)$.

Proof: Let $c_i$ be an integer such that $v_i = uc_i$, for each $i = 1,2, \ldots n$. Thus $v_1 = uc_1$, $v_2 = uc_2$, $\ldots$, $v_n = uc_n$. Hence, $(v_1 + v_2 + \ldots v_n) = (uc_1) + (uc_2) + \ldots + (uc_n)$

$$= u(c_1 + \ldots + c_n).$$

Since $c_1 + c_2 + \ldots + c_n$ is an integer,

$c = c_1 + c_2 + \ldots + c_n$, and $(v_1 + v_2 + \ldots + v_n) = uc$, therefore $u|(v_1 + v_2 + \ldots + v_n)$. Q.E.D.

Definition 2.1.4.(Greatest Common Divisor). Let a and b be integers; the natural number d is called the greatest common divisor(GCD) of a and b if d satisfies the following two conditions:

(i) $d|a$ and $d|b$.

(ii) If $c \in N$ such that $c|a$ and $c|b$, then $c \leq d$.

Write this as $(a,b) = d$.

Define $(a,0) = |a|$, where $|x|$ denotes the absolute

value of a real number x. Note that (a,b) = (b,a) = (-a,b).

## 2.2. The Division Algorithm

Theorem 2.2.1.(The Division Algorithm). Given n and d in Z with $d \geq 1$, there are unique integers q and r with $0 \leq r < d$ such that $n = qd + r$. In particular, $d|n$ if and only if $r = 0$.

Proof: Because the real line $\mathbb{R}$ is the disjoint union of the semiclosed intervals

$$I_j = [jd,(j + 1)d) = \{x \in \mathbb{R} | jd \leq x < (j + 1)d\},$$

where $j = 0, \pm 1, \pm 2, \ldots$, the integer n is in a unique interval $I_q$. Since each interval $I_j$ is of length d, $0 \leq n - qd = r < d$.

Q.E.D.

Note that integers $q_1$ and $r_1$ exist such that $n = q_1d + r_1$ where $|r_1| \leq \frac{d}{2}$. Indeed, if $0 \leq r \leq \frac{d}{2}$ above, then $q_1 = q$ and $r_1 = r$.

However, if $\frac{d}{2} < r < d$, let $r_1 = r - d$ and $q_1 = q + 1$. Hence,

$n = qd + r = qd + d - d + r = (q + 1)d + (r - d) = q_1d + r_1$ where $-\frac{d}{2} < r_1 < 0$.

Lemma 2.2.2. If $\alpha > 2$, then $\frac{3\alpha^2}{4} > 3$.

Proof: If $\alpha > 2$, then $\alpha^2 > 4$ and $3\alpha^2 > 12$. Thus $\frac{3\alpha^2}{4} > 3$.

Q.E.D.

## 2.3. Primes

If x and y are both even or both odd, then x and y is said to have the same parity. Note, x and y have the same parity if and only if x + y is even. Also x and $x^n$ have the same parity. If a is odd, then x and ax have the same parity.

Given integers a and b, it may or may not happen that a|b. Of course, if a = ±1 or a = ± b, then a automatically divides b. It is a fact, moreover that for some choices of b these will be the only possible divisors of b. For example, if b = 5, then the only divisors of b are 1, -1, 5, -5. Numbers such as 5 play a central role in what is to follow.

Definition 2.3.1. An integer p ≥ 2 is called a prime number or simply a prime if and only if ±1 and ± p are the only divisors of p.

Definition 2.3.2. Two integers u and v are relatively prime if and only if (u,v) = 1.

Definition 2.3.3. x,y,z, are pairwise relatively prime if and only if (x,y) = (x,z) = (y,z) = 1.

Prime numbers are very important because every integer greater than 1 is a product of prime numbers. Consider for example 420 = 42 x 10 and 42 = 7 x 6 while 10 = 2 x 5, so that 420 = 7 x 6 x 2 x 5. Now each of 7, 2, and 5 is a prime number. However, 6 = 2 x 3, giving us 420 = 7 x 2 x 3 x 2 x 5, and now each factor is a prime number and 420 has been shown to be a product of primes.

Theorem 2.3.4 (Fundamental Theorem of Arithmetic). Every integer greater than 1 can be expressed as a product of prime numbers (see [2]).

Definition 2.3.5. For an integer $n > 1$, a product of primes $p_1p_2...p_k$ is a prime factorization of n if and only if:

(1) $n = p_1p_2...p_k$ and

(2) $p_1 \leq p_2 \leq ... \leq p_k$.

Lemma 2.3.6. Let p be a prime number and let n be any integer. If $p|n$, then $(n,p) = p$. If $p\nmid n$, then $(n,p) = 1$.

Proof: If $p|n$, then p is a common divisor of n and p, and is clearly the largest such common divisor. Now suppose that $p\nmid n$ and let $d = (n,p)$. Since $d|p$, then $d = 1$ or $d = p$. However, $d|n$ and $p\nmid n$, therefore $d \neq p$. Thus, $d = 1$. Q.E.D.

Theorem 2.3.7. Let p be a prime number. If $p|ab$, then either $p|a$ or $p|b$.

Proof: Since $p|ab$, then p must appear in the prime factorization of ab. If $p|a$, we are done. If $p\nmid a$, then by Lemma 2.3.6, $(a,p) = 1$. Since the prime p must appear in the factorization of either a or b, $p|b$. Q.E.D.

Corollary 2.3.8. Let p be a prime number and $a_1,a_2,...,a_n$ be integers. If $p|a_1a_2...a_n$, then $p|a_i$ for some $1 \leq i \leq n$.

Theorem 2.3.9. If n is any integer greater than 1, then there is exactly one prime factorization for n (see [2]).

Theorem 2.3.10. Let p be a prime and n a positive integer such that $p^n|rs$ where $(r,s) = 1$. Then either $p^n|r$ or $p^n|s$.

Proof: Using induction on n, the case $n = 1$ is

Theorem 2.3.7. Assume the proposition is true for n. If $p^{n+1}|rs$ where $(r,s) = 1$ and $n \geq 1$, then $rs = ap^{n+1} = app^n$. Thus, $p^n|rs$ and by our assumption $p^n|r$ or $p^n|s$. If $p^n|r$, then $r = p^n r_1$. Thus, $ap^{n+1} = rs = p^n r_1 s$. Also $(r,s) = 1$ and $p|r$, then $p \nmid s$. Now $ap = r_1 s$, thus $p|r_1 s$. Hence, $p|r_1$ or $p|s$. But $p \nmid s$, thus $r_1 = pr_2$. Therefore, $r = p^n r_1 = p^n pr_2 = p^{n+1} r_2$. Consequently, $p^{n+1}|r$. The case $p^n|s$ is similar. Q.E.D.

Proposition 2.3.11. For a fixed n, if $a^n = rs$ where $r,s > 0$ and $(r,s) = 1$, then there exist b and c such that $r = b^n$ and $s = c^n$.

Proof: Let P(a,r,s) be the statement of the proposition and $S = \{|a| \mid$ there exist r and s such that P(a,r,s) is false$\}$. Note, if $1^n = rs$ with $r,s > 0$, then $r = s = 1 = 1^n$. Hence, $1 \notin S$. Assume, $S \neq \emptyset$. Since $S \subset N$, then S contains a minimum element w. Thus, there exist a,r,s such that $|a| = w$, $r,s > 0$, $(r,s) = 1$, and $a^n = rs$ where either r is not a perfect $n^{th}$ power or s is not a perfect $n^{th}$ power. Since $|a| > 1$, let p be any prime dividing a. Thus, $a = pa_1$, and so $p^n a_1^n = a^n = rs$, hence $p^n|rs$. Since p is prime and $(r,s) = 1$, then either $p^n$ divides r or $p^n$ divides s. Without loss of generality, assume $p^n|r$. Thus, $r = p^n r_1$. Note $1 = (r,s) = (p^n r_1 s,)$ implies $(r_1,s) = 1$. Consequently, $p^n a_1^n = rs = p^n r_1 s$, and so $a_1^n = r_1 s$. Since $a = p^n a_1$, then $|a_1| < |a| = w$ and so $|a_1| \notin S$. Thus $r_1$ and s are perfect $n^{th}$ powers, $r_1 = b^n$ and $s = c^n$. Thus, $r = p^n b^n = (pb)^n$ and $s = c^n$ which contradicts the fact that either r or s is not a perfect $n^{th}$ power. Therefore, $S = \emptyset$ which proves the proposition. Q.E.D.

## 2.4 Congruence

One of the beauties of mathematics is that many times a seemingly simple idea can have far-reaching effects. For example, show that the equation

$$x^9 + x^5 = 3,226,583,002,173,942,667,832,111$$

has no integer solutions.

