

2005

Fermat numbers : historical view with applications related to fermat primes

Faun C. Maddux
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

Recommended Citation

Maddux, Faun C., "Fermat numbers : historical view with applications related to fermat primes" (2005). *Master's Theses*. 2857.
DOI: <https://doi.org/10.31979/etd.33vf-wuzn>
https://scholarworks.sjsu.edu/etd_theses/2857

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

NOTE TO USERS

This reproduction is the best copy available.

UMI[®]

FERMAT NUMBERS:
HISTORICAL VIEW WITH APPLICATIONS RELATED TO FERMAT PRIMES

A Thesis
Presented to
The Faculty of the Department of Mathematics
San Jose State University

In Partial Fulfillment
Of the Requirements for the Degree
Master of Sciences

by
Faun C. Maddux
December 2005

UMI Number: 1432475

INFORMATION TO USERS

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

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

UMI[®]

UMI Microform 1432475

Copyright 2006 by ProQuest Information and Learning Company.

All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

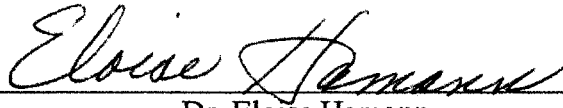
ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

© 2005

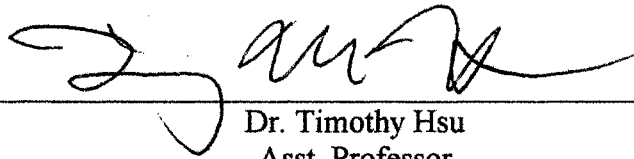
Faun C. Maddux

ALL RIGHTS RESERVED

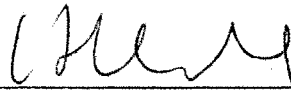
APPROVED FOR THE DEPARTMENT OF MATHEMATICS



Dr. Eloise Hamann
Professor




Dr. Timothy Hsu
Asst. Professor



Dr. Ho Kuen Ng
Professor

APPROVED FOR THE UNIVERSITY

 11/07/05

ABSTRACT

FERMAT NUMBERS: HISTORICAL VIEW WITH APPLICATIONS RELATED TO FERMAT PRIMES

By Faun C. Maddux

According to Philip Davis, “One of the endlessly alluring aspects of mathematics is that its thorniest paradoxes have a way of blooming into beautiful theories” (Guillemets). This thesis examines some of the exciting historical developments surrounding one of these thorny dilemmas: Fermat’s conjecture that numbers of the form $2^{2^n} + 1$ are prime for all $n \in \mathbb{Z}^{\text{nonnegative}}$. While it took almost 100 years before Euler found a counterexample, and another sixty years for Gauss to make the discovery that ignited interest in these numbers, serious mathematical strides resulting in beautiful theories have been made ever since. After examining several highlights pertaining to Fermat numbers, this paper focuses on three applications whose proofs rely heavily upon the power of Fermat primes: Gauss’ aforementioned theorem followed by modern results due to Dr. Florian Luca (concerning Heron triangles) and Carrie Finch and Lenny Jones (regarding finite minimal POS groups). Lastly, the reader is offered several open problems.

ACKNOWLEDGEMENT

Without the countless hours of teaching, advising, prodding, and editing provided by my tireless advisor, Dr. Eloise Hamann, I would have remained forever an outsider to the stunning world of perplexing charm concealed within the arms of abstract algebra and number theory. Having further glimpsed a small portion of the amazing and intricate connections between these subjects and Geometry through the eyes of Fermat primes has brought another level of depth to my awareness of a subject already dear to my heart. I can now appreciate Leonhard Euler's statement, "mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate," and I can smile with Paul Erdős comment, "God may not play dice with the universe, but something strange is going on with the prime numbers," for I now have an experience scarcely deep enough to ponder these things.

I also wish to thank my thesis committee members, Dr. Timothy Hsu and Dr. Ho-Kuen Ng, for their faithful encouragement and patience during my thesis research. I will always remember their kind requests, gentle reminders, and excellent editing advice.

Last but not least, I must reveal my gratitude to my family. My mother's exceptional enthusiasm and willingness to proof my paper, listen to my explanations, and pray for my progress have been invaluable to me. My husband's long-suffering tolerance and steadfast love during my many hours of study have carried me farther than I ever dreamed possible. To my sister, Jody, and brothers, Ed and Dustin, and all my remaining family and friends who have helped and prayed for me, I give considerable thanks.

TABLE OF CONTENTS

List of Tables and Figures.....	vii
Glossary of Symbols.....	viii
CHAPTER ONE.....	1
INTRODUCTION: FERMAT’S PLACE IN HISTORY	1
CHAPTER TWO.....	7
A QUICK SURVEY OF RESULTS ASSOCIATED WITH FERMAT NUMBERS	7
CHAPTER THREE.....	12
INTERESTING APPLICATIONS WITH FERMAT PRIMES IN KEY ROLES.....	12
Application One: Gauss’s Theorem.....	13
A. Introduction To Gauss’s Theorem.....	13
B. Geometric Constructions and the First Biconditional	15
C. Background Information Needed for the Forward Direction of the Proof.....	18
D. Forward Direction of the Proof.....	22
E. Background Information Needed for the Reverse Direction of the Proof.....	26
F. Reverse Direction of the Proof.....	28
G. Illustrations	30
Application Two: Heron Triangles.....	31
A. Introduction	31
B. Preliminary Information About Heron Triangles	32
C. Classical Parameterization of Pythagorean Triples.....	39
D. Some Important Theorems and a Key Lemma.....	42
E. Proving the Main Theorem.....	48
Application Three: Finite Minimal POS Groups.....	55
A. Introduction	55
B. Reviewing Key Ideas.....	56
C. Setting the Stage: New Ideas and Definitions	58
D. Immediate Consequences	60
E. Crucial Facts Used in the Proof of the Culminating Theorem	70
F. Proving The Main Theorem	71
CHAPTER FOUR	82
CONCLUDING COMMENTS AND OPEN PROBLEMS	82
Works Cited.....	90
Works Referenced	91

LIST OF TABLES

Table		Page
1	Number of elements of given orders in $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$	59
2	Number of elements of given orders in $G = (\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	65
3	Number of elements of given orders in $G_1 = (\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	66
4	Number of elements of given orders in $(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$	74
5	Number of elements of given orders in $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$	76
6	The number of prime factors for the first thirteen Fermat numbers.....	86

LIST OF FIGURES

Figure		Page
1.1	Constructing a product.....	16
1.2	Constructing a quotient.....	16
1.3	Constructing the angle $2\pi/n$	17
1.4	Three regular n -gons constructed with Geometer's Sketchpad ($n = 6, 8, 10$)	30
2.1	Illustrations of right, acute, and obtuse Heron triangles.....	33
2.2	A triangle with altitude inside the triangle.....	36
2.3	A triangle with altitude outside the triangle.....	37

Glossary of Symbols

F_m	Fermat number: $F_m = 2^{2^m} + 1$ for $m = 0, 1, 2, \dots$
\mathbb{N}, \mathbb{Z}	set of natural numbers (with or without 0), set of integers
$\mathbb{Z}^+, \mathbb{Z}^*$	set of positive integers, nonzero integers
$\mathbb{Z}^{\text{nonnegative}}$	set of nonnegative integers (specifically includes 0)
$\mathbb{Q}, \mathbb{C}, \mathbb{R}$	set or field of rational numbers, complex numbers, and real numbers
$\mathbb{R} \setminus \mathbb{Q}$	set of all elements of \mathbb{R} that are not elements of \mathbb{Q}
\mathbb{Z}_n	elements of \mathbb{Z} mod n : $\{0, 1, \dots, n-1\}$
\bar{F}	algebraic closure of the field F
$a \equiv_n b$	a congruent to b modulo n
$a \not\equiv_n b$	a is not congruent to b modulo n (backward slash generally indicates <i>not</i>)
$m n$	m divides n
$m n$	m maximally divides n
$\gcd(a, b)$	greatest common divisor of a and b
$\min(a, b)$	the minimum value of a or b
$\phi(n)$	Euler totient function (<i>counts</i> $m \in \mathbb{N}$ where $m < n$ and $\gcd(m, n) = 1$)
$\Phi_n(x)$	n^{th} Cyclotomic polynomial
\bar{a}	coset of a (under a homomorphism)
$\text{irr}_{\mathbb{Q}}(\varepsilon)$	the unique monic irreducible polynomial for which ε is a root over \mathbb{Q}
$\text{Gal}(E/F)$	Galois group of E over F (group of all Galois automorphisms of E over F)
E_S	the set of elements of E left fixed by elements of a subset $S \in \text{Gal}(E/F)$
$\{G : H\}$	index of H in G (H is a subgroup of G)
$\{K : L\}$	index of K over L (K is a finite extension of field L) <i>(number of isomorphisms of K onto a subfield of \bar{L} leaving L fixed)</i>
$[K : L]$	degree of K over L (K is a finite extension of field L)
$ G $	cardinality of group G (<i>number of elements in G</i>)
$\langle a \rangle$	subgroup generated by a
\rightarrow	implies
\leftrightarrow	if and only if
\Rightarrow	forward direction of if and only if ($p \rightarrow q$ for $p \leftrightarrow q$ statement)
\Leftarrow	reverse direction of if and only if ($q \rightarrow p$ for $p \leftrightarrow q$ statement)
$\rightarrow \leftarrow$	contradiction
\mapsto	mapped to (under a homomorphism)
\leq	subgroup or subfield
\triangleleft	normal subgroup
\cong	isomorphic to
\square	end of proof

CHAPTER ONE

INTRODUCTION: FERMAT'S PLACE IN HISTORY

“In most sciences, one generation tears down what another has built, and what one has established, another undoes. In mathematics alone each generation adds a new story to the old structure.”

Hermann Hankel

Considering developments in recorded mathematical history is an incredible journey of wonder and awe. Unleashing fundamental truths governing the world, its properties and laws of motion, and witnessing the seemingly impossible connections between these truths offers adventure to the avid learner. Sadly, however, many take these advances for granted or, even worse, as nuisances to be tolerated. For instance, is there a beginning algebra student that fully appreciates the beauty of the abstraction they are learning or the countless hours that went into developing the simplicity and logic of the system he or she is being asked to use? Much deeper understanding is needed before such an appreciation can occur. Similarly, when deep-rooted theories are being uncovered, it has frequently taken society years to accept and understand the consequences. Therefore, as mankind has developed the mathematical tools needed to dissect scientific questions, not every participant has been blessed to see the culminating crescendo of beautiful harmony that his or her contribution has had within the orchestra of the mathematical framework being constructed. Pierre de Fermat was such a participant, for the questions he raised have had far-reaching consequences to this day. Thus, before going directly to current theoretical results, looking briefly at Fermat's

background may increase the reader's appreciation for the scope of Fermat's contribution to the small piece of the mathematical framework being examined in this thesis.

Pierre de Fermat was born into a wealthy family in Beaumont-de-Lomagne, France, on August 17, 1601. While his father, Dominique Fermat, was a leather merchant who held an important position akin to being mayor, his mother, Claire née de Long, was the daughter of a prominent family (notice that "de" indicated nobility, a status the Pierre Fermat achieved in 1631 in association with a career promotion). When Pierre de Fermat later married Louis de Long, his cousin fourth removed, an entire upper class family surrounded him.