A trial-and-error attack would be quite lengthy even with a computer. However, reasoning may be used. Every integer is either even or odd. Also the sum of two even integers is even and the sum of two odd integers is even. There are two cases. Either x is even or x is odd. If x is an even integer, then $x^9$ is even, as is $x^5$. Thus $x^9 + x^5$ will be even. But the number on the right-hand side is odd. Therefore, no even integer can be a solution of the equation. What if x is any odd integer? In this case $x^9$ and $x^5$ would both be odd integers. Thus, their sum would be even. Therefore, there can be no integer solution to the equation. This concept is the focus of this section.

Definition 2.4.1. Let $m > 1$ be a fixed integer, called the modulus, and let $a,b \in Z$. We say that a is congruent to b modulo m, written as $a \equiv b \bmod m$, if and only if $m|(a - b)$.

Theorem 2.4.2. Let $m > 1$ be an positive integer.

(1) For any integer a, $a \equiv a \bmod m$.

(2) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a + c \equiv b + d \bmod m$.

(3) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $ac \equiv bd \bmod m$.

(4) If $c \equiv d \bmod m$, then $-c \equiv -d \bmod m$.

(5) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a - b \equiv c - d \bmod m$.

(6) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$.

(7) If $a \equiv b \bmod m$, then $b \equiv a \bmod m$.

Proof:

(1) For any integer a, $a - a = 0$ and $m|0$. Thus, $a \equiv a \bmod m$.

(2) $a \equiv b \bmod m$ means that $m|(a-b)$; $c \equiv d \bmod m$ means that $m|(c - d)$. By Lemma 2.1.3, $m|[(a - b) + (c - d)]$. However,

$(a - b) + (c - d) = (a + c) - (b + d)$, so $m|[(a + c) - (b + d)]$. Thus, $a + c \equiv b + d \bmod m$.

(3) Since $m|(a - b)$, $m|(c - d)$, and $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$, then $m|(ac - bd)$ by Theorem 2.1.2 (6).

(4) This is a consequence of (1) and (3), since $-1 \equiv -1 \bmod m$, $-c = -1 \cdot c$, and $-d = -1 \cdot d$.

(5) This follows from (2) and (4).

(6) If $m|(a - b)$ and $m|(b - c)$, then $m|[(a - b) + (b - c)] = a - c$. Thus, $a \equiv c \bmod m$.

(7) If $a \equiv b \bmod m$, then $m|(a - b)$. Therefore, $m|-(a-b) = b - a$ and so $b \equiv a \bmod m$. Q.E.D.

Theorem 2.4.3. Let a and b be integers.

(a) If $(a,b) = d$, then there exist integers u and v such that $ua + vb = d$.

(b) $(a,b) = 1$ if and only if $1 = ua + vb$ for some

integers u and v.

(c) If $(a,b) = d$ where $a = da_1$ and $b = db_1$, then $(a_1,b_1) = 1$.

Proof: (a) Let $S = \{d_1 = (u_1a + v_1b) | u_1, v_1 \in Z \text{ and } d_1 > 0\}$. Thus, $S \subset N$. Furthermore, since $a = 1 \cdot a + 0 \cdot b$ and $-a = -1 \cdot a + 0 \cdot b$, then either $a \in S$ or $-a \in S$ depending on the sign of a. Therefore, $S \neq \emptyset$ and so S contains a minimum number $d = ua + vb$. Thus, $d > 0$ and $p|d$ whenever $p|a$ and $p|b$. Assume d does not divide a. Using the Division Algorithm we can write $a = td + r$ where $0 < r < d$. Thus,

$$\begin{aligned} r &= a - td \\ &= a - t(ua + vb) \\ &= (1 - tu)a + (-tv)b. \end{aligned}$$

Since $r > 0$, then $r \in S$. This contradicts the fact that d is the minimal number in S. Hence $d|a$, and $d|b$ by a similar argument. Therefore, $d > 0$, $d|a$, $d|b$ and $p|d$ whenever $p|a$ and $p|b$. This proves $(a,b) = d$.

(b) If $(a,b) = 1$, then $1 = ua + vb$ by part (a) of this theorem. Conversely, if $1 = ua + vb$, then any number dividing both a and b would have to divide 1. Thus, $(a,b) = 1$.

(c) Assume $(a,b) = d$, $a = a_1d$ and $b = b_1d$. Then for some u and v, $d = ua + vb$, $= ua_1d + vb_1d = (ua_1 + vb_1)d$. Hence, $1 = ua_1 + vb_1$, which proves $(a_1,b_1) = 1$. Q.E.D.

Theorem 2.4.4. If $(m,n) = 1$ and $m|nk$, then $m|k$.

Proof: If $(m,n) = 1$ and $m|nk$, then there exist integers a,b and r such that $am + bn = 1$ and $rm = nk$. Thus,

$k = k \cdot 1 = k(am + bn) = kam + bkn = kam + brm = (ka + br)m$,

which proves $m|k$. Q.E.D.

Theorem 2.4.5. Let $m > 1$ and suppose that $ab \equiv ac \bmod m$. If $(a,m) = 1$, then $b \equiv c \bmod m$.

Proof: We have $ab \equiv ac \bmod m$, so that $m|(ab - ac)$. But $ab - ac = a(b - c)$ and $(a,m) = 1$, therefore by 2.4.4, we have $m|(b - c)$. Hence, $b \equiv c \bmod m$. Q.E.D.

## 2.5 Sums of Two Squares

The goal in this section is to determine those integers n for which there exist integral solutions to the equation $X^2 + Y^2 = n$.

One of the first topics in number theory that Fermat studied, and one that led him to many other important questions, was the problem of representing numbers as sums of two squares.

A basic fact in the study of numbers that are sums of two squares is the formula

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

which shows that if two numbers are sums of two squares then their product is also a sum of two squares.

Theorem 2.5.1. If X and Y are the sums of two squares, then so is $X \cdot Y$.

Proof: Let X and Y be the sum of two squares such that $X = (a^2 + b^2)$ and $Y = (c^2 + d^2)$.

Then,

$$XY = (a^2 + b^2)(c^2 + d^2)$$
$$= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2.$$

But

$$(ac - bd)^2 + (ad + bc)^2 = -2acbd + a^2c^2 + b^2d^2 + 2acbd + a^2d^2 + b^2c^2$$

$$= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$$

$$= XY.$$

Then,

$$(ac - bd)^2 + (ad + bc)^2 = XY.$$

Therefore,

$$(a^2 + b^2)(c^2 + d) = (ac - bd)^2 + (ad + bc)^2.$$

Q.E.D.

Example: This result can be applied in two different ways to $5 = 2^2 + 1^2$ and $13 = 3^2 + 2^2$.

Thus,

$$65 = 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2)$$

$$= (2 \cdot 3 - 1 \cdot 2)^2 + (2 \cdot 2 + 1 \cdot 3)^2$$

$$= 4^2 + 7^2$$

and

$$65 = 5 \cdot 13 = (2^2 + 1^2)(2^2 + 3^2)$$

$$= (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2$$

$$= 1^2 + 8^2.$$

## 2.6 Properties of Integers

This section presents some deeper properties of integers needed in Chapter 3 to prove Fermat's Theorem for the case $n = 3$.

Theorem 2.6.1. Let $m > 2$ and $m$ be odd. Then the congruence $N^2 \equiv -3 \bmod m$ has a solution if and only if there exist $x$ and $y$ such that

(1) $x^2 + 3y^2 = m$ and

(2) $(x,y) = 1$.

Proof: Assume $x$ and $y$ exist and $(x,y) = 1$. Since $x^2 = m - 3y^2$ then any prime factor of $y$ and $m$ would also be a factor of $x$. Hence, $(x,y) = 1$ implies $(y,m) = 1$. Thus, there exists $r$ and $s$ such that $ry + sm = 1$. Therefore, $x = rxy + sxm = Ny + cm$. Hence,

$$x^2 = N^2y^2 + 2cNym + c^2m^2 = N^2y^2 + dm.$$

Consequently,

$$\begin{aligned} y^2(N^2 + 3) &= y^2N^2 + 3y^2 \\ &= N^2y^2 + m - x^2 \\ &= m - dm \\ &= m(1 - d). \end{aligned}$$

Thus, $m \mid y^2(N^2 + 3)$. But $(m,y) = 1$, then $m$ divides $N^2 + 3$. Therefore, $N^2 \equiv -3 \bmod m$.