Young Fermat was educated primarily at home. He spoke five different languages and was highly intelligent; however, he had a rather slow work style and was quite modest and retiring. After his home-based education, Fermat studied law at a local school and subsequently joined the legal profession on May 14, 1631, which was a natural progression given the era and his family status. Although Fermat was interested in mathematics, performing his first serious research in 1629 (restoring Apollonius's *Plane Loci* and uncovering important results with maxima and minima), this was not a viable career option. During the first half of the Seventeenth Century, the term mathematician referred to what one would call an astronomer today, and the study of mathematics was not a professional discipline. Instead, those who pursued mathematics were identified by the predecessors, or "schools," of thought and conventions that they followed. The reader may recall that Western mathematical study, in particular algebra and number theory, was first revitalized with Leonardo de Pisa (Fibonacci) in the early

Twelfth Century. Fibonacci was followed by Ferro, Tartaglia, Cardano and Ferrari, who were succeeded by François Viète (among others). Fermat followed the school of Viète, a school with cumbersome notation, which may have separated him from some of his contemporaries.

Ironically, those who investigated mathematics out of love and without professional recognition during the Seventeenth Century forged the foundations for modern mathematics. The four men who made the most cutting advances were Girard Desargues, René Descartes, Blaise Pascal, and Pierre Fermat. Winifried Scharlau and Hans Opolka, in From Fermat to Minkowski, gave interesting classifications for each: Desargues was the most original, Descartes the most famous, Pascal the most ingenious, and Fermat the most important (Scharlau, 5). While the reader may or may not agree with the awards thus given, the author had to smile with Fermat's well-deserved status. Interestingly, many other sources indicate similar reverence for Fermat, calling him one of the leading mathematicians of the Seventeenth Century to one of the greatest mathematicians of all times. Even Descartes, with whom Fermat had a famous disagreement, begrudgingly admired Fermat's work, calling Fermat's Four Square Theorem (every natural number is the sum of four squares of natural numbers), "one of the most beautiful (theorems) that can be found in number theory," the proof of which would be so difficult that he would "not even attempt to search for it" (9). While Fermat made advances in modern calculus methods (independently of Descartes), two and three dimensional analytic geometry, optics, quadrature and tangents of curves, and probability (to name a few), his true love was number theory, an area of the mathematical foundation

that many of his contemporaries simply weren't attracted to or had difficulty understanding. Ironically, Fermat had no interest in real-life applications, yet he produced some very applicable results, most notably in physics, and investigations of his number theory work "has originated several new mathematical disciplines" (Křížek, xvi), much of which is highly applicable to modern technology.

Most of what is known about Fermat's work comes from his correspondence with his contemporaries. He shared his work with maxima and minima with Jean Beaugrand (another follower of Viète) and Étienne d'Espagnet around 1630. This led to correspondence with Pierre de Carcavi, Marin Mersenne, Étienne Pascal, Gilles Roberval, Bernard Frénicle de Bessy, and René Descartes. After the Descartes controversy in which Fermat realized that Descartes' sine law was in conflict with the Aristotelian viewpoint that nature chooses the shortest path, Fermat lost touch with his contemporaries due to work pressure, a Civil War and the Plague (he nearly lost his life to the latter). During these silent years, Fermat quietly worked on number theory, finding his true love. Then, in the 1650's, he rejoined his colleagues, writing to mathematicians in Paris as well. He worked on spirals and falling bodies (reporting errors in Galileo's calculations) and generalized Archimedes' methods. During this time Fermat began writing his "challenge" letters in which he would present his discoveries as challenge problems (without giving the solutions). This led to his quick reputation as a leading mathematician, but many were annoyed with his challenges, as they seemed impossibly difficult. In 1654 he co-founded probability theory with Blaise Pascal (Étienne Pascal's son) and tried to generate a focus on number theory, but no one was interested. This

drove Fermat even deeper into his challenge letters, and the first hints of Fermat's far-reaching influence began to emerge. John Wallis and William Brouncker developed the method of continued fractions in their solution to one of Fermat's challenges. This result was one of the first breakthroughs accomplished in connection with work done in association with Fermat's achievements. Other results that followed included discovery of commutative ring theory, the first questioning of unique factorization in integral domains, development of the theory of quadratic forms, innovation of quadratic reciprocity, creation of class field theory, introduction of Pell's equation, and many deeper results in number theory, all of which emerged in connection with proofs of Fermat's theorems. Not surprisingly, Fermat is thus credited with founding modern number theory. Speaking of six theorems Fermat listed as some of his most important theorems in a letter written in 1656 to Carcavi, Scharlau noted that "it is remarkable with what certainty he (Fermat) identified central problems in number theory. Each of these theorems ... is the starting point for a deep and rich theory" (Scharlau, 9). However, Fermat only published one mathematical paper (in the appendix of a colleague's book) and, in all of his writings, left us only one proof (O'Connor, Fermat's Last Theorem), so mathematicians who succeeded Fermat were left with the exciting framework of his results without the body to support it. Fortunately, several able thinkers took up the mantle and ran with it. One of these mathematicians who further developed Fermat's work, creating some of the theory mentioned above, was Leonhard Euler. Euler believed "Fermat's assertions were serious theorems deserving of proofs" (Cox, 8), and he spent forty years proving and generalizing Fermat's results. Other notable mathematicians,

beyond Fermat's contemporaries, who were fascinated with Fermat's results include Christian Huygens, Isaac Barrow (teacher of Isaac Newton - Křížek, xv), Carl Gauss, Joseph Lagrange, and, most recently, Andrew Wiles.

As Euler discovered in 1732, not all of Fermat's conjectures were true, yet even this did not limit the influence of the incorrect "theorem." In fact, the subsequent results had rippling effects in the foundation of mathematics from number theory to geometry and led to the theorems investigated in this thesis. The conjecture in question, that numbers of the form $2^{2^m} + 1$ are prime for any nonnegative integer m , was introduced in 1650. Numbers of this form, $F_m = 2^{2^m} + 1$, are called Fermat numbers in honor of Fermat. In the numerous attempts to prove this assertion, before Euler found that F_5 was composite, a wealth of properties inherent to numbers of this type was discovered, and numerous factorization and computational advances were made. The reader may find it interesting, for example, that the largest computation ever performed to obtain a yes or no answer (whether the number was or was not prime) was performed in 1999 when checking the primality of F_{24} (5). This paper will not consider computational results, but will instead look at more theoretical applications. However, before examining the modern applications being considered in this paper, some of the more fascinating results concerning Fermat numbers will be reviewed.

CHAPTER TWO

A QUICK SURVEY OF RESULTS ASSOCIATED WITH FERMAT NUMBERS

The body of work accomplished in association with Fermat numbers is almost overwhelming. One could spend days, if not years, studying any single piece of the puzzle. This section, therefore, is in no way meant to be comprehensive, but rather the reader is offered a few highlights in order that he or she may glimpse the framework under-girding the applications to be explored in the following chapter. The author surveyed several sources, and the majority of the information presented here paraphrases the results she encountered. Among the many diverse paths of study related to Fermat numbers, one will find numerous recurrence relations, tests for compositeness and divisibility, connections with Geometry, and modern day applications to technology.

As mentioned previously, it took many years for mathematicians to have any interest in Fermat numbers, yet once curiosity was generated, many recurrence relations among the numbers sprang forward. One that the author found interesting is the following (for a proof, see Křížek, 26):

$$F_m = \left(\prod_{i=0}^{m-1} F_i \right) + 2 \text{ for all } m \geq 1$$

There are two immediate consequences of the above relation. First, notice that for all $1 \leq i < m$, $F_i \mid F_m - 2$ or $F_m \equiv_{F_i} 2$. In particular, since $F_1 = 5$, we know $F_m \equiv_5 2$ for any $m > 1$. However, $F_m \equiv_2 1$ (since every Fermat number is odd), whence $F_m \equiv_{10} 7$ for any

$m > 1$. This results in the remarkable fact that every Fermat number (except the first) ends in 7. The second result is Goldbach's Theorem:

Given any two distinct Fermat numbers, the only common divisor is 1.

To see this, pick any two Fermat numbers, say F_m and F_{m-k} for some $m > k \geq 1$, and let

$q \in \mathbb{N}$ be a common divisor. Then, $q \mid F_{m-k}$ and, by the recurrence relation, we know

$F_{m-k} \mid F_m - 2$, whence $q \mid F_m - 2$. But then $q \mid 2$ since $q \mid F_m$ and $q \mid F_m - 2$, so $q = 1$

(since $2 \nmid F_m$ for any m). Interestingly, this result provides another way to show there are infinitely many primes.

In addition to the myriad of recurrence relations, a plethora of tests for compositeness have been unearthed. For instance, one can prove that if an integer can be expressed as the sum of two different non-zero squares (of integers) in two different ways ($n = a^2 + b^2 = c^2 + d^2$ with $a > c \geq d > b \geq 1$), then the number must be composite (see Křížek, 7 and 49). Following this fact, notice that any Fermat number can be written as (for $m > 0$):

$$2^{2^m} + 1 = 2^{2^{m+1-1}} + 1 = 2^{2(2^{m-1})} + 1 = \left(2^{2^{m-1}}\right)^2 + 1^2$$

From this it follows that if one can find two integral squares, neither of which is 1, that add to give any F_m , then that particular Fermat number must be composite. The calculations involved in the above, however, are often tedious and difficult, whence further tests have been developed. Two well-known tests that give necessary and sufficient conditions for testing whether or not a number is prime are Lucas's Test and

Selfridge's Test (the latter is a refinement of the former). Both of these tests are, in turn, used to prove Pepin's Test:

any Fermat number is prime if and only if $3^{(F_m-1)/2} \equiv_{F_m} -1$ where $m \geq 1$

(for a proof, see Křížek, 42). The reader may find it interesting that instead of using three in the congruence just stated, Pepin actually used five as his base, and many other bases including ten and certain Fermat primes have been shown to work as well; however, three is the common base used today. Although this test is easily applied, it gives no insight into the factors hidden within a composite Fermat number, and numerous other tests have been developed since Pepin introduced this test in 1877.

On the flip side of testing for primality of the Fermat numbers themselves, many mathematicians have investigated properties of the prime divisors of Fermat numbers. For instance, in 1878 Édouard Lucas showed that if $m > 1$ and p is a prime number that divides F_m , then $p = k2^{m+2} + 1$ for some $k \in \mathbb{N}$ (59). This generated a lot of interest, and these prime factors began receiving a lot of attention. Many results followed, some opening new questions that still are not answered to this day. For example, in 1960 Sierpiński showed that there are infinitely many values for $k \in \mathbb{N}$ such that all the numbers in the set $\{k2^n + 1 : n \in \mathbb{N}\}$ are composite (71), yet the smallest value of k for which this holds has not been found (60).

While considerable attention is still given to Fermat numbers, the discovery that initially established interest in these numbers came in 1796 when Gauss announced the following relationship between constructible regular n -gons and Fermat primes:

There exists a Euclidean construction of the regular n -gon if and only if

$$n = 2^i \prod_{j=0}^l p_j \text{ where } n \geq 3, i \geq 0, l \geq 0, \text{ and each } p_j \text{ is a distinct Fermat prime.}$$

This theorem will be addressed in detail in the following section, yet there is something of extreme curiosity to be said here. To begin, notice that since there are only five known Fermat primes ($F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$), Gauss's theorem tells us there are exactly 31 known constructible n -gons with odd number of sides (if, as is widely conjecture, these are the only Fermat primes). For instance, letting $i = 0$, we have constructible regular triangles, pentagons, 15-gons, 17-gons, 51-gons, 85-gons, 255-gons and so forth. Now, if one considers Pascal's famous triangle, rewriting each entry with its equivalent modulo 2, the following results:

$$\begin{array}{c} 1 \\ 1\ 1 \\ 1\ 0\ 1 \\ 1\ 1\ 1\ 1 \\ 1\ 0\ 0\ 0\ 1 \\ 1\ 1\ 0\ 0\ 1\ 1 \\ 1\ 0\ 1\ 0\ 1\ 0\ 1 \end{array}$$

and so forth. Then, considering each row to be a number written in base 2, one obtains a particularly interesting sequence of numbers:

1	1
1 1	$2 + 1 = 3$
1 0 1	$4 + 0 + 1 = 5$
1 1 1 1	$8 + 4 + 2 + 1 = 15$
1 0 0 0 1	$16 + 0 + 0 + 0 + 1 = 17$
1 1 0 0 1 1	$32 + 16 + 0 + 0 + 2 + 1 = 51$
1 0 1 0 1 0 1	$64 + 0 + 16 + 0 + 4 + 0 + 1 = 85$

These numbers, with the exception of 1, are precisely the same as the number of sides of the regular constructible n -gons (with odd number of sides)! In fact, the first thirty-two

rows give all thirty-one such n -gons. William Watkins discovered this remarkable connection (Křížek, 35), although another mathematician proved it. Interestingly, there are several other connections with Fermat numbers and Pascal's triangle, some of which further relate to a connection with Geometry as well.

Fermat may have been pleased with the connection between his primes and Geometry, but his first fascinations were perfect and amicable numbers (Scharlau, 6), thus he would have been sad to discover that a Fermat number is never perfect or part of an amicable pair (Luca, 171). On the other hand, he loved brain-teasers (Scharlau, 6), so he would have been delighted with the use of his numbers in generating pseudoprimes and other technologic-specific functions. Some of the many applications that use Fermat primes are number-theoretic transforms, fast multiplication of large numbers, analysis of the logistic equation, hashing schemes, and pseudorandom generation (see Křížek, 165 – 186). The reader should note that there are many interesting connections between Fermat numbers and pseudoprimes. Recall that a composite number n is a pseudoprime (to the base a) if there exists an $a \in \mathbb{N}$ such $n \mid a^n - a$. It follows (with some work) that all Fermat numbers are either prime or are pseudoprime to the base 2, and Fermat may have realized this (36 – 37). Another fun fact is that Fermat numbers were used in the first proof of the infinitude of the pseudoprimes (133). One could say that even though Fermat was not particularly interested in real-life applications, his challenges and discoveries have certainly had far-reaching consequences, some with real-life relevance (particularly in technology) and many with theoretical relevance. We shall now shift our focus to three specific results that rely heavily on Fermat primes in their proofs.

CHAPTER THREE

INTERESTING APPLICATIONS WITH FERMAT PRIMES IN KEY ROLES

Before presenting the following applications, the author wishes to alert the reader that all of the material presented herein originated from other sources. Therefore, the author wishes to begin this exciting chapter by acknowledging the primary source from which each application arose. The first application is the oldest and is, naturally, due to Gauss. The author surveyed several different proofs of this theorem and has distilled the information. Therefore, rather than giving the shortest proof possible, the author has chosen to present several interesting approaches in the various stages of the proof. The second application also has its roots in antiquity, yet the result under consideration is due to the current research of Dr. Florian Luca and is found in the journal article, "Fermat Primes and Heron Triangles with Prime Power Sides." Finally, a modern result in finite abelian group research presented by Carrie Finch and Lenny Jones in "A Curious Connection Between Fermat Numbers and Finite Groups" is examined. The author is indebted to the above for the framework they created. Taking pieces of the puzzle thus put in place, the author filled in missing details and supplied omitted proofs.

Application One: Gauss's Theorem

A. Introduction To Gauss's Theorem

Note that there are many theorems due to Gauss, yet we are only considering his famous constructibility theorem, so we call it simply Gauss's Theorem.

Gauss's Theorem: There exists a Euclidean construction (via straightedge and compass)

of the regular n -gon if and only if $n = 2^i \prod_{j=0}^l p_j$ where

$n \geq 3$, $i \geq 0$, $l \geq 0$, and each p_j is a distinct Fermat prime.

Although one may argue that Euclidean constructions are hobby material, the author finds this theorem very intriguing. Indeed, modern mathematicians do not spend a lot of time with collapsible compasses, painstakingly pursuing constructibility patterns, yet the intricate designs a student may encounter during a Geometry course still elicit a sense of excitement as simple lines and arcs bring forth concise sketches. Meeting significant challenges in attempting to reveal much simpler tasks than constructing a regular 257-gon, the author felt a sense of awe upon reading this theorem, wondering what Gauss must have encountered in his hours of study to realize such a truth. Not only did he determine how to construct regular n -gons with a large number of sides, but he also made the striking connection between the geometrical properties he encountered and the numerical power of the seemingly unrelated Fermat primes.

The author is not alone in her wonderment over this connection. Gauss's thought provoking theorem has been called one of the most beautiful theorems on Fermat numbers (Křížek, 33) and has been proved in many varied and elegant ways over the centuries. While the original proof due to Gauss is reported to have been over fifty pages in length (187) covering only the forward direction (2), modern mathematical machinery has enabled very concise proofs covering both directions (Grillet, for instance, gives a proof only nine lines in length: Grillet, 260); however, as can be expected, these condensed proofs are fueled by sophisticated thought inherent between the lines of the proofs. The goal of this paper is to distill some of these thoughts into a more digestible manner without suffering the reader to labor through fifty pages of material. Following the line of thought found in the proofs offered in Křížek and Grillet, we will prove Gauss's Theorem with the following outline (let ε be a primitive n th root of unity):

A regular n -gon is constructible \leftrightarrow a primitive n^{th} root of unity, ε , is constructible
 $\leftrightarrow \varepsilon$ is algebraic over \mathbb{Q} with degree a power of 2
 $\leftrightarrow \phi(n) = 2^q$ for some $q \in \mathbb{Z}$
 $\leftrightarrow n = 2^i \prod_{j=0}^l p_j$ where $n \geq 3$, $i \geq 0$, $l \geq 0$, and each p_j
 is a distinct Fermat prime

We begin with the forward direction and subsequently offer the reverse direction; however, in order to simplify the proof slightly for the reader, we present the first biconditional separately as we give a brief summary of geometric constructions.

B. Geometric Constructions and the First Biconditional

As the reader may recall, a Euclidean construction involves using only a straightedge and compass to create various geometric objects (in a plane). Bearing in mind constructions introduced in high school geometry, one may easily construct a perpendicular or parallel line, an angle bisector, and numerous other interesting combinations thereof, yet many students fail to realize that behind each construction is the simple elegance of a finite number of intersections of lines and / or circles. This reality is critical when viewing constructions through the eyes of algebra.

When extending geometric constructions to the realm of algebra, one says that a number $\alpha \in \mathbb{C}$ (in the complex plane) is constructible if and only if one can construct a segment of length $|\alpha|$ taking an arbitrary given length as a single unit. Equivalently, $\alpha = a + bi \in \mathbb{C}$ ($a, b \in \mathbb{R}$) is constructible if and only if a and b are constructible (recall that if $\alpha = a + bi$, then $|\alpha| = \sqrt{a^2 + b^2}$, the length of the hypotenuse of the right triangle with legs a and b). Seeing that if $\alpha, \beta \in \mathbb{C}$ are constructible, then $\alpha + \beta$ and $\alpha - \beta$ are constructible is fairly trivial (indeed, most high school students find this to be a minor task), and noticing that $\alpha\beta$ and α/β (if $\beta \neq 0$) are also constructible only requires a slightly more advanced viewpoint using similar triangles (see figure 1.1 and 1.2 – note that the bold face letters represent the magnitudes of the corresponding complex numbers; \mathbf{a} represents $|\alpha|$, and so forth). From this it follows easily that the set of all

constructible numbers forms a field (indeed, they form a subfield of the complex numbers), planting the constructible numbers firmly within the powerful arms of algebra.

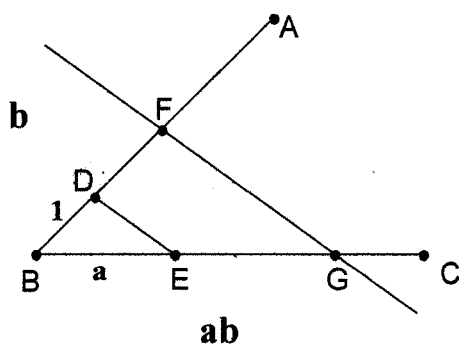


Figure 1.1. Constructing a product.

Construct $BD = 1$, $BF = \mathbf{b}$,
and $BE = \mathbf{a}$ on two sides of an
angle. Construct $FG \parallel DE$.
Then $BG = \mathbf{ab}$ by similarity.

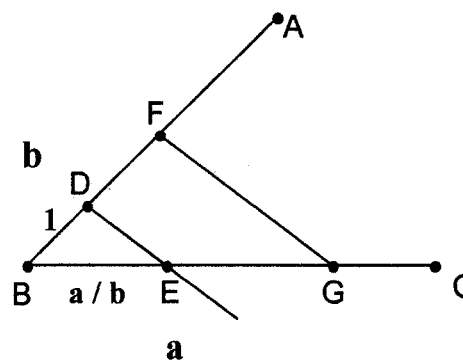


Figure 1.2 Constructing a quotient.

Construct $BD = 1$, $BF = \mathbf{b}$,
and $BG = \mathbf{a}$ on two sides of an
angle. Construct $DE \parallel FG$.
Then $BE = \mathbf{a/b}$ by similarity.

Before looking more closely at the algebraic properties of the constructible numbers (this will be done in the following sections), notice that if a segment of length $\cos(2\pi/n)$ is constructible, then it must be possible to construct the angle $2\pi/n$. To see this, let $\cos(2\pi/n) = a$ be constructible (assume $a \neq 0$ so that we do not have a trivial case); then, to construct the angle in question, make a segment AB of length a and a circle of radius one centered at A ; subsequently, construct the perpendicular to AB at B (call the intersection of the perpendicular with the circle point C), and the desired angle may be easily constructed (by AB and AC) as illustrated in figure 1.3.

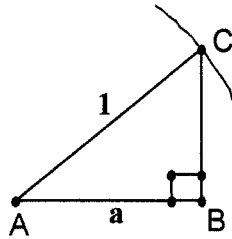


Figure 1.3. Constructing the angle $2\pi/n$.

The converse is similarly true; simply consider the sides of any right triangle formed by a perpendicular to one of the sides of the angle to obtain the two segment lengths and construct their ratio. Thus $\cos(2\pi/n)$ is constructible if and only if the angle $2\pi/n$ is constructible.

Moving forward, if the angle $2\pi/n$ is constructible, then an arbitrary circle can be cut into n congruent arcs (by copying the $2\pi/n$ angle n times from the circle's center, each angle adjacent to the previous angle, and intersecting the rays with the circle, for instance). Connecting the endpoints of these arcs gives n consecutive congruent segments, forming a regular n -gon. Similarly, if the regular n -gon can be constructed, one need only find the center of the n -gon to construct the angle $2\pi/n$ (via two consecutive vertices of the n -gon with the center). In other words, the angle $2\pi/n$ is constructible if and only if the regular n -gon can be constructed. Therefore, a regular n -gon is constructible if and only if $\cos(2\pi/n)$ is constructible.

A similar argument can be made for $\sin(2\pi/n)$, making the number $\cos(2\pi/n) + i \sin(2\pi/n)$, a primitive n^{th} root of unity, constructible if and only if the

regular n -gon is constructible. This shows the first biconditional of our proof: A regular n -gon is constructible \leftrightarrow a primitive n^{th} root of unity, ε , is constructible. We now turn our attention briefly to some background information needed for the forward direction of the remaining biconditionals in the proof.