Conversely, assume $N^2 \equiv -3 \bmod m$ has a solution. Now find $N$ such that $N^2 \equiv -3 \bmod m$ and $|N| \leq \frac{m}{2}$. To see this, observe if $N^2 \equiv -3 \bmod m$, then $(N + km)^2 \equiv -3 \bmod m$ because

$$\begin{aligned} (N + km)^2 + 3 &= N^2 + 2knm + km^2 + 3 \\ &= sm + 2kNm + km^2 \text{ (since } m \mid N^2 + 3) \\ &= (s + 2kN + km)m. \end{aligned}$$

Thus, an integer k can be found such that $-\frac{m}{2} \leq N + km \leq \frac{m}{2}$, and

$(N + km)^2 \equiv -3 \bmod m$. Thus, assume $N^2 \leq \frac{m^2}{4}$. It can be proven

by induction that there exist integers

$m_1, m_2, \ldots, m_{k+1}$ and $N_1, N_2, \ldots, N_k$ satisfying:

(1) $m_1 > m_2 > \ldots > m_k > m_{k+1}$,

(2) $m_{k+1} = 1$ or 2

(3) $N_i^2 + 3 = m_i \cdot m_{i+1}$ (therefore $N_i^2 \equiv -3 \bmod m_{i+1}$)

(4) $N_{i-1} \equiv N_i \bmod m_i$.

Set $m_1 = m$ and $N_1 = N$. Thus, $N_1^2 \equiv -3 \bmod m_1$ and so

there exists $m_2$ such that $N_1^2 + 3 = m_1 m_2$. Since $m_1 = m > 2$,

then $m_2 > 0$. Now $m_1 m_2 = N^2 + 3 \leq \frac{m^2}{4} + 3 < \frac{m^2}{4} + \frac{3m^2}{4}$ by

Lemma 2.2.2, since $m > 2$. Therefore, $m_1 m_2 < m^2 = m_1^2$, which

implies $m_2 < m_1$. Furthermore, there exists a and $N_2$ such that $N_1$

$= am_2 + N_2$ and $|N_2| \leq \frac{m_2}{2}$ (see the note following Theorem 2.2.1.).

Observe $N_1 \equiv N_2 \bmod m_2$.

Assume $m_1 > m_2 > \ldots > m_n > 0$ and $N_1, N_2, \ldots, N_{n-1}$ for $n \geq 2$

have been defined. If $m_n = 1$ or 2, then set $k + 1 = n$ and the

proof is complete. Otherwise $m_n > 2$. Now there exist $N_n$ such

that $N_{n-1} = am_n + N_n$ and $|N_n| \leq \frac{m_n}{2}$. Therefore, $N_{n-1} \equiv N_n \bmod m_n$.

Therefore, $N_n^2 \equiv N_{n-1}^2 \equiv -3 \bmod m_n$. So, there exists $m_{n+1}$ such that $N_n^2 + 3 = m_n m_{n+1}$. Since $m_n > 0$, then $m_{n+1} > 0$. Finally,

$m_n m_{n+1} = N_n^2 + 3 < \frac{m_n^2}{4} + \frac{3m_n^2}{4}$, which implies $m_n\, m_{n+1} < m_n^2$.

Therefore, $m_{n+1} < m_n$. Since $m_{i+1} < m_i$ are positive integers, then, $m_{i+1} \leq m_i - 1$. After a finite number of steps we arrive at $m_n \leq 2$. Then, set $k + 1 = n$. This completes the inductive proof.

For each $n \leq k$, $N_{n-1} \equiv N_n \bmod m_n$. Let $\gamma_n$ be such that $N_{n-1} = N_n + \gamma_n m_n$. Set $\lambda = m_{k+1}$, then $\lambda = 1$ or 2. Next show there exist $z_k, y_k$; $z_{k-1}, y_{k-1}$; ...; $z_1, y_1$ such that for every (z y in each pair) n, $\lambda m_n = (m_n z_n + N_n y_n)^2 + 3\, y_n^2$ and $(y_n, z_n) = 1$. (*)
Hence, $N_k^2 + 3 = m_k m_{k+1} = \lambda m_k$. Thus, set $z_k = 0$ and $y_k = 1$.
Therefore, $(m_k z_k + N_k y_k)^2 + 3y_k^2 = N_k^2 + 3 = \lambda m_k$. Assume, $(z_k, y_k; \ldots z_n, y_n)$ satisfying(*) have been found. Let $z_{n-1} = y_n$ and $y_{n-1} = z_n - \gamma_n y_n$. Therefore, $z_n = y_{n-1} + \gamma_n y_n = y_{n-1} + \gamma_n z_{n-1}$. Since $(y_n, z_n) = 1$ then $(y_{n-1}, z_{n-1}) = 1$.
Now

$$\begin{aligned}
\lambda m_n &= (m_n z_n + N_n y_n)^2 + 3y_n^2 \\
&= [m_n(y_{n-1} + \gamma_n z_{n-1}) + N_n z_{n-1}]^2 + 3z_{n-1}^2 \\
&= [m_n y_{n-1} + (m_n \gamma_n + N_n)\, z_{n-1}]^2 + 3z_{n-1}^2 \\
&= [m_n y_{n-1} + N_{n-1}\, z_{n-1}]^2 + 3z_{n-1}^2 \\
&= m_n^2 y_{n-1}^2 + 2y_{n-1}\, N_{n-1}\, z_{n-1}\, m_n + (N_{n-1}^2 + 3) z_{n-1}^2 \\
&= (m_n y_{n-1}^2 + 2y_{n-1}\, N_{n-1}\, z_{n-1})\, m_n + m_{n-1}\, m_n z_{n-1}^2.
\end{aligned}$$

Therefore $\lambda = m_n y_{n-1}^2 + 2y_{n-1}\, N_{n-1}\, z_{n-1} + m_{n-1}\, z_{n-1}^2$.
However, $m_n m_{n-1} = N_{n-1}^2 + 3$, therefore

$$\lambda m_{n-1} = m_n m_{n-1} y^2_{n-1} + 2y_{n-1} N_{n-1} z_{n-1} m_{n-1} + m^2_{n-1} z^2_{n-1}$$
$$= (N^2_{n-1} + 3) y^2_{n-1} + 2y_{n-1} N_{n-1} z_{n-1} m_{n-1} + m^2_{n-1} z^2_{n-1}$$
$$= N^2_{n-1} y^2_{n-1} + 2y_{n-1} N_{n-1} z_{n-1} m_{n-1} + m^2_{n-1} z^2_{n-1} + 3y^2_{n-1}.$$

So $\lambda m_{n-1} = (m_{n-1} z_{n-1} + N_{n-1} y_{n-1})^2 + 3y^2_{n-1}$.

This completes the induction step.

For n = 1 we have $(mz_1 + Ny_1)^2 + 3y_1^2 = \lambda m$. Let $x = mz_1 + Ny_1$ and $y = y_1$. Then $x^2 + 3y^2 = \lambda m$ with $\lambda = 1$ or 2. Also $(y_1, z_1) = 1$. Recall m is odd, thus $4 \nmid 2m$. Assume $\lambda = 2$. Then, $x^2 + 3y^2 = 2m$ is even, hence x and y have the same parity. If x and y are even, then $4 | (x^2 + 3y^2)$, a contradiction. If $x = 2n + 1$, $y = 2k + 1$ are odd then $x^2 + 3y^2 = 4n^2 + 4n + 1 + 12k^2 + 12k + 3$, which is also divisible by 4. Thus, we have a contradiction in either case. Therefore, $\lambda = 1$ and $x^2 + 3y^2 = m$. Let $p = (x,y)$, whence p divides x and y. Hence, p divides m. Thus,

$$m = x^2 + 3y^2 = (mz_1 + Ny)^2 + 3y^2$$
$$= m^2 z_1^2 + 2Nz_1 ym + (N^2 + 3)y^2$$
$$= m^2 z_1^2 + 2Nz_1 ym + mm_2 y^2.$$

Therefore $1 = z_1^2 m + 2Nz_1 y + m_2 y^2$.

Since p divides m and y, then p divides 1. Therefore, $p = 1 = (x,y)$. Q.E.D.

<u>Proposition 2.6.2.</u> Assume $x^2 + 3y^2 = m$ where $(x,y) = 1$. Then, there exist N such that $N^2 \equiv -3 \bmod m$ and $x \equiv Ny \bmod m$.

<u>Proof:</u> Since $(x,y) = 1$ then $(y,m) = 1$. Thus, there exist r and s such that $1 = ry + sm$. Whence, $x = rxy + sxm = Ny + cm$. Therefore, $x \equiv Ny \bmod m$. Also,

$$m = x^2 + 3y^2 = N^2y^2 + 2Nycm + c^2m^2 + 3y^2.$$

Thus, $m = (N^2 + 3)\,y^2 + dm$. Therefore, m divides $y^2(N^2 + 3)$. Since $(m,y) = 1$, then $N^2 \equiv -3 \bmod m$ by Theorem 2.4.4. Q.E.D.