C. Background Information Needed for the Forward Direction of the Proof

Before moving to the forward direction of the remaining biconditionals in the proof of Gauss's Theorem, we need to establish a key theorem (theorem 1.1), which will give us much needed information. The following theorems and other properties needed to prove theorem 1.1 are usually studied in an undergraduate course of Algebra (for instance, see Fraleigh).

I. **Freshman Theorem:** In a field of characteristic p , $(a+b)^p = a^p + b^p$.

II. **Fermat's Theorem:** If $a \in \mathbb{Z}$, then $a^p \equiv_p a$ for any prime p .

(This is sometimes referred to as a corollary to Fermat's Little Theorem.)

III. Polynomial factorization over a field (and a ring), including irreducible polynomials and uniqueness, is assumed to be familiar to the reader.

IV. The n^{th} Cyclotomic Polynomial:
$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive } n^{\text{th}} \\ \text{root of unity}}} (x - \zeta) \in \mathbb{C}[X]$$

- All roots of $\Phi_n(x)$ are primitive n^{th} roots of unity (by design).
- Any primitive n^{th} root of unity is a root of $\Phi_n(x)$ (also by design).

- $\Phi_n(x)$ is separable over \mathbb{C} (since the primitive n^{th} roots of unity are distinct and have multiplicity one).
- $\Phi_n(x)$ has degree $\phi(n)$ (the number of primitive n^{th} roots of unity).
- $\Phi_n(x)$ is monic with integer coefficients (easily shown by induction).
- $\Phi_n(x) \mid x^n - 1$ (it can be shown that $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$, from which it

follows that $x^n - 1 = \Phi_n(x) \prod_{d \mid n, d < n} \Phi_d(x)$).

- V. Properties of n^{th} roots of unity are assumed to be familiar to the reader; however, key facts are evoked in the following proof.

Theorem 1.1: $\Phi_n(x)$ is irreducible over $\mathbb{Q}[X]$.

Proof: (This proof follows the ideas presented in Grillet, 241, with details added.)

Assume that $\Phi_n(x)$ is not irreducible over $\mathbb{Q}[X]$. Note that the cases for $n = 1$ and $n = 2$ are trivial, so let $n > 2$. Recall that a polynomial factors into a product of two polynomials of lesser degree, say m_1 and m_2 , in $\mathbb{Q}[X]$ if and only if it factors into a product of two polynomials of lesser degree m_1 and m_2 in $\mathbb{Z}[X]$ (since \mathbb{Z} is a UFD and \mathbb{Q} is a field of quotients for \mathbb{Z}), whence $\Phi_n(x)$ is not irreducible over $\mathbb{Z}[X]$ if it is not irreducible over $\mathbb{Q}[X]$. Now, let $q(x) \in \mathbb{Z}[X]$ be an irreducible factor of $\Phi_n(x)$, and let $r(x) \in \mathbb{Z}[X]$ be the corresponding factor. Then $\Phi_n(x) = q(x)r(x)$, and a moment's thought shows that $\deg q, \deg r > 1$ (since if either has degree one, then $\Phi_n(x) = q(x)(x - a)$ or $\Phi_n(x) = (x - b)r(x)$ with $a, b \in \mathbb{Z}$, and the only roots of unity in

\mathbb{Z} are ± 1 , neither of which are primitive if $n > 2$ and, therefore, not a root of $\Phi_n(x)$.

Furthermore, notice that since $\Phi_n(x)$ is monic, the leading coefficients of $q(x)$ and $r(x)$ are ± 1 , and we may arrange that $q(x)$ and $r(x)$ are monic as well.

Now, let ε and $\gamma \in \mathbb{C}$ be roots of $q(x)$ and $r(x)$ respectively. Since $q(x)$ is monic and irreducible over $\mathbb{Q}[X]$, $q(x) = \text{irr}_{\mathbb{Q}}(\varepsilon)$. Furthermore, since $\Phi_n(x) = q(x)r(x)$, it follows that ε and γ are roots of $\Phi_n(x)$, whence they are primitive n^{th} roots of unity (since all the roots of $\Phi_n(x)$ are primitive). We know that all the n^{th} roots of unity form a finite (whence cyclic) multiplicative subfield of \mathbb{C} , which is generated by any primitive n^{th} root of unity, so it follows that $\gamma = \varepsilon^k$ for some $k > 1$ where $\text{gcd}(k, n) = 1$ (otherwise γ will not be a primitive n^{th} root of unity since ε^k is a primitive n^{th} root of unity if and only if $\text{gcd}(k, n) = 1$). Choose ε and γ so that k is as small as possible, and let p be a prime divisor of k . Since $\text{gcd}(k, n) = 1$, and $p \mid k$, it follows that $\text{gcd}(p, n) = 1$, whence ε^p is another primitive n^{th} root of unity and, as such, a root of $\Phi_n(x)$. Now notice that if $p \neq k$ and ε^p is a root of $q(x)$, then $(\varepsilon^p)^{k/p} = \varepsilon^k = \gamma$ shows that γ is a smaller power of another primitive n^{th} root of unity (since $k/p < k$), which contradicts the choice of ε and γ ; therefore, either $k = p$ or ε^p is not a root of $q(x)$. In either case, we see that ε^p must be a root of $r(x)$, for if $k = p$, then we have $\varepsilon^p = \gamma$ (a root of $r(x)$), and if ε^p is not a root of $q(x)$, then it must be a root of $r(x)$ (since it must be a root of one or the other). Finally, since $q(x) = \text{irr}_{\mathbb{Q}}(\varepsilon)$

and ε is a root of $r(x^p)$ (because ε^p is a root of $r(x)$), it follows that $q(x) \mid r(x^p)$ in $\mathbb{Z}[X]$.

We now appeal to the powerful information that p can unlock by turning our focus to the projection $a \mapsto \bar{a}$ of \mathbb{Z} onto the field \mathbb{Z}_p , which induces a homomorphism $f(x) \mapsto \bar{f}(x)$ of $\mathbb{Z}[X]$ onto $\mathbb{Z}_p[X]$. (Recall that if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, then $\bar{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \dots + \bar{a}_0$.) Note that since $q(x)$ and $r(x)$ are monic with $\deg q, \deg r > 1$, it follows that $\deg \bar{q}, \deg \bar{r} > 1$ (the leading coefficient is $\bar{1} \in \mathbb{Z}_p$, so we do not lose the leading power, and the degree stays the same). Let $\deg \bar{r} = m$. Then under the induced homomorphism, $r(x) = x^m + a_{m-1} x^{m-1} + \dots + a_0 \mapsto \bar{r}(x) = x^m + \bar{a}_{m-1} x^{m-1} + \dots + \bar{a}_0$.

Since \mathbb{Z}_p has characteristic p , we may apply the Freshman Theorem:

$$[\bar{r}(x)]^p = \bar{r}^p(x) = (x^m + \bar{a}_{m-1} x^{m-1} + \dots + \bar{a}_0)^p = x^{pm} + \bar{a}_{m-1}^p x^{p(m-1)} + \dots + \bar{a}_0^p$$

Then, by Fermat's Theorem, we have:

$$\begin{aligned} [\bar{r}(x)]^p &= \bar{r}^p(x) = (x^m + \bar{a}_{m-1} x^{m-1} + \dots + \bar{a}_0)^p = x^{pm} + \bar{a}_{m-1}^p x^{p(m-1)} + \dots + \bar{a}_0^p \\ &= (x^p)^m + \bar{a}_{m-1} (x^p)^{m-1} + \dots + \bar{a}_0 = \bar{r}(x^p) \end{aligned}$$

Now, since $q(x) \mid r(x^p)$ in $\mathbb{Z}[X]$, we know that $\bar{q}(x) \mid \bar{r}(x^p) = \bar{r}^p(x)$ in $\mathbb{Z}_p[X]$, whence

$\bar{q}(x)$ and $\bar{r}(x)$ have a common irreducible factor, $\bar{h}(x) \in \mathbb{Z}_p[X]$. Since

$q(x)r(x) = \Phi_n(x) \mid x^n - 1 \in \mathbb{Z}[X]$, it follows that $\bar{q}(x)\bar{r}(x) \mid x^n - \bar{1} \in \mathbb{Z}_p[X]$, whence

$\bar{h}^2(x) \mid x^n - \bar{1} \in \mathbb{Z}_p[X]$ (since $\bar{h}(x)$ is a common irreducible factor of $\bar{q}(x)$ and $\bar{r}(x)$).

Therefore, $x^n - \bar{1}$ has a root of multiplicity greater than one (namely any root of $\bar{h}^2(x)$)

in $\overline{\mathbb{Z}}_p$. However, looking at the formal derivative shows that $x^n - \overline{1}$ does not have multiple roots in $\overline{\mathbb{Z}}_p$ ($(x^n - \overline{1})' = nx^{n-1} \neq 0$ since p does not divide n ; the only root is 0 , which is not a root of $x^n - \overline{1}$). This is a contradiction, so it must be that $\Phi_n(x)$ is irreducible over $\mathbb{Q}[X]$. \square

We have now established the following useful fact. Since $\Phi_n(x)$ is monic and irreducible over $\mathbb{Q}[X]$, for any given primitive n^{th} root of unity, ε , $\Phi_n(x) = \text{irr}_{\mathbb{Q}}(\varepsilon)$. Furthermore, we know that $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \deg(\text{irr}_{\mathbb{Q}}(\varepsilon)) = \deg(\Phi_n(x)) = \phi(n)$.

D. Forward Direction of the Proof

We are now ready to begin the forward direction in verifying Gauss's Theorem, proving the remaining three conditionals. For the remainder of this section, let ε be a primitive n^{th} root of unity.

1. ε is constructible $\rightarrow \varepsilon$ is algebraic over \mathbb{Q} with degree a power of 2:

Rather than encumber the reader with notation, we will proceed through this first piece heuristically. The reader who desires more specific detail may consult an undergraduate text for a proof.

Notice that following the arguments in section B, every rational number is constructible. Thus if K is the smallest field containing the constructible numbers,

then $\mathbb{Q} \leq K$. Clearly if $\varepsilon \in \mathbb{Q}$, the $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 1 = 2^0$. However, if $\varepsilon \in K \setminus \mathbb{Q}$ is constructible, we must show that $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q$ for some $q \in \mathbb{Z}$ ($q \neq 1$).

Now, if we consider the real plane, every point in the plane, (a, b) , is easily constructed if a and b are rational. To construct any other point in the plane, we must intersect two lines, two circles, or a line and circle through our rational points, the equations of which then have rational coefficients. The intersection of two lines with rational coefficients gives another rational point (both coordinates in \mathbb{Q} , a point we already had); however, intersecting a line and a circle with rational points leads to potential new points. If we use substitution to solve the system, as in high school algebra, we may substitute the equation for the line into the equation for the circle, subsequently using the quadratic formula. If the solution for one of the coordinates is

$$x = \frac{c + d\sqrt{e}}{f} \text{ with } c, d, e, f \in \mathbb{Q} \text{ but } \sqrt{e} \notin \mathbb{Q}, \text{ then } x \in K \setminus \mathbb{Q} \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = 2$$

(obviously if \sqrt{e} is a perfect square, then the coordinate is nothing new). The same argument holds for the second coordinate. Lastly, if we intersect two circles, we may condense the solution process by considering one of the circles and the line through the points of intersection in place of the second circle, reducing this case to the one just considered. Therefore, our intersection points will also have coordinates that are either degree 1 (rational) or degree 2 over \mathbb{Q} .

Continuing in this manner will yield similar results at each step. Since subsequent square roots will only potentially increase the degree by a power of 2 (for instance

$[\mathbb{Q}(\sqrt{\sqrt{c}}) : \mathbb{Q}] = 4$), it is clear that for $\varepsilon \in K \setminus \mathbb{Q}$ to be constructible, $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q$ for some $q \in \mathbb{Z}$ ($q \neq 1$). Therefore, if ε is constructible, then ε is algebraic over \mathbb{Q} with degree a power of 2.

Before moving on, notice that if we build our field of constructible numbers by adjoining each new point not found in \mathbb{Q} , then subsequent new points will only have degree 1 or 2 over the field we have built up. In other words, if $\alpha_1, \alpha_2, \dots, \alpha_n$ are the first n constructible points we encounter that are not in \mathbb{Q} , nor in any of the extensions of \mathbb{Q} with previous α_i 's, then $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = 2$, and $[\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_n) : \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n-1})] = 2$, whence $[\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}] = 2^n$. This reinforces the fact that constructing a number reduces to solving a 2^{nd} degree equation with coefficients in an algebraic extension of \mathbb{Q} as defined. This observation will be useful in the reverse direction of this conditional.

2. ε is algebraic over \mathbb{Q} with degree a power of 2 $\rightarrow \phi(n) = 2^q$ for some $q \in \mathbb{Z}$:

Since ε is algebraic over \mathbb{Q} with degree a power of 2, we know $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q$ for some $q \in \mathbb{Z}$. However, we also know that $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \deg(\text{irr}_{\mathbb{Q}}(\varepsilon)) = \phi(n)$ (from part C). Therefore, it follows easily that $\phi(n) = 2^q$ for some $q \in \mathbb{Z}$.

3. $\phi(n) = 2^q$ for some $q \in \mathbb{Z} \rightarrow n = 2^i \prod_{j=0}^l p_j$, where $n \geq 3$, $i \geq 0$, $l \geq 0$, and each p_j is

a distinct Fermat prime:

We now appeal to the multiplicative property of the Euler totient function. Let

$n = 2^i \prod_{j=0}^l p_j^{e_j}$ be the prime factorization of n in \mathbb{Z} (with each p_j a distinct odd prime

and $e_j \geq 1$). We know that $n \geq 3$ (since we began with a constructible n -gon), and

clearly $i \geq 0$ (since n is an integer, we can not have negative exponents) and $l \geq 0$

(depending on whether there are any odd prime factors in n). It remains to show that

$e_j = 1$ and that p_j is a Fermat prime for $0 \leq j \leq l$.

Since $\phi(n)$ is multiplicative, we have:

$$\phi(n) = \phi\left(2^i \prod_{j=0}^l p_j^{e_j}\right) = \phi(2^i) \prod_{j=0}^l \phi(p_j^{e_j})$$

Now, using the fact that $\phi(p^e) = p^{e-1}(p-1)$ for any prime p , we have:

$$\phi(n) = \phi(2^i) \prod_{j=0}^l \phi(p_j^{e_j}) = 2^{i-1}(2-1) \prod_{j=0}^l p_j^{e_j-1}(e_j-1) = 2^{i-1} \prod_{j=0}^l p_j^{e_j-1}(p_j-1)$$

Since we also have $\phi(n) = 2^q$, we now have:

$$2^{i-1} \prod_{j=0}^l p_j^{e_j-1}(p_j-1) = 2^q$$

Since p_j is odd for $0 \leq j \leq l$, this implies that $e_j \leq 1$ for $0 \leq j \leq l$ (or we would have

an odd factor on the left hand side of the equation with no odd factors on the right

hand side of the equation). However, $e_j \geq 1$ and $e_j \leq 1$ implies $e_j = 1$, whence we have:

$$2^{l-1} \prod_{j=0}^l (p_j - 1) = 2^a$$

Now, since $p_j - 1$ is even (p_j is odd), and since there are no odd factors on the right hand side of the equation, this implies that $p_j - 1 = 2^{f_j}$, $f_j \geq 1$ for $0 \leq j \leq l$. Suppose that for some $j \in \{0, 1, \dots, l\}$, $f_j = ab$ for some odd prime b and $a \in \mathbb{Z}$. Then we would have:

$$p_j = 2^{f_j} + 1 = 2^{ab} + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \dots - 2^a + 1)$$

This is a contradiction (p_j is prime), so it must be that f_j does not have any odd prime factors for any j , whence $f_j = 2^{m_j}$ for some $m_j \geq 0$, $0 \leq j \leq l$. Therefore, p_j is a Fermat prime, and we have finished the forward direction of the proof.

E. Background Information Needed for the Reverse Direction of the Proof

Before moving to the reverse direction of the proof, we remind the reader of four key theorems which are usually studied in an undergraduate algebra course (and are therefore presented here without proof). All four theorems are taken from Fraleigh.

First Sylow Theorem: (Fraleigh, 220)

Let G be a finite group with $|G| = p^n m$, where $n \geq 1$ and p does not divide m .

Then:

- a. G contains a subgroup of order p^i for each $1 \leq i \leq n$
- b. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for each $1 \leq i < n$.

Main Theorem of Galois Theory: (468)

Let K be a finite normal extension of a field F , with Galois group $\text{Gal}(K/F)$. For a field E , where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $\text{Gal}(K/F)$ leaving E fixed.

Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $\text{Gal}(K/F)$. The following properties hold for λ :

- a. $\lambda(E) = \text{Gal}(K/E)$
- b. $E = K_{\text{Gal}(K/E)} = K_{\lambda(E)}$
- c. For $H \leq \text{Gal}(K/F)$, $\lambda(E_H) = H$
- d. $[K : E] = |\lambda(E)|$ and $[E : F] = \{ \text{Gal}(K/F) : \lambda(E) \}$, the number of left cosets of $\lambda(E)$ in $\text{Gal}(K/F)$.
- e. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $\text{Gal}(K/F)$. When $\lambda(E) \triangleleft \text{Gal}(K/F)$, then $\text{Gal}(E:F) \cong \frac{\text{Gal}(K/F)}{\lambda(E)}$.
- f. The lattice of subgroups of $\text{Gal}(K/F)$ is the inverted lattice of intermediate fields of K over F .

Theorem 1.2: If $F \leq \bar{G}$ is a splitting field of finite degree over G , then

$$\{F : G\} = |\text{Gal}(F / G)|. \quad (450)$$

Theorem 1.3: If F is a finite field or a field of characteristic zero, then every finite extension G of F is separable, and $\{G : F\} = [G : F]$. (455 and 457)

F. Reverse Direction of the Proof

We are now ready to begin the reverse direction in proving Gauss's Theorem.

1. $n = 2^i \prod_{j=0}^l p_j$, where $n \geq 3$, $i \geq 0$, $l \geq 0$, and each p_j is a distinct Fermat prime

$$\rightarrow \phi(n) = 2^q \text{ for some } q \in \mathbb{Z} :$$

Let n be as given. Then, applying the Euler totient function to n gives:

$$\begin{aligned} \phi(n) &= \phi\left(2^i \prod_{j=0}^l p_j\right) = \phi(2^i) \prod_{j=0}^l \phi(p_j) = 2^{i-1}(2-1) \prod_{j=0}^l p_j^0(p_j-1) \\ &= 2^{i-1} \prod_{j=0}^l 2^{2^{m_j}} = 2^q \text{ where } q = i-1 + \sum_{j=0}^l 2^{m_j} \in \mathbb{Z}. \end{aligned}$$

2. $\phi(n) = 2^q$ for some $q \in \mathbb{Z} \rightarrow \varepsilon$ is algebraic over \mathbb{Q} with degree a power of 2:

Let $\phi(n) = 2^q$ for some $q \in \mathbb{Z}$. We know that any n^{th} root of unity is algebraic over

\mathbb{Q} (since the roots of unity are roots of $\Phi_n(x) \in \mathbb{Q}[X]$). Furthermore, we know

$$[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \deg(\text{irr}_{\mathbb{Q}}(\varepsilon)) = \deg(\Phi_n(x)) = \phi(n) \text{ (see part C), so we have}$$

$$[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q.$$

3. ε is algebraic over \mathbb{Q} with degree a power of 2 $\rightarrow \varepsilon$ is constructible:

Now let $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q$ for some $q \in \mathbb{Z}$. We shall take advantage of this information in two ways. First notice that it is fairly straightforward to see that $\mathbb{Q}(\varepsilon)$ is a splitting field of $\Phi_n(x)$, and since $[\mathbb{Q}(\varepsilon) : \mathbb{Q}]$ is finite, it follows by theorem 1.2 that $|\{\mathbb{Q}(\varepsilon) : \mathbb{Q}\}| = |\text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})|$. Then, by theorem 1.3, since $\text{char}(\mathbb{Q}) = 0$, we also know that $|\{\mathbb{Q}(\varepsilon) : \mathbb{Q}\}| = [\mathbb{Q}(\varepsilon) : \mathbb{Q}]$. Putting these two pieces of information together, we have:

$$|\text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})| = \{\mathbb{Q}(\varepsilon) : \mathbb{Q}\} = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q$$

Now, since $|\text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})| = 2^q$, we may apply the First Sylow Theorem to see that $\text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ contains a subgroup of order 2^i for $1 \leq i < q$, every such subgroup being a normal subgroup of a subgroup of order 2^{i+1} :

$$\{0\} = H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_q = \text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$$

Finally, notice that since $\mathbb{Q}(\varepsilon)$ is a finite normal extension of \mathbb{Q} (it is a finite separable splitting field over \mathbb{Q}), we may apply the Main Theorem of Galois Theory to see there exists a corresponding chain of subfields of $\mathbb{Q}(\varepsilon)$:

$$\mathbb{Q} = \mathbb{Q}_0 \leq \mathbb{Q}_1 \leq \dots \leq \mathbb{Q}_q = \mathbb{Q}(\varepsilon).$$

Now, since $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2^q$ and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon) : \mathbb{Q}_{q-1}][\mathbb{Q}_{q-1} : \mathbb{Q}_{q-2}] \dots [\mathbb{Q}_1 : \mathbb{Q}]$, we have $[\mathbb{Q}_i : \mathbb{Q}_{i-1}] = 2$ for $1 \leq i \leq q$. However, this is equivalent to saying that every real positive number in \mathbb{Q}_i can be constructed with a straightedge and compass from

elements of \mathbb{Q}_{i-1} ($1 \leq i \leq q$) since each has degree 2 (recall that constructing a number reduces to solving a 2nd degree equation with coefficients in an algebraic extension of \mathbb{Q} as discussed in the forward direction of this conditional). Therefore ε is constructible (since $\varepsilon \in \mathbb{Q}(\varepsilon)$). \square

G. Illustrations

The reader may find it interesting that while there are thirty-one known constructible n -gons with odd number of sides, there are twenty-four constructible n -gons with number of sides between three and 100 ($n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, \text{ and } 96$), and both sets of constructible n -gons quickly begin to resemble a circle (which is not surprising). Indeed, this is true even as early as the sixth constructible n -gon (with number of sides between three and 100), the decagon, as seen in figure 1.4.

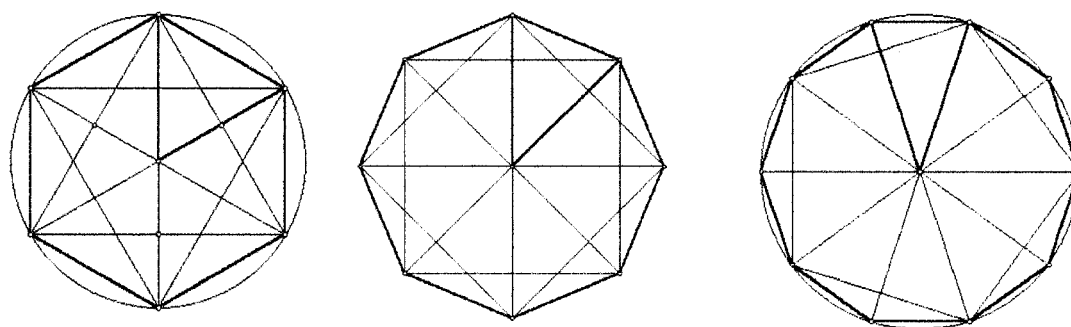


Figure 1.4. Three regular n -gons constructed with Geometer's Sketchpad ($n = 6, 8, 10$).