Proposition 2.6.3. For $m > 2$, m = odd, if $N_1$ is any solution to $N^2 \equiv -3 \bmod m$, then there exist x and y such that $(x,y) = 1$, $x^2 + 3y^2 = m$, and $x \equiv N_1y \bmod m$.

Proof: In the proof of 2.6.1 above we replaced $N_1$ with $N = N_1 + km$ such that $|N| \leq \frac{m}{2}$. Since $x = Ny + mz_1$ in this proof then $x = N_1y + ykm + z_1m \equiv N_1y + dm$. Therefore, $x \equiv N_1y \bmod m$. Q.E.D.

If $A = x + y\sqrt{-3}$, $x,y \in J$, then define $\overline{A} = x - y\sqrt{-3}$.

*Define* $h(x + y\sqrt{-3}) = x^2 + 3y^2$.

Theorem 2.6.4.

(1) $h(A) = A\cdot\overline{A}$

(2) $h(\overline{A}) = h(A)$

(3) $\overline{(A\cdot B)} = \overline{A}\cdot\overline{B}$

(4) $h(A\cdot B) = h(A)\cdot h(B)$

(5) $h(A^n) = (h(A))^n$, $n = 1,2,3,\ldots$

Proof: (1) *Let* $A = x + y\sqrt{-3}$, *then*

$$\begin{aligned} A\cdot\overline{A} &= (x + y\sqrt{-3})(x - y\sqrt{-3}) \\ &= x^2 - (y\sqrt{-3})^2 \\ &= x^2 + 3y^2 \\ &= h(A). \end{aligned}$$

(2) $h(\overline{A}) = h(x - y\sqrt{-3}) = x^2 + 3(-y)^2 = x^2 + 3y^2 = h(A)$.

(3) Let $A = x + y\sqrt{-3}$ and $B = w + u\sqrt{-3}$. Then, $A \cdot B =$

$(x + y\sqrt{-3}) \cdot (w + u\sqrt{-3}) = (xw - 3yu) + (xu + yw)\sqrt{-3}$, *thus* $\overline{A \cdot B} =$

$\overline{(x + y\sqrt{-3}) \cdot (w + u\sqrt{-3})} = (xw - 3yu) - (xu + yw)\sqrt{-3}$.

$\overline{A} \cdot \overline{B} =$

$$\overline{(x + y\sqrt{-3})} \cdot \overline{w + u\sqrt{-3}} = (x - y\sqrt{-3})(w - u\sqrt{-3})$$
$$= (xw - 3yu) + (-xu - yw)\sqrt{-3}$$
$$= \overline{(x + y\sqrt{-3}) \cdot (u + w\sqrt{-3})}.$$

Hence, $\overline{A \cdot B} = \overline{A} \cdot \overline{B}$.

(4)

$$h(A \cdot B) = A \cdot B \cdot \overline{A \cdot B} + A \cdot B \cdot \overline{A} \cdot \overline{B}$$
$$= A \cdot \overline{A} \cdot B \cdot \overline{B}$$
$$= h(A) \cdot h(B).$$

(5) Fact (4) can be used to prove (5) by induction on n. Q.E.D.

Theorem 2.6.5. Let $\beta > 2$, be an odd integer. If $x^2 + 3y^2 = \beta^3$ has a solution with $(x,y) = 1$, then there exist $r_1, s_1$, such that (1) $(r_1, s_1) = 1$ and (2) $(x + y\sqrt{-3}) = (r_1 + s_1\sqrt{-3})^3$.

Proof: Since $x^2 + 3y^2 = \beta^3$ with $(x,y) = 1$, $\beta^3 > 2$ an odd

integer, then there exists a solution to the congruence $N^2 \equiv -3 \mod \beta^3$ (Theorem 2.6.1.). Thus, there exists n such that $N^2 + 3 = n\beta^3 = (n\beta^2)\beta$. Therefore, N is a solution to $N^2 \equiv -3 \mod \beta$. Furthermore, N can be chosen such that $x \equiv Ny \mod \beta^3$ according to Proposition 2.6.2. Since $N^2 \equiv -3 \mod \beta$, there exist r and s with $(r,s) = 1$, $r^2 + 3s^2 = \beta$ and $r \equiv Ns \mod \beta$ by Proposition 2.6.3. Then there exist a,b,c such that

$$(1)\quad N^2 = -3 + a\beta^3$$

$$(2)\quad x = Ny + b\beta^3$$

and

$$(3)\quad r = Ns + c\beta.$$

Consider

$$(r - s\sqrt{-3})^3 = r^3 - 3r^2 s\sqrt{-3} - 9rs^2 + 3s^3\sqrt{-3}$$

$$= P - Q\sqrt{-3},$$

where $P = r^3 - 9rs^2$ and $Q = 3r^2s - 3s^3$.

Now

$$\begin{aligned}(r - sN)^3 &= r^3 - 3r^2sN + 3rs^2N^2 - s^3NN^2\\ &= r^3 - 3r^2 sN + 3rs^2(-3 + a\beta^3) - s^3N(-3 + a\beta^3)\\ &= r^3 - 3r^2sN - 9rs^2 + 3rs^2a\beta^3 + 3s^3N - as^3N\beta^3\\ &= (r^3 - 9rs^2) - (3r^2s - 3s^3)N + d\beta^3.\end{aligned}$$

Therefore $(r - sN)^3 = P - QN + d\beta^3$. But $r - sN = c\beta$, whence $P - QN = (r - sN)^3 - d\beta^3 = (c^3 - d)\beta^3$. Therefore $P \equiv NQ \mod \beta^3$.

Next consider

$$\begin{aligned} P^2 + 3Q^2 &= h(P - Q\sqrt{-3}) \\ &= h((r - s\sqrt{-3})^3) \\ &= h(r - s\sqrt{-3})^3 \\ &= (r^2 + 3s^2)^3 \\ &= \beta^3. \end{aligned}$$

Thus, $P^2 + 3Q^2 = \beta^3$.

Consider $x \equiv Ny \bmod \beta^3$, $N^2 \equiv -3 \bmod \beta^3$ and $P \equiv NQ \bmod \beta^3$.

Therefore, $xP \equiv N^2yQ \equiv -3yQ \bmod \beta^3$. So $xP + 3yQ = m\beta^3$ for some m.

Also $Py \equiv NQy \equiv Qx \bmod \beta^3$. Therefore, $Py - Qx = n\beta^3$ for some n.

Consider:

$$\begin{aligned} \frac{x + y\sqrt{-3}}{P + Q\sqrt{-3}} &= \frac{(x + y\sqrt{-3})(P - Q\sqrt{-3})}{(P + Q\sqrt{-3})(P - Q\sqrt{-3})} \\ &= \frac{(Px + 3Qy) + (Py - xQ)\sqrt{-3}}{P^2 + 3Q^2} \\ &= \frac{m\beta^3 + n\beta^3\sqrt{-3}}{\beta^3} \\ &= m + n\sqrt{-3}. \end{aligned}$$

Therefore, $x + y\sqrt{-3} = (m + n\sqrt{-3})(P + Q\sqrt{-3})$.

Next consider

$$\begin{aligned}\beta^3 &= x^2 + 3y^2 \\ &= h(x + y\sqrt{-3}) \\ &= h((m + n\sqrt{-3})\ (P + Q\sqrt{-3})) \\ &= h(m + n\sqrt{-3})\,h(P + Q\sqrt{-3}) \\ &= (m^2 + 3n^2)\,(P^2 + 3Q^2) \\ &= (m^2 + 3n^2)\,\beta^3.\end{aligned}$$

Thus, $m^2 + 3n^2 = 1$, whence $m = \pm 1$ and $n = 0$. Consequently,

$x + y\sqrt{-3} = (m + n\sqrt{-3})\,(P + Q\sqrt{-3}) = \pm(P + Q\sqrt{-3})$.

But $(r + s\sqrt{-3})^3 = r^3 + 3r^2s\sqrt{-3} - 9rs^2 - 3s^3\sqrt{-3} = P + Q\sqrt{-3}$.

So

$$\begin{aligned}x + y\sqrt{-3} &= \pm(P + Q\sqrt{-3}) \\ &= \pm(r + s\sqrt{-3})^3 \\ &= (r_1 + s_1\sqrt{-3})^3, \text{ where } r_1 = \pm r \text{ and } s_1 = \pm s.\end{aligned}$$

Hence, there exist $r_1$ and $s_1$ such that $(x + y\sqrt{-3}) = (r_1 + s_1\sqrt{-3})^3$.

Since $(r,s) = 1$, then $(r_1,s_1) = 1$. Q.E.D.