Application Two: Heron Triangles

A. Introduction

When the author was choosing her thesis topic, she was particularly interested in choosing a topic that united her first two loves in math: abstract algebra and number theory. What she discovered, as seen in the prior section, was that there is also a surprising connection between these two fields of study and geometry. In this section, we take a look at a second case that unites these three mathematical areas in a beautiful harmony, interweaving a very special kind of Heron triangle with the power unleashed by Fermat primes. We begin with a brief history and review of properties of Heron triangles (triangles with integral sides and areas) before focusing on the main theorem of this section. Attention is also given to the classical parameterization of Pythagorean triples for the reader who is not familiar with (or who wants a refresher about) this process as well as specific theorems and a key lemma that serve as useful tools in our quest toward proving the following theorem, which was discovered by Florian Luca:

Theorem 2.1: If $a \geq b \geq c$ are the lengths of the sides of a Heron triangle, and all three are powers of primes, then either $(a, b, c) = (5, 4, 3)$ or, for some integer $m \geq 1$ with F_m a Fermat prime, $(a, b, c) = (F_m, F_m, 4(F_{m-1} - 1))$.

B. Preliminary Information About Heron Triangles

Before discussing the general properties of Heron triangles, it is fitting to place them in their historical context. Heron triangles are, naturally, named after Heron of Alexandria who is credited with their recognition. Although no one knows for sure when Heron lived (most scholars place his life around 70 AD based upon a reference to an eclipse – believed to have occurred on March 13, 62 AD – in one of Heron’s books), there is considerable agreement that Heron was an imaginative inventor and a creative mathematician. While Heron’s books document nearly eighty ingenious inventions, perhaps his most famous work is the formula $A = \sqrt{s(s-a)(s-b)(s-c)}$ for the area of a triangle, although the authorship has been questioned. Heron presented this formula in the same book (*Metrica*) in which he gave a method, known by the Babylonians almost 2000 years earlier, for approximating square roots. The author found this interesting since the connection suggests that Heron may have been intrigued by Babylonian mathematics or, at the very least, that Babylonian advances were known to him. Since the Babylonians had numerous cuneiform tablets listing integral Pythagorean triples, could it be that Heron studied this and asked the obvious questions? Are there non-right triangles with special properties related to the sides? If so, what properties can one generalize? If one considers the fact that the Egyptians were fiercely reluctant to deal with irrational numbers, it would be only natural for Heron to look for situations that dealt with rational numbers (which, of course, can be transferred to an integral arena). Perhaps Heron did not ask these questions, but the thoughts that led Heron to his famous

triangles could not have been too far from this, and the results of the initial investigation have reached far into the future, landing firmly in the lap of modern math and raising additional questions along the way. We shall now take a look at the properties of Heron's triangles before advancing to a modern application.

One may recall that a Heron triangle is a triangle in which the area and all three sides of the triangle are integers. Notice that this definition alone does not place restrictions upon the class of the triangle. In other words, the triangle may be acute, obtuse or right. For example, consider the three triangles in figure 2.1.

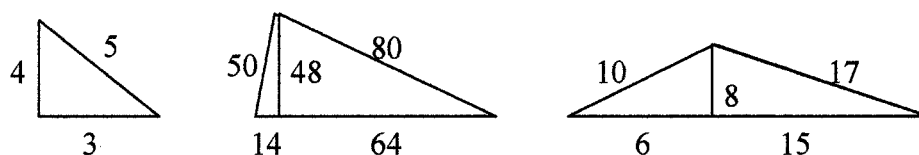


Figure 2.1. Illustrations of right, acute, and obtuse Heron Triangles (not to scale).

One can easily verify that each triangle pictured exists (the triples corresponding to the appropriate right triangles are Pythagorean triples) and that the triangles' sides and areas are all integers. Furthermore, while the first triangle is clearly a right triangle, the law of cosines quickly reveals that the second triangle is acute (obviously both base angles are acute since they are inside a right triangle, so only the top angle need be checked). The third triangle is similarly seen to be obtuse. Although it is believed that Heron was interested only in non-right triangles in his work with these very intriguing triangles, the theorem being considered in this section clearly allows for a right triangle to occur.

While the reader may have used the traditional formula for the area of a triangle ($A = bh/2$) to verify that the areas of the above triangles are indeed integers, Heron's well known formula for the area of a triangle is useful for obtaining further information about the sides of a Heron triangle. Recall that $A = \sqrt{s(s-a)(s-b)(s-c)}$, where $s = (a+b+c)/2$ is the semiperimeter of the triangle. Notice that since the area is an integer, this forces s to be an integer as well. To see this, assume that $a+b+c$ is odd (so that $s \notin \mathbb{Z}$). Then either all three lengths are odd, or two are even and one is odd. A moment's thought shows that $s-a = (b+c-a)/2$, where $b+c-a$ is odd in either case. Similarly $a+c-b$ and $a+b-c$ are odd, but this leads to:

$$\sqrt{s(s-a)(s-b)(s-c)} = \sqrt{(1/16)(\text{odd})} \notin \mathbb{Z}$$

whence $A \notin \mathbb{Z}$ ($\rightarrow\leftarrow$). Therefore, $s \in \mathbb{Z}$. Furthermore, it follows that $a+b+c$ is even with all three lengths of the sides of a Heron triangle even, or two odd and one even.

Building upon this information about the nature of the lengths of the sides of a Heron triangle, another useful fact about the lengths emerges as a result of the area being an integer: $\min(a,b,c) \geq 3$. This is easily seen as follows:

Suppose the minimum value is 1, say $a=1$. Then b and c must have opposite parity. If $b=2k+1$ and $c=2n$ for some $k,n \in \mathbb{Z}$, then by the Triangle Inequality:

$$b-a < c < b+a \Rightarrow 2k < 2n < 2k+2, \text{ or } k < n < k+1 \text{ } (\rightarrow\leftarrow).$$

On the other hand, if the minimum value is 2, say $a=2$, then b and c must have the same parity. If both are odd, then $b=2k+1$ and $c=2n+1$ for some $k,n \in \mathbb{Z}$, and we have:

$$b-a < c < b+a \Rightarrow 2k-1 < 2n+1 < 2k+3, \text{ or } k < n+1 < k+2$$

However, this forces $k+1 = n+1$, so $k = n$. Consequently, we know $s = 2k + 2$, $s - a = 2k$, and $s - b = s - c = 1$, whence we have $A = \sqrt{(2k+2)(2k)} = 2\sqrt{k(k+1)} \notin \mathbb{Z}$ since the product of two consecutive integers is not a perfect square. $\rightarrow\leftarrow$

Similarly, if b and c are both even, then $b = 2^k n$ and $c = 2^j m$ for some $k, n, m, j \in \mathbb{Z}$ where $k \geq 1, j \geq 1$, and $\gcd(2, n) = \gcd(2, m) = 1$, and we have:

$$\begin{aligned} b - a < c < b + a &\Rightarrow 2^k n - 2 < 2^j m < 2^k n + 2 \\ 2^{k-1} n - 1 < 2^{j-1} m < 2^{k-1} n + 1 \\ 2^{k-1} n < 2^{j-1} m + 1 < 2^{k-1} n + 2 \end{aligned}$$

However, this forces $2^{k-1} n + 1 = 2^{j-1} m + 1$, or $k = j$ and $n = m$. Therefore, $a = 2$ and $b = c = 2^k n$, whence $s = 2^k n + 1$, $s - a = 2^k n - 1$, and $s - b = s - c = 1$. Thus

$$A = \sqrt{(2^k n - 1)(2^k n + 1)} = \sqrt{(2^k n)^2 - 1} \notin \mathbb{Z} \text{ since two squares cannot differ by one. } \rightarrow\leftarrow$$

Therefore, $\min(a, b, c) \geq 3$.

The last observation about Heron triangles, presented here with proof, is the first that places a restriction on the class of the triangle.

Theorem 2.2: A Heron triangle is isosceles if and only if the base, c , is even, the altitude

to c (h_c) is an integer, and a , h_c , and $c/2$ form a Pythagorean triple.

Proof: Let $\triangle ABC$ be a Heron triangle with h_c the altitude to side c .

\Rightarrow : Let $a = b$. Then $s = (2a + c)/2 = a + (c/2) \in \mathbb{Z}$ implies that $c/2 \in \mathbb{Z}$

(since $s, a \in \mathbb{Z}$). Thus $2 \mid c$ and c is even. Now, since the altitude of an

isosceles triangle is also a median, the foot of h_c divides c in half, so by

the Pythagorean Theorem, we have $a^2 = h_c^2 + (c/2)^2$ or

$h_c^2 = a^2 - (c/2)^2 \in \mathbb{Z}$. If $h_c \in \mathbb{R} \setminus \mathbb{Q}$, then $A = (c/2)h_c \notin \mathbb{Z}$ ($\rightarrow \leftarrow$), so

$h_c \in \mathbb{Q}$. However, if $h_c \in \mathbb{Q} \setminus \mathbb{Z}$, then $h_c^2 \notin \mathbb{Z}$ ($\rightarrow \leftarrow$). Therefore, $h_c \in \mathbb{Z}$,

and a , h_c , and $c/2$ form a Pythagorean triple.

\Leftarrow : Now let the base, c , be even, the altitude to c (h_c) be an integer, and a , h_c , and $c/2$ form a Pythagorean triple. We consider two different cases for the triangle in question: whether h_c lies within or without the triangle (notice that h_c cannot be a side of the triangle, for if it were a side of the triangle, then it would be a right triangle and $h_c = b$; however, it is not possible for both (a, b, c) and $(a, b, c/2)$ to be right triangles).

1. Let h_c lie within the triangle:

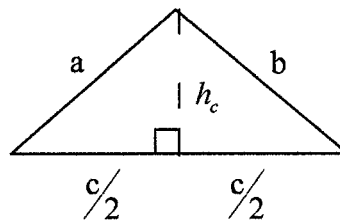


Figure 2.2. A triangle with altitude inside the triangle.

This case is trivial. First notice that h_c is the median (since h_c lies within the triangle and clearly bisects c given that a , h_c , and $c/2$ form a Pythagorean triple). Thus h_c is

simultaneously a median and an altitude, whence $\triangle ABC$ is an isosceles triangle (a standard result from high school geometry).

2. Let h_c lie without the triangle:

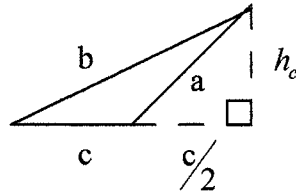


Figure 2.3. A triangle with altitude outside the triangle.

This case is far more complex. For the theorem in question to be true, one can easily see that this case must be impossible, but proving this is not so easy. After numerous failed attempts to prove this result through contradiction, and without success in locating documentation, the author of “Fermat Primes and Heron Triangles with Prime Power Sides” (the journal article inspiring this section) was consulted. Dr. Florian Luca was most generous in outlining a proof, the details of which were carefully checked by the author of this thesis; however, the manipulations stray from the focus of this paper and may be cumbersome to the reader. Therefore, the initial setup followed by a general explanation of the remaining procedure is given here in place of the finer details.

To begin, notice that in this case $b > a, c$. Since h_c lies without the triangle, we can consider the two different right triangles that are formed by h_c and $\triangle ABC$ (see figure 2.3).

From the outer triangle we obtain:

$$b^2 = h_c^2 + (3c/2)^2$$

Similarly, from the inner triangle, we have:

$$a^2 = h_c^2 + (c/2)^2$$

Multiplying these two equations gives:

$$[(h_c^2 + (c/2)^2)][h_c^2 + (3c/2)^2] = (ab)^2$$

Manipulating this equation yields:

$$\left(\frac{h_c}{c/2}\right)^4 + 10\left(\frac{h_c}{c/2}\right)^2 + 9 = \frac{(ab)^2}{(c/2)^4}$$

At this point, the first of several changes of variables is used.

Letting $X = \frac{h_c}{c/2}$ and $Y = \frac{ab}{(c/2)^2}$, the elliptic curve

$X^4 + 10X^2 + 9 = Y^2$ emerges, offering a foundation for

resolution. The answer to whether or not the triangle configuration in question exists lies in the number of solutions to this particular elliptic curve. In order to answer this question, a series of changes of variables is used to transform

the equation into a form that has been studied. In particular,

$X^4 + 10X^2 + 9 = Y^2$ can be written as:

$$U^2 = Z^3 - 27(208)Z - 56(2240)$$

At this point, one appeals to Kraus's existence conditions for such an elliptic curve (see Cremona, 63). Performing the required calculations reveals that the elliptic curve in question has a reduced equation:

$$y^2 = x^3 + x^2 - 4x - 4$$

Happily, this curve has been studied, and the Mordell Weil group of the points on the curve is finite (it has only four elements). In fact, all four points lead to $X = 0$ (after tracing back through the changes of variables), whence $h_c = 0$ ($\rightarrow\leftarrow$). Therefore, h_c cannot lie without the triangle.

Putting all of the above together, we have shown that $\triangle ABC$ is an isosceles triangle. \square *

C. Classical Parameterization of Pythagorean Triples

Since this topic is used repeatedly in this section, the author felt it necessary to include information about the classical parameterization for the reader who is less familiar with this well known process. (The parameterization follows the author's class notes, with a few details added.)

To begin, let (a, b, c) represent the integral sides of a right triangle where $a^2 + b^2 = c^2$ (for convenience of calculation we shall assume all values are positive, which is also intuitively desirable since they are sides of a triangle, but in theory, Pythagorean triples can be negative numbers as well). The triple is said to be a primitive triple if the three have no common factor ($\gcd(a, b, c) = 1$). When we have a primitive triple, it is also pairwise relatively prime, for if two of the numbers, say a and b , have a common factor with $\gcd(a, b) = d \neq 1$, then:

$$\left. \begin{array}{l} d \mid a \rightarrow d^2 \mid a^2 \\ d \mid b \rightarrow d^2 \mid b^2 \end{array} \right\} \rightarrow d^2 \mid a^2 + b^2 = c^2 \rightarrow d \mid c \quad \rightarrow \leftarrow$$

(then d is a common factor of a , b , and c)

From this it is easy to see that not all three can be even (not primitive), nor can exactly two of them be even (not pairwise relatively prime). Similarly, it is not possible that a and b are both odd, for if both are odd, then $a = 2k_1 + 1$ and $b = 2k_2 + 1$ for some $k_1, k_2 \in \mathbb{Z}^+$, and we have:

$$a^2 + b^2 = (2k_1 + 1)^2 + (2k_2 + 1)^2 = 4(k_1^2 + k_2^2 + k_1 + k_2) + 2$$

Therefore, $a^2 + b^2 \equiv_4 2$, which implies that $a^2 + b^2$ is not a perfect square (since the remainder of any squared integer when divided by 4 is 0 or 1), but $a^2 + b^2 = c^2$. $\rightarrow \leftarrow$

From this it follows that exactly one of a and b is even, whence c is odd.

Without loss of generality, let a be even and b and c be odd. Then

$$a^2 = c^2 - b^2 = (c + b)(c - b) \text{ with } c + b \text{ and } c - b \text{ both even. Let } c + b = 2u \text{ and}$$

$$c - b = 2v \text{ for some } u, v \in \mathbb{Z}^+. \text{ Then } c = 2(u + v)/2 = u + v \text{ and } b = 2(v - u)/2 = v - u.$$

Since $b > 0$, it must be that $v > u$. Furthermore, since $\gcd(b, c) = 1$, it follows that $\gcd(u + v, v - u) = 1$, whence $\gcd(u, v) = 1$. From this it follows that u and v cannot be simultaneously even (since $\gcd(u, v) = 1$) or odd (since $\gcd(u + v, u - v) = 1$).

Returning to the fact that $c + b$ and $c - b$ are both even, we can see that

$$\left(\frac{a}{2}\right)^2 = \left(\frac{c+b}{2}\right)\left(\frac{c-b}{2}\right) = uv, \text{ from which it follows that } u \text{ and } v \text{ are perfect squares (since}$$

u and v are relatively prime, and their product gives a square, each of the prime factors in the square had to come from either u or v). Let $v = m^2$ and $u = n^2$ for some $m, n \in \mathbb{Z}^+$.

Then a similar argument to the above shows that m and n cannot be simultaneously even or odd, and because $v > u$, it follows that $m > n$. Putting all of this together gives:

$$\left(\frac{a}{2}\right)^2 = uv = n^2 m^2 \rightarrow a = 2mn, \quad b = v - u = m^2 - n^2, \quad \text{and} \quad c = v + u = m^2 + n^2$$

Therefore, if (a, b, c) is a primitive Pythagorean triple, then one obtains the parameterization of two relatively prime integers m and n with $m > n$, exactly one of which is odd, such that $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$. The converse also holds, providing a convenient method for finding Pythagorean triples. Before proceeding, it is interesting to note that if the restrictions on m and n are not met, one still finds a Pythagorean triple, but it will not be primitive. For example, let $m = 4$ and $n = 2$. Then $(a, b, c) = (16, 12, 20)$, a relative of the primitive triple $(4, 3, 5)$.

D. Some Important Theorems and a Key Lemma

Before moving to the proof of the main theorem mentioned in section A, we recall a few important theorems from number theory (most presented without proof) and establish a lemma that will prove to be useful. Theorems 2.3 through 2.9, along with the definitions for quadratic residue and the Legendre symbol, were taken from Long or were encountered during the author's undergraduate study of number theory; hence, the reader is assumed to be familiar with the concepts (a proof is provided for theorem 2.9 for the less familiar reader). The author first examined Theorem 2.10, Catalan's Conjecture, and Lemma 2.1 when investigating the original journal article. Therefore, the author has provided a proof for theorem 2.10 and filled in details of the proof for lemma 2.1.

Theorem 2.3: If $p^n \mid ab$, and $\gcd(p^n, a) = 1$, then $p^n \mid b$.

Theorem 2.4: If $a \mid c$ and $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.

Theorem 2.5: If $a \equiv_{p^m} b$, then $a \equiv_{p^n} b$ for any integer n such that $0 < n \leq m$.

Theorem 2.6: If $a^2 \equiv_{n^2} 0$, then $a \equiv_n 0$.

Theorem 2.7: If $a^2 = b^2c$, then $c = k^2$ for some $k \in \mathbb{Z}$.

Quadratic Residue: If $x^2 \equiv_p n$, where p is an odd prime and $\gcd(p, n) = 1$, is solvable,

then n is a quadratic residue mod p .

Note that if n is not a quadratic residue, it is called a quadratic nonresidue.

Theorem 2.8: The only quadratic residues mod 4 are 0 and 1.

Legendre Symbol: For any odd prime p and integer n with $(n, p) = 1$, let:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue mod } p \\ -1 & \text{if } n \text{ is a quadratic nonresidue mod } p \end{cases}$$

Euler's Criterion: For any odd prime p and $n \in \mathbb{Z}$ with $\gcd(n, p) = 1$, $\left(\frac{n}{p}\right) \equiv_p n^{(p-1)/2}$.

Theorem 2.9: If p is a prime such that $p \equiv_4 3$, then -1 is not a quadratic residue mod p .

Proof: Let $p \equiv_4 3$. Then $p = 3 + 4k$ for some $k \in \mathbb{Z}$, and by Euler's Criterion:

$$\left(\frac{-1}{p}\right) \equiv_p (-1)^{(p-1)/2} = (-1)^{(3+4k-1)/2} = (-1)^{2(2k+1)/2} = (-1). \quad \square^*$$

Theorem 2.10: If $2^n + 1 \in \mathbb{N}$ is prime, then $n = 2^m$ for some $m \in \mathbb{W}$.

Proof: Let $2^n + 1 \in \mathbb{N}$ be prime. Then $n = jk$ for some $j, k \in \mathbb{N}$ where $\gcd(k, 2) = 1$ (in other words, all the factors of 2 are in j), and $k > 1$ (otherwise we are done), and we have:

$$2^n + 1 = 2^{jk} + 1 = (2^j + 1)(2^{j(k-1)} - 2^{j(k-2)} + \dots - 2^j + 1) \quad (\rightarrow\leftarrow). \quad \square^*$$

Catalan's Conjecture: The equation $a^n - b^m = 1$ has no positive integer solutions for $n, m > 1$ except when $a = m = 3$ and $b = n = 2$.

NOTE: This conjecture is still open, but the case with m even has been proved by V.A. Lebesgue (Luca, 47).

Lemma 2.1: Assume that a , b , and c are lengths of the sides of a Heron triangle such that

$p^\alpha \parallel a$ for some positive integer α and some prime p where $p = 2$ or

$p \equiv_4 3$. If $p = 2$, then $p^{\alpha+1} \mid \gcd((b^2 - c^2), 4A)$, and if $p \equiv_4 3$, then

$p^\alpha \mid \gcd((b^2 - c^2), A)$.

Proof: (The author has followed Luca's proof with significant details added.)

Let a , b , and c be lengths of the sides of a Heron triangle, and let p be a prime

such that $p^\alpha \parallel a$ for some positive integer α . We have two cases to consider.

Case 1: Let $p = 2$. (This case is similar to case two, and is omitted in the original article,

but is included here for sake of completeness). From Heron's formula, we know

that $A^2 = s(s-a)(s-b)(s-c)$, so using the fact that $s = (a+b+c)/2$, it follows

that we have:

$$A^2 = \frac{a+b+c}{2} \cdot \frac{-a+b+c}{2} \cdot \frac{a-b+c}{2} \cdot \frac{a+b-c}{2}$$

$$16A^2 = (a+b+c)(-a+b+c)(a-b+c)(a+b-c)$$

$$(4A)^2 = (-a^2 + b^2 + 2cb + c^2)(a^2 - b^2 + 2cb - c^2)$$

$$(4A)^2 = -a^4 + 2a^2b^2 + 2a^2c^2 - b^4 + 2b^2c^2 - c^4$$

$$(4A)^2 = 2a^2(b^2 + c^2) - a^4 - (b^2 - c^2)^2$$

Now, since $p^\alpha = 2^\alpha \parallel a$, we know $2^{2\alpha} \parallel a^2$. Furthermore, since a is even, we

know b and c have the same parity, whence $b^2 + c^2$ will be even. Therefore, we

know $2^{2(\alpha+1)} \mid 2a^2(b^2 + c^2)$. In addition, $2^{2\alpha} \parallel a^2 \rightarrow 2^{2(\alpha+1)} \mid a^4$, so the equation above becomes:

$$-(b^2 - c^2)^2 \equiv_{2^{2(\alpha+1)}} (4A)^2$$

If $2^{\alpha+1} \mid (b^2 - c^2)$, then $2^{\alpha+1} \mid 4A$ since $0 \equiv_{2^{2(\alpha+1)}} (4A)^2$ implies $0 \equiv_{2^{\alpha+1}} 4A$

by Theorem 2.6. But then $2^{\alpha+1}$ is a common divisor of $b^2 - c^2$ and $4A$, whence $2^{\alpha+1} \mid \gcd((b^2 - c^2), 4A)$. So we have only to consider the case when $2^{\alpha+1} \nmid (b^2 - c^2)$ to finish the proof.