# CHAPTER 3

# PYTHAGOREAN TRIPLES

Fermat's Last Theorem was inspired by the proposition in Diophantus' Arithmetic which is one of the oldest problems in mathematics, that is, "to write a square rational number as the sum of two square rational numbers." One solution of this problem is derived from the equation $3^2 + 4^2 = 5^2$, which implies that for any square $a^2$, where a is rational, $a^2 = (3a/5)^2 + (4a/5)^2$. In a similar way, any triple of positive integers x,y,z such that $x^2 + y^2 = z^2$ gives a solution $a^2 = (xa/z)^2 + (ya/z)^2$ and every rational solution arises in this way. In short, Diophantus' problem amounts to the problem of finding triples of positive whole numbers that satisfy $x^2 + y^2 = z^2$.

Any triple of positive integers x,y,z which satisfies $x^2 + y^2 = z^2$ determines a set of ratios x:y:z such that a triangle whose sides are in this ratio is a right triangle. A triple of positive integers that satisfies $x^2 + y^2 = z^2$ is called a Pythagorean triple.

## 3.1 Pythagorean Triples

Definition 3.1.1. A Pythagorean triple is a triple of positive integers (x,y,z) such that $x^2 + y^2 = z^2$. If (x,y,z) is a Pythagorean triple, then each of x and y is said to be a leg of

the triple. Note that $x^2 < x^2 + y^2 = z^2$, hence $x < z$. Similarly $y < z$.

Since $3^2 + 4^2 = 5^2$, then (3,4,5) is a Pythagorean triple whose legs are 3 and 4. Pythagoras is credited with noting that if n is a positive integer, then $(2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$ is a pythagorean triple. This can be proved by direct calculation; $(2n + 1)^2 + (2n^2 + 2n)^2 = (2n^2 + 2n + 1)^2$.

Theorem 3.1.2. For each integer $x > 2$ there exist integers y and z such that (x,y,z) is a Pythagorean triple.

Proof. Suppose first that x is even. Then $2|x$, so $4|x^2$; hence $(x^2 - 4)/4$ and $(x^2 + 4)/4$ are both integers. If $y = (x^2 - 4)/4$ and $z = (x^2 + 4)/4$, then (x,y,z) is a Pythagorean triple. If x is odd, then $x = 2n + 1$ and by Pythagoras' observation, $(2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$ is a Pythagorean triple. Q.E.D.

Definition 3.1.3. The Pythagorean triple (x,y,z) is said to be primitive if $(x,y) = 1$.

Lemma 3.1.4. Suppose that (x,y,z) is a Pythagorean triple and let $d = (x,y)$. Then $d|z$. Furthermore, if a,b, and c are integers such that $x = ad$, $y = bd$, and $z = cd$, then (a,b,c) is a primitive Pythagorean triple.

Proof: If d divides x and y, then $d^2$ divides $x^2$ and $y^2$ and, therefore, $d^2$ divides $x^2 + y^2 = z^2$. Hence, d divides z. Since $x^2 + y^2 = z^2$, then $a^2d^2 + b^2d^2 = c^2d^2$. Consequently, $a^2 + b^2 = c^2$. Furthermore, $(a,b) = 1$ by Theorem 2.4.3. Q.E.D.

This lemma says that each Pythagorean triple (x,y,z) is the

dth multiple of the primitive Pythagorean triple (a,b,c) obtained by dividing each of x,y,z by d = (x,y). Thus, once all primitive Pythagorean triples are known, then all Pythagorean triples are known. Note that if (a,b,c) is a primitive Pythagorean triple, then a,b and c are relatively prime in pairs. To see this, assume $a^2 + b^2 = c^2$ where (a,b) = 1. If p is a prime that divides b and c, then p divides $a^2$ and so p divides a. But this contradicts (a,b) = 1. Thus, (b,c) = 1. Similarly (a,c) = 1.

Lemma 3.1.5. If (a,b,c) is a primitive Pythagorean triple, then c is odd and $a \not\equiv b \bmod 2$.

Proof: If $a \equiv b \bmod 2$, then a and b are both even or both odd. If a and b are both even, then $2 \mid (a,b)$, contrary to (a,b,c) being primitive. If a and b are both odd, then $c^2 = a^2 + b^2$ is even: hence c is even. Write a = 2k + 1, b = 2n + 1, and c = 2m. Then,

$$a^2 = 4k^2 + 4k + 1 \equiv 1 \bmod 4$$

$$b^2 = 4n^2 + 4n + 1 \equiv 1 \bmod 4$$

$$c^2 = 4m^2 \equiv 0 \bmod 4,$$

so

$$a^2 + b^2 \equiv 2 \bmod 4.$$

But $c^2 = a^2 + b^2$, so $0 \equiv 2 \bmod 4$, a contradiction. Thus, $a \not\equiv b \bmod 2$. Since $a^2 + b^2 = c^2$ and exactly one of a or b is odd, $c^2$ must be odd and so c is odd. Hence, if (a,b,c) is a primitive Pythagorean triple, we may assume a is even and b is odd without loss of generality. Q.E.D.

Theorem 3.1.6. Let a,b, and c be positive integers with a

even. Then (a,b,c) is a primitive Pythagorean triple if and only if there exist integers x and y such that

1. $x > y > 0$,

2. $x \not\equiv y \bmod 2$,

3. $(x,y) = 1$, and

4. $a = 2xy$, $b = x^2 - y^2$, and $c = x^2 + y^2$.

Proof: Assume such x and y exist. Then condition (1) guarantees that $a > 0$, $b > 0$ and $c > 0$. Also

$$\begin{aligned} a^2 + b^2 &= 4x^2y^2 + x^4 - 2x^2y^2 + y^4 \\ &= x^4 + 2x^2y^2 + y^4 \\ &= c^2. \end{aligned}$$

Since x and y have opposite parity from (2), then $b = x^2 - y^2$ is odd, thus 2 is not a common factor of a and b. If p is an odd prime that divides a and b, then $p \mid 2xy$, $p \neq 2$. Hence, $p \mid x$ or $p \mid y$. But if $p \mid b$ and $p \mid x$, then $p \mid (y^2 = x^2 - b)$. Thus $p \mid y$. Similarly, if $p \mid y$ then $p \mid x$. Therefore, p divides x and y which contradicts (3). Thus, $(a,b) = 1$ which implies (a,b,c) is a primitive Pythagorean triple.

Conversely, assume that (a,b,c) is a primitive Pythagorean triple. By Lemma 3.1.5. we may assume that a is even. Suppose that $[(c + b)/a] = x/y$ with x/y in lowest terms and $y > 0$. Since $c > a > 0$, then $x/y = \frac{(c + b)}{a} > 1$. Thus, x and y satisfy (1) and (3). Now there is a $k \in J$ such that $c + b = kx$ and $a = ky$. Furthermore,

$[(c + b)/a][(c - b)/a] = \frac{c^2 - b^2}{a^2} = 1$, so that $[(c - b)/a] = y/x$.

Hence, there is a $t \in J$ with $c - b = ty$ and $a = tx$. Since $tx = a = ky$, then $x|ky$. Since $(x,y) = 1$, then $x|k$. Thus, $k = mx$ for some integer m. Therefore, $tx = ky = mxy$, which implies $t = my$. From $c + b = kx = mx^2$ and $c - b = ty = my^2$, by adding and subtracting these equations we get $c = m(x^2 + y^2)/2$ and $b = m(x^2 - y^2)/2$. If $x \equiv y \bmod 2$, then x and y are both odd because $(x,y) = 1$. Thus, $x^2 + y^2$ and $x^2 - y^2$ are even, thus m must divide b and c. But $(c,b) = 1$, so $m = 1$. Hence, $a = ky = mxy = xy$ where a is even, and x and y are both odd, a contradiction. Consequently, (2) holds. Thus, $c = m(x^2 + y^2)/2$ and $b = m(x^2 - y^2)/2$ where $x^2 + y^2$ and $x^2 - y^2$ are odd. Thus, m is even and, in fact, m/2 must divide both a and b. Since $(a,b) = 1$, then $m = 2$. Hence $a = mxy = 2xy$, $b = (x^2 - y^2)$, and $c = (x^2 + y^2)$. Therefore (4) holds. Q.E.D.

## 3.2 Current Results

The constructions given in Theorem 3.1.6 do not provide all Pythagorean triples. However, Andrea Rothbart and Bruce Paulsell developed a theorem in 1974 that will provide all Pythagorean Triples. This theorem appeared in the article "Pythagorean Triples: A New, Easy-to-Derive Formula with Some Geometric Applications," which appeared in Mathematics Teacher, Vol.67 (March, 1974), pp 215-218.

Theorem 3.2.1. A triple (x,y,z) is a Pythagorean triple if and only if there exist integers u and v which satisfy the

following conditions:

(i) $u > v > 0$,

(ii) $u \equiv v \bmod 2$, (a simple way of saying that u and v are both even or both odd)

(iii) uv is a perfect square,

(iv) $x = \sqrt{uv}$, $y = (u - v)/2$, $z = (u + v)/2$.

Proof: First suppose that u and v satisfy conditions (i) through (iv). Then (i) and (iv) imply that x,y, and z are positive. Also, (iii) and (iv) yield that x is an integer, while (ii) and (iv) yield that y and z are integers. Finally, from (iv),

$$x^2 + y^2 = (\sqrt{uv})^2 + \left[\frac{(u - v)}{2}\right]^2 = \frac{4uv}{4} + \frac{u^2 - 2uv + v^2}{4}$$

$$= \tfrac{1}{4}(u^2 + 2uv + v^2)$$

$$= [(u + v)/2]^2 = z^2.$$

Thus, (x,y,z) is a Pythagorean triple.

Conversely, assume that (x,y,z) is a Pythagorean triple. Then find integers u and v satisfying the four conditions. Let $u = z + y$ and $v = z - y$. Since y and z are positive and $z > y$, we have $u > v > 0$, so that (i) is satisfied. Also, $u - v = 2y$, so $2 \mid (u - v)$ and condition (ii) holds. Furthermore, $uv = (z + y)(z - y) = z^2 - y^2 = x^2$, so (iii) is satisfied. Finally, because $uv = x^2$, $x = \sqrt{uv}$, while $(u - v)/2 = (2y)/2 = y$ and $(u + v)/2 = 2z/2 = z$, showing that (iv) holds. This

completes the proof. Q.E.D.

Example: Let us find all Pythagorean triples that have 30 as one of their legs. Since (x,30,z) is such a triple, then (30,x,z) is also. Therefore, all Pythagorean triples (a,b,c) having a = 30 can be found. Find all pairs of integers u and v satisfying conditions (i),(ii), and (iii) of Theorem 3.2.1 and such that $a = \sqrt{uv} = 30$. Thus $uv = 30^2$, and uv is even. Next, claim that $u > 30$. For if $u \leq 30$, then by condition (i) $30 \geq u > v > 0$. So $30^2 > uv = 30^2$, a contradiction. Thus, (1) $u \mid 30^2$; (2) $u > 30$; (3) u is even; (4) $v = 30^2/u$ is even. Therefore, $u = 2 \cdot 3^2 \cdot 5^2 = 450$, $u = 2 \cdot 3^2 \cdot 5 = 90$, $u = 2 \cdot 3 \cdot 5^2 = 150$, or $u = 2 \cdot 5^2 = 50$. With $v = 30^2/u$ the following pairs (u,v): (450,2), (90,10), (150,6), and (50,18) exists. The corresponding Pythagorean triples are

(30,224,226), (30,40,50), (30,72,78), (30,16,34).

Therefore, these triples, together with their variations (224,30,226), and so on, are all the Pythagorean triples having 30 as a leg.

One might be interested in predicting the number of Pythagorean triples with a given leg a. The answer depends on whether a is odd or even. For a odd it is $(\tau[a^2]-1)/2$, while for even a it is $(\tau[(a/2)^2] -1)/2$, where $\tau[n]$ is the total number of positive divisors of n. Thus, if a = 30, $\tau[(\frac{a}{2})^2] = \tau(225) = 9$, then $(9 - 1)/2 = 4$.

Henry Klostergaard also developed a formula that will yield

all Pythagorean triples. This article "Tabulating All Pythagorean Triples" was published in Mathematics Magazine, VOL. 51, NO. 4, September 1978.

Theorem 3.2.2. The general solutions of the Pythagorean Equation, $x^2 + y^2 = z^2$ $(x,y,z \in N)$ can be found in non-redundant form by letting $x = 2n + d$, $y = 2(n + n^2/d)$ and $z = 2n + d + 2n^2/d$ such that n runs through all integers while d is in turn all divisors of $2n^2$ less than $n\sqrt{2}$.

Another method that can be used to find the general solutions of the Pythagorean Equation that is similar to Theorem 3.2.1. but easier to calculate is Theorem 3.2.3.

Theorem 3.2.3. The general solutions of The Pythagorean Equation, $x^2 + y^2 = z^2$ $(x,y,z \in N)$ are as follows, $x = 2n + a$, $y = 2n + b$, $z = 2n + a + b$, where n is an arbitrary natural number, $a,b \in N$, $ab = 2n^2$.

Proof: Assume $x = 2n + a$, $y = 2n + b$, and $z = 2n + a + b$ where $ab = 2n^2$. Then

$$x^2 + y^2 = 4n^2 + 4na + a^2 + 4n^2 + 4nb + b^2$$

$$= 4n^2 + 4na + a^2 + 2ab + 4nb + b^2 \text{ (using } 2ab = 4n^2)$$

$$= (2n + a + b)^2$$

$$= z^2.$$

Conversely, assume (x,y,z) is a Pythagorean triple. (Let $m = x + y - z$ which is positive because $z^2 = x^2 + y^2 < (x + y)^2$ implies $z < x + y$). Substituting $x + y - m$ for z in the given

equation, $x^2 + y^2 = (x + y - m)^2$...(1).

By (1), $x + y - m > y$, hence $x - m > 0$...(2).

Similarly $x + y - m > x$, hence $y - m > 0$...(3).

By (1) $x^2 + y^2 = x^2 + y^2 + m^2 + 2xy - 2xm - 2ym$

$= x^2 + y^2 - m^2 + 2(x - m)(y - m)$.

Therefore, $2(x - m)(y - m) = m^2$. Consequently, m is even and so $m = 2n$, $n \in N$. Then $(x - 2n)(y - 2n) = 2n^2$. Thus, both $x - 2n$ and $y - 2n$ are divisors of $2n^2$. If $a = x - 2n$ and $b = y - 2n$, then $ab = 2n^2$. Hence $x = 2n + a$, $y = 2n + b$, and $z = x + y - 2n$ $= a + b + 2n$, where $ab = 2n^2$. Therefore, the general solutions are as shown in the theorem. Q.E.D.

This method will also provide all Pythagorean triples with a given leg. Example: Find all Pythagorean triples that have 30 as one of their legs. Thus, if $x = 30$, then $a = x - 2n$ and $b = \frac{2n^2}{a}$; consequently,

$$a = 30 - 2n,\ 2n = 30 - a,\ b = \frac{2n^2}{30 - 2n} = \frac{n^2}{15-n}.$$

If p is a prime that divides $15 - n$, then $p|n^2$ because $\frac{n^2}{15 - n}$ is an integer. Thus $p|(15 - n)$ and $p|n$, hence $p|15$. Thus, the prime factors of $15 - n$ are 1, 3 and 5. Since $15 - n < 15$, then $15 - n$ can only equal 1, 5, 3 and 9. Thus, $n = 14$, 10, 12 or 6 and, therefore, $a = 2$, 10, 6, and 18. Consequently, $b = 196$, 20, 48, and 4. Substituting a, b, and n into the equations for x,y,

and z the Pythagorean triples are

(30,224,226), (30,40,50), (30,72,78), and (30,16,34).

# CHAPTER 4

## FERMAT'S THEOREM FOR n = 3 AND 4

Equations of the form $x^n + y^n = z^n$, $n = 3,4,5...(1)$ are considered in this chapter. A solution to this equation is a triple of positive integers (x,y,z) satisfying (1). A primitive solution is a solution such that $(x,y) = (y,z) = (x,z) = 1$; x,y and z are said to be pairwise relatively prime in this case.

### 4.1 Equations of the Form $x^n + y^n = z^n$, $n \geq 3$

Proportion 4.1.1. Let $S = \{p|p$ is an odd prime or $p = 4\}$. If $x^n + y^n = z^n$ has no non-trivial solutions for all $n \in S$, then there is no solution for any integer $n \geq 3$.

Proof: Assume there is a solution for some $n \geq 3$. Since by assumption, $n \notin S$, then n is not prime and $n \neq 4$. If $n = 2^k$ where $k > 2$, then $n = p \cdot 4$. Otherwise $n = p \cdot q$ where q is an odd prime. In either case there exists $q \in S$ such that $n = p \cdot q$. Consider the solution $x^n + y^n = z^n$. Then we have $x^{pq} + y^{pq} = z^{pq}$ or $x_1^q + y_1^q = z_1^q$ where $x_1 = x^p$, $y_1 = y^p$, $z_1 = z^p$. Since $x,y,z \neq 0$ then $x_1,y_1,z_1 \neq 0$. Thus, there exists $q \in S$ and a non-trivial solution to $x_1^q + y_1^q = z_1^q$, contrary to the assumption. Q.E.D.

Proposition 4.1.2. If there exists a non-trivial solution to the equation $x^n + y^n = z^n$, then there exists a solution that minimizes $|z|$ (i.e. there exists a solution $x_1 + y_1 = z_1$ such that

if $x^n + y^n = z^n$ is any solution, then $|z_1| \leq |z|$). Furthermore, there is a primitive solution $(x_1,y_1,z_1)$ such that one of these numbers is even and the other two are odd.

Proof: Let $S = \{r \mid$ there exists a solution $x^n + y^n = z^n$ such that $|z| = r\}$. Since $S \subset N$ and $S \neq \emptyset$ (by our assumption that a solution exists) then S contains a minimal element $r_1$ by the Well Ordering Principle for N. Hence, there exists a solution $(x_1,y_1,z_1)$ such that $|z_1| = r_1$ and for any solution $(x,y,z)$, $|z| \geq r_1$.

For this solution, if p is a prime that divides any two of $(x_1,y_1,z_1)$, then p divides the third. For example, if p divides $x_1$ and $z_1$, then p divides $x_1^2$ and $z_1^2$. Hence, p must divide $y_1^2 = z_1^2 - x_1^2$ and so p divides $y_1$. Therefore, $x_1 = px$, $y_1 = py$ and $z_1 = pz$. Hence, $p^nx^n + p^ny^n = p^nz^n$ and so $x^n + y^n = z^n$ is a solution also. Since $x_1 \neq 0$, $y_1 \neq 0$, $z_1 \neq 0$, $p \neq 0$, then neither x,y, nor z is 0. But $|z_1| = |pz| > |z|$, which contradicts the minimality of $|z_1|$. Therefore, $(x_1,y_1,z_1)$ are pairwise relatively prime. Also, no two of these can be even. Moreover, if any two are odd, the third must be even. Q.E.D.

## 4.2 The Biquadratic Equation

This proof uses the method of infinite descent. The idea is the following: assume that $(x_0,y_0,z_0)$ is one solution in nonzero integers, then there is another solution $(x_1,y_1,z_1)$ of the same kind, with $0 < |x_1| < |x_0|$. Since this procedure may be repeated indefinitely, one would obtain an infinite decreasing sequence of positive integers $|x_0| > |x_1| > |x_2| > \ldots > 0$, which is absurd.

So, there couldn't be any solution in nonzero integers.

Theorem 4.2.1. The equation $x^4 + y^4 = z^2$ has no non-trivial solution.

Proof: Assume $x^4 + y^4 = z^2$ has a non-trivial solution. Then, there exists a solution such that $|z|$ is minimal. Thus, $(x,y) = 1$. (To see that $(x,y) = 1$, let p be a prime that divides x and y. Then $x = px_1$, $y = py_1$, and $p^4x_1^4 + p^4y_1^4 = z^2$. Therefore, $p|z$. Hence, $p^4x_1^4 + p^4y_1^4 = p^2z_1^2$, where $z = pz_1$. Since $p^2x_1^4 + p^2y_1^4 = z_1^2$, $p|z_1$. Let $z_1 = pz_2$. We have $x_1^4 + y_1^4 = z_2^2$ where $|z| = |pz_1| = |p^2z_2| > |z_2|$ gives a contradiction to the minimality of $|z|$.) Thus, $(x,y) = 1$. Thus, $(x^2)^2 + (y^2)^2 = z^2$ with $(x^2,y^2) = 1$. Therefore, $(x^2,y^2,z)$ is a Primitive Pythagorean triple.

Now by Lemma 3.1.5. z is odd and $x^2$ and $y^2$ has opposite parity. Assume x is odd and y is even. According to Theorem 3.1.6. there exist integers a and b such that $x^2 = a^2 - b^2$, $y^2 = 2ab$ and $z = a^2 + b^2$, a and b have opposite parity, $(a,b) = 1$ and $a > b > 0$.

Case 1. Assume a is even and therefore b is odd.

Let $a = 2n$ and $b = 2m + 1$. Therefore, $x^2 = a^2 - b^2 = 4n^2 - 4m^2 - 4m - 1$. Thus, $x^2 \equiv -1 \bmod 4$. But x is odd. So $x = 2k + 1$ and $x^2 = 4k^2 + 4k + 1$, whence $x^2 \equiv 1 \bmod 4$. This is a contradiction. (In other words, $4k^2 + 4k + 1 = 4n^2 - 4m^2 - 4m - 1$, therefore $2 = 4(n^2 - m^2 - m - k^2 - k)$.)

Case 2. Assume a is odd and therefore b is even. If

$b = 2m$, then $y^2 = 2ab = 4am$, hence $(\frac{y}{2})^2 = am$.

Since $1 = (a,b) = (a,2m)$, then $(a,m) = 1$. Therefore, $a = r^2$ and $m = s^2$ by Proposition 2.3.11. Since $a,b \neq 0$ then $r,s \neq 0$. Therefore, $a = r^2$, $b = 2s^2$, and $y = 4r^2s^2$. Since $x^2 = a^2 - b^2 = r^4 - 4s^4$, we have $x^2 + 4s^4 = r^4$. Therefore, $x^2 + (2s^2)^2 = (r^2)^2$ where $(x,2s^2) = 1$. (Note: x is odd, $(x,y) = 1$ and $y = 2ab$, thus $(x,b) = 1$. But $b = 2s^2$, thus $(x,2s^2) = 1$.) Therefore, there exists p and q where $(p,q) = 1$ such that $p^2 - q^2 = x$, $2pq = 2s^2$, and $r^2 = p^2 + q^2$. Since $s \neq 0$, then $p,q \neq 0$. Thus, $s^2 = pq$ and $p^2 + q^2 = r^2$. But $(p,q) = 1$ and $s^2 = pq$ implies $p = u^2$ and $q = v^2$ (Proposition 2.3.11.). Also, since $p,q \neq 0$ then $u,v \neq 0$. Therefore, $p^2 + q^2 = r^2$ implies $u^4 + v^4 = r^2$. Hence, a non-trivial solution to the original equation. Since $x^4 + y^4 = z^2$ is the solution with minimal $|z|$, then $|r| \geq |z|$. But $z = a^2 + b^2 = r^4 + b^2 > |r|$. This is a contradiction. Therefore, $x^4 + y^4 = z^2$ has no non-trivial solution. Q.E.D.

Corollary 4.2.2. There is no non-trivial solution of $x^4 + y^4 = z^4$.

Proof: If $(x,y,z)$ is a solution to the above equation then $(x,y,z^2)$ is a solution to $x^4 + y^4 = (z^2)^2$. Q.E.D.

## 4.3 The Cubic Equation

The first published proof of Fermat's theorem for the case of cubes is due to Euler. An important step in Euler's proof,

which used divisibility properties of integers of the form $a^2 + 3b^2$, was done without sufficient justification. Legendre, who reproduced Euler's proof did not give any further explanations. Since he was himself also an expert on such matters, he understood Euler's reasoning. However, later mathematicians were less comfortable about the possible gap, and in 1894, Schumacher pointed it out explicitly. The gap occurred in Euler's proof of the statement that if s is odd and $s^3 = a^2 + 3b^2$, with gcd(a,b) = 1, then $s = u^2 + 3v^2$, with u,v integers.

Another proof of Fermat's theorem for cubes was given by Gauss. Both proofs use the method of infinite descent. However, while Euler worked with integers of the form $a^2 + 3b^2$, Gauss used complex algebraic numbers of the form $a + b\sqrt{-3}$.

Theorem 4.3.1. The equation $x^3 + y^3 = z^3$ has no non-trivial solutions.

Proof: Assume there are solutions of $x^3 + y^3 = z^3$. Then according to Proposition 4.1.2., there exists (x,y,z) that is pairwise relatively prime such that exactly one of these integers is even. If x is even, rewrite the equation as $(-z)^3 + y^3 = (-x)^3$. A similar rearrangement is possible if y is even. Thus, assume without lost of generality that x and y are odd and z is even. Thus, a non-trivial solution to $x^3 + y^3 = z^3$, where z is even, which minimizes $|z|$. Now x and y are odd, therefore, write $p = \frac{x+y}{2}$ and $q = \frac{x-y}{2}$. Since (x,y) = 1, then

$p \neq 0$ and $q \neq 0$. Since $p + q = x$ and $p - q = y$ then p and q must have opposite parity because x and y are odd. Furthermore, $(p,q) = 1$ because $(x,y) = 1$.

Now

$$z^3 = (p + q)^3 + (p - q)^3$$
$$= p^3 + 3p^2q + 3pq^2 + q^3 + p^3 - 3p^2q + 3pq^2 - q^3$$
$$= 2p^3 + 6pq^2$$
$$= 2p(p^2 + 3q^2).$$

Consider 2 cases, (1) z is not divisible by 3 and (2) z is divisible by 3.

Case 1. Suppose $3 \nmid z$.

Consider p and $p^2 + 3q^2$. Now $(p,q) = 1$ and $3 \nmid z^3$. Since $z^3 = 2p(p^2 + 3q^2)$, thus $3 \nmid p$. If $r|p$ where r is prime and $r \neq 3$ then $r \nmid q$. Thus $r \nmid (p^2 + 3q^2)$. Consequently $(p, p^2 + 3q^2) = 1$. Now if q is even, then p would be odd because p and q have opposite parity. Thus, $p(p^2 + 3q^2)$ is odd, and therefore $4 \nmid [2p(p^2 + 3q^2)] = z^3$. But since z is even, $4|z^3$ which is a contradiction. Therefore, q is odd and p is even. So $p^2 + 3q^2$ is odd. Thus, $(2p, p^2 + 3q^2) = 1$. Thus, by Proposition 2.3.11. $z^3 = 2p(p^2 + 3q^2)$ implies $2p = \alpha_1^3$ and $p^2 + 3q^2 = \beta^3$, where $\beta > 1$ is odd. Since $\alpha_1$ must be even, say $\alpha_1 = 2\alpha$, then $p = 4\alpha^3$, $p^2 + 3q^2 = \beta^3$ and $z^3 = 2p(p^2 + 3q^2) = 8\alpha^3\beta^3$. Thus, $z = 2\alpha\beta$. Now $p \neq 0$ and $q \neq 0$ implies $\alpha \neq 0$ and $\beta \neq 0$. So $p^2 + 3q^2 = \beta^3$ with $(p,q) = 1$. Hence, according to Theorem 2.6.5., there exists r,s such that $(r,s) = 1$ and

$p+q\sqrt{-3} = (r+s\sqrt{-3})^3 = r^3-9rs^2+(3r^2s-3s^3)\sqrt{-3}$. Therefore,

$p = r(r^2 - 9s^2)$ and $q = 3s(r^2 - s^2)$. But $p = 4\alpha^3$, thus $4\alpha^3 = r(r + 3s)(r - 3s)$. Now $3 \nmid p = r(r^2 - 9s^2)$, whence $3 \nmid r$. Also $q = 3s(r^2 - s^2)$ is odd, thus s is odd and r is even. Therefore, $r + 3s$ and $r - 3s$ must be odd and $2r$, $r + 3s$, $r - 3s$ are pairwise relative prime. (Note that $2r = (r + 3s) + (r - 3s)$ while $6s = (r + 3s) - (r - 3s)$.) Thus, $4\alpha^3 = r(r + 3s)(r - 3s)$ implies $(2\alpha)^3 = 2r(r + 3s)(r - 3s)$, and therefore implies $2r = m^3$, $r + 3s = n^3$, $r - 3s = k^3$. Also, $3 \nmid r$ and $r,s \neq 0$ implies m,n and $k \neq 0$. Thus, $n^3 + k^3 = 2r = m^3$ is a non-trivial solution with m even. Finally, $|z| = |2\alpha\beta|$

$$= |\beta[2r(r+3s)(r-3s)]^{\frac{1}{3}}|$$

$$= |\beta| \; |[m^3n^3k^3]^{\frac{1}{3}}|$$

$$= |\beta| \; |nk| \; |m| > |m|.$$

(Note $|\beta^3| = |p^2 + 3q^2| > 1$ implies $|\beta| > 1$.)
This contradicts the minimality of $|z|$.

Case 2. Assume $3|z$.

Recall $z^3 = 2p(p^2 + 3q^2)$ where $(p,q) = 1$ and p,q have opposite parity. Again, z is even, thus 8 divides $z^3 = 2p(p^2 + 3q^2)$ and since $(p^2 + 3q^2)$ is odd, then p is even and q Thus, a contradiction. Therefore, 3 divides both z and p.

Let $p = 3p_1$ and $z = 3z_1$. Therefore $27z_1^3 = 6p_1(9p_1^2 + 3q^2)$, which implies $3z_1^3 = 2p_1(3p_1^2 + q^2)$. Now $3p_1^2 + q^2$ is odd and $3 \nmid q$ since $(p,q) = 1$ and $3|p$. Hence, $3 \nmid (3p_1^2 + q^2)$. If r is a prime dividing both $2p_1$ and $3p_1^2 + q^2$, then $r \neq 2$ since $(3p_1^2 + q^2)$ is

odd, and $r \neq 3$. Also $r|p = 3p_1$. Therefore, $r|p_1$ and since $r|(3p_1^2 + q^2)$, then r would divide $q^2$. This is impossible since $(p,q) = 1$. Therefore, $(2p_1, 3p_1^2 + q^2) = 1$. Since $3 \nmid 3p_1^2 + q^2$ then $3z_1^3 = 2p_1(3p_1^2 + q^2)$ implies $3\alpha_1^3 = 2p_1$ and $3p_1^2 + q^2 = \beta^3$. Since $\alpha_1$ is even, and if $\alpha_1 = 2\alpha$, we have $24\alpha^3 = 2p_1$ implies $12\alpha^3 = p_1$. Therefore, $p = 3p_1 = 36\alpha^3$. Thus, $p = 36\alpha^3$, $3p_1^2 + q^2 = \beta^3$ and

$$\begin{aligned} z^3 &= 2p(p^2 + 3q^2) \\ &= 2p(9p_1^2 + 3q^2) \\ &= 6p(3p_1^2 + q^2) \\ &= 6(36\alpha^3)\ (\beta^3) \\ &= (6\alpha\beta)^3. \end{aligned}$$

Therefore, $z = 6\alpha\beta$. Also note that $(p,q) = 1$ and $p = 3p_1$ implies $(p_1,q) = 1$. Now $3p_1^2 + q^2 = \beta^3$ where $\beta > 2$ is odd, then by Theorem 2.6.5. there exists r and s with $(r,s) = 1$ such that

$$q+p_1\sqrt{-3} = (r+s\sqrt{-3})^3 = (r^3-9rs^2)+(3r^2s-3s^3)\sqrt{-3}.$$

Therefore, $q = r(r^2 - 9s^2)$ and $p_1 = 3s(r^2 - s^2) = 3s(r + s)(r - s)$. But $p_1 = 12\alpha^3$, hence $4\alpha^3 = s(r + s)(r - s)$. Since $p_1$ is even and q is odd then r is odd and s is even. Also $(r,s) = 1$ implies s, $r + s$ and $r - s$ are pairwise relatively prime. Thus, $s = 4n^3$, $r + s = m^3$, $r - s = -k^3$ and $2s = 8n^3 = n_1^3$. Therefore, since $(r + s) - (r - s) = 2s$ we have $m^3 + k^3 = n_1^3$ where $n_1^3$ is even and

$$\begin{aligned} 8\alpha^3 &= 2s(r + s)(r - s) \\ &= n_1^3 m^3(-k)^3 = -(n_1 mk)^3. \end{aligned}$$

Therefore, $|2\alpha| = |n_1 mk|$. Thus $|z| = |6\alpha\beta|$

$$\begin{aligned} &= |6\alpha|\ |\beta| > |2\alpha| \\ &= |n_1 mk| \geq |n_1|. \end{aligned}$$

Therefore, $m^3 + k^3 = n_1^3$ and $n_1$ is even is a solution such that $|n_1| < |z|$, which contradicts the fact that $|z|$ is minimal.

Q.E.D.

# CHAPTER 5

## SUMMARY

Many new theorems have been proved concerning some Diophantine equations, in particular, Fermant's Last Theorem. However, these theorems are old methods stated a new way. No one has been able to prove Fermant's Last Theorem past n = 125,000,000 not even today in the age of high speed super computers.

In conclusion, "THE MYSTERY OF THE QUEEN LIVES ON."

REFERENCES

(1) Efraim P. Armendariz and Stephen McAdam, Elementary Number Theory, Macmillan, 1980.

(2) J. S. Chahal, Topics in Number Theory, Plenum Press, New York, and London, 1988.

(3) David A. Cox, Primes of the Form $X^2 + NY^2$, John Wiley & Sons, 1989.

(4) Emil Grosswald, Topics From The Theory Of Numbers, Second Edition, Birkhauser, 1984.

(5) G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford At The Clarendon Press, 1979.

(6) Henry Klostergaard, "Tabulating All Pythagorean Triples," Mathematics Magazine, Volume 51, Number 4, September 1978.

(7) Paulo Robenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York, 1979.

(8) Andrea Rothbart and Bruce Paulsell, "Pythagorean Triples: A New, Easy-to-Derive Formula with Some Geometric Applications," Mathematics Teacher, Vol.67

(9) G. J. Simmons, "Some Results Pertaining to Fermat's Conjecture," Mathematics Magazine 1978, (March, 1974), pp 215 - 218.

(10) J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, McGraw-Hill, New York, 1939.