Assume that $2^{\alpha+1} \nmid (b^2 - c^2)$. Then $2^\delta \parallel (b^2 - c^2)$ for some nonnegative

$\delta \in \mathbb{Z}$ where $\delta \leq \alpha$, and we have:

$$\begin{aligned} (4A)^2 \equiv_{2^{2(\alpha+1)}} -(b^2 - c^2)^2 &\rightarrow (4A)^2 = -(b^2 - c^2)^2 + 2^{2(\alpha+1)} k_1 \text{ for some } k_1 \in \mathbb{Z} \\ &\rightarrow (4A)^2 = -(b^2 - c^2)^2 + 2^{2\delta} (2^{2(\alpha+1-\delta)} k_1) \end{aligned}$$

and

$$2^\delta \parallel (b^2 - c^2) \rightarrow b^2 - c^2 = 2^\delta k_2 \text{ for some } k_2 \in \mathbb{Z}.$$

Putting these together, we obtain:

$$(4A)^2 = -(2^\delta k_2)^2 + 2^{2\delta} (2^{2(\alpha+1-\delta)} k_1) = 2^{2\delta} (2^{2(\alpha+1-\delta)} k_1 - k_2^2)$$

which shows that $2^{2\delta} \mid (4A)^2$, whence $2^\delta \mid (4A)$ and $\left(\frac{4A}{2^\delta}\right)^2 = k_3^2$ for $k_3 \in \mathbb{Z}$

where $k_3^2 = 2^{2(\alpha+1-\delta)} k_1 - k_2^2$ (we know $2^{2(\alpha+1-\delta)} k_1 - k_2^2$ is a perfect square by

Theorem 2.7). Similarly, since $2^\delta \parallel (b^2 - c^2)$, we know $\left(\frac{b^2 - c^2}{2^\delta}\right)^2 = k_2^2$.

Therefore, if $-(b^2 - c^2)^2 \equiv_{2^{2(\alpha+1)}} (4A)^2$, then we have:

$$-\left(\frac{b^2 - c^2}{2^\delta}\right)^2 \equiv_{2^{2(\alpha+1-\delta)}} \left(\frac{4A}{2^\delta}\right)^2 \rightarrow -k_2^2 \equiv_{2^{2(\alpha+1-\delta)}} k_3^2$$

Now, in the finite ring $\mathbb{Z}_{2^{2(\alpha+1)}}$ every element that is relatively prime to $2^{2(\alpha+1)}$ has a multiplicative inverse, and since $\gcd(2, k_2) = 1$, we know $k_2 \not\equiv_{2^{2(\alpha+1)}} 0$ (whence $k_2^2 \not\equiv_{2^{2(\alpha+1)}} 0$ and, subsequently, $k_3^2 \not\equiv_{2^{2(\alpha+1)}} 0$), so we have:

$$-1 \equiv_{2^{2(\alpha+1)}} k_3^2 k_2^{-2} = (k_3 k_2^{-1})^2$$

We know that $\alpha \geq 1$ (by hypothesis), so $2^2 < 2^{2(\alpha+1)}$, and the above congruence can be reduced to $-1 \equiv_4 (k_3 k_2^{-1})^2$ (by Theorem 2.5), which is a contradiction (the only quadratic residues mod 4 are 0 and 1 – Theorem 2.8). Therefore, it must be that $2^{\alpha+1} \mid (b^2 - c^2)$, which we have already seen leads to $2^{\alpha+1} \mid \gcd((b^2 - c^2), 4A)$.

Case 2: Let $p \equiv_4 3$. (Note that $\gcd(p^\alpha, 4) = 1$.) As in case one, Heron's formula gives us

$$(4A)^2 = 2a^2(b^2 + c^2) - a^4 - (b^2 - c^2)^2. \text{ Now, since } p^\alpha \parallel a, \text{ we know } p^{2\alpha} \parallel a^2, \text{ so}$$

the equation above implies:

$$-(b^2 - c^2)^2 \equiv_{p^{2\alpha}} (4A)^2$$

If $p^\alpha \mid (b^2 - c^2)$, then $p^\alpha \mid A$ (since $0 \equiv_{p^{2\alpha}} (4A)^2$ implies $0 \equiv_{p^\alpha} 4A$ as before,

whence, by Theorem 2.3, $0 \equiv_{p^\alpha} A$ since $\gcd(p^\alpha, 4) = 1$). But then p^α is a

common divisor of $b^2 - c^2$ and A , whence $p^\alpha \mid \gcd((b^2 - c^2), A)$. So we have only to consider the case when $p^\alpha \nmid (b^2 - c^2)$ to finish the proof.

Assume that $p^\alpha \nmid (b^2 - c^2)$. Then $p^\delta \parallel (b^2 - c^2)$ for some nonnegative $\delta \in \mathbb{Z}$ where $\delta < \alpha$, and we have:

$$\begin{aligned} (4A)^2 &\equiv_{p^{2\alpha}} -(b^2 - c^2)^2 \rightarrow (4A)^2 = -(b^2 - c^2)^2 + p^{2\alpha}k_1 \text{ for some } k_1 \in \mathbb{Z} \\ &\rightarrow (4A)^2 = -(b^2 - c^2)^2 + p^{2\delta}(p^{2(\alpha-\delta)}k_1) \end{aligned}$$

and

$$p^\delta \parallel (b^2 - c^2) \rightarrow b^2 - c^2 = p^\delta k_2 \text{ for some } k_2 \in \mathbb{Z}.$$

Putting these together, we obtain:

$$(4A)^2 = -(p^\delta k_2)^2 + p^{2\delta}(p^{2(\alpha-\delta)}k_1) = p^{2\delta}(p^{2(\alpha-\delta)}k_1 - k_2^2)$$

which shows that $p^{2\delta} \mid (4A)^2$, whence $p^\delta \mid (4A)$ and $\left(\frac{4A}{p^\delta}\right)^2 = k_3^2$ for $k_3 \in \mathbb{Z}$

where $p^{2(\alpha-\delta)}k_1 - k_2^2 = k_3^2$ (we know $p^{2(\alpha-\delta)}k_1 - k_2^2$ is a perfect square by

Theorem 2.7). Similarly, since $p^\delta \parallel (b^2 - c^2)$, we know $\left(\frac{b^2 - c^2}{p^\delta}\right)^2 = k_2'^2$.

Therefore, if $-(b^2 - c^2)^2 \equiv_{p^{2\alpha}} (4A)^2$, then we have:

$$-\left(\frac{b^2 - c^2}{p^\delta}\right)^2 \equiv_{p^{2(\alpha-\delta)}} \left(\frac{4A}{p^\delta}\right)^2 \rightarrow -k_2'^2 \equiv_{p^{2(\alpha-\delta)}} k_3^2 \rightarrow -k_2'^2 \equiv_p k_3^2$$

Now, in the finite field \mathbb{Z}_p every nonzero element has a multiplicative inverse, and since $\gcd(p, k_2) = 1$, we know $k_2 \not\equiv_p 0$ (whence $k_2^2 \not\equiv_p 0$ and, subsequently, $k_3^2 \not\equiv_p 0$), so we have:

$$-1 \equiv_p k_3^2 k_2^{-2} = (k_3 k_2^{-1})^2 \rightarrow \leftarrow (-1 \text{ is not a quadratic residue since } p \equiv_4 3)$$

Therefore, it must be that $p^\alpha \mid (b^2 - c^2)$ whence $(4A)^2 \equiv_{p^{2\alpha}} 0$, so $p^\alpha \mid A$. Now, as before, p^α is a common divisor of $b^2 - c^2$ and A , and $p^\alpha \mid \gcd((b^2 - c^2), A)$. \square

We are now equipped to prove the main theorem of this section.

E. Proving the Main Theorem

Recall that the primary theorem being considered in this section is the following:

Theorem 2.1: If $a \geq b \geq c$ are the lengths of the sides of a Heron triangle, and all three are powers of primes, then either $(a, b, c) = (5, 4, 3)$ or, for some integer $m \geq 1$ with F_m a Fermat prime, $(a, b, c) = (F_m, F_m, 4(F_{m-1} - 1))$.

The author has followed Luca's approach in proving this theorem, yet some reorganizing has been done in order to fill significant gaps found in the original proof.

Proof: Let a, b , and c (without ordering initially) be lengths of the sides of a Heron triangle such that all three are powers of primes. Then there are two cases we must consider: isosceles and non-isosceles triangles.

Case 1: Let the triangle be isosceles, so let $a = b$ (we can do so without loss of generality since we can rename the vertices if need be). Then note that c must be even (since either all are even or two are odd and one is even). Thus we can designate $a = p^\alpha = b$ and $c = 2^\beta$ for some $\alpha, \beta \in \mathbb{Z}^+$. Note that $\beta \geq 2$ (since $\min(a, b, c) \geq 3$). Now, since the triangle is isosceles, we have (with h_c being the altitude to side c):

$$a^2 = h_c^2 + (c/2)^2 \rightarrow p^{2\alpha} = h_c^2 + 2^{2(\beta-1)}$$

At this point we consider whether $p = 2$ or $p > 2$.

$p = 2$: If $p = 2$, then $p^{2\alpha} = h_c^2 + 2^{2(\beta-1)}$ becomes:

$$2^{2\alpha} = h_c^2 + 2^{2(\beta-1)} \rightarrow h_c^2 = 2^{2\alpha} - 2^{2(\beta-1)}$$

But this implies that $2\alpha > 2(\beta-1)$, so $\alpha + 1 > \beta$, and we have:

$$h_c^2 = 2^{2(\beta-1)}(2^{2(\alpha-\beta+1)} - 1)$$

Therefore $2^{2(\beta-1)} \mid h_c^2$, whence $2^{(\beta-1)} \mid h_c$ and $\left(\frac{h_c}{2^{\beta-1}}\right)^2 = k^2$ for some

$k \in \mathbb{Z}$, and we have:

$$2^{-2(\beta-1)} \left[2^{2\alpha} = h_c^2 + 2^{2(\beta-1)} \right] \rightarrow 2^{2(\alpha-\beta+1)} = k^2 + 1 \rightarrow \leftarrow$$

(The difference of two distinct squares is strictly greater than 1.)

Therefore, p must be odd.

$p > 2$: Notice that since p is odd, $\gcd(a, h_c, c/2) = \gcd(p^\alpha, h_c, 2^{\beta-1}) = 1$,

whence $(a, h_c, c/2)$ is a primitive Pythagorean triple, and we may

apply the classical parameterization of such triples:

$$p^\alpha = m^2 + n^2, \quad h_c = m^2 - n^2, \quad \text{and} \quad 2^{\beta-1} = 2mn$$

for some $m, n \in \mathbb{Z}$ with $m > n$ and $\gcd(m, n) = 1$, exactly one of

which is odd. But then we have:

$$2^{\beta-1} = 2mn \rightarrow m = 2^{\beta-2}, n = 1$$

whence:

$$p^\alpha = m^2 + n^2 \rightarrow p^\alpha = 2^{2(\beta-2)} + 1 \rightarrow \beta > 2 \quad (\text{since } p > 2)$$

Now let $w = 2(\beta - 2) > 1$ (since $\beta > 2$). Then if $\alpha > 1$, we have:

$$p^\alpha = 2^w + 1 \quad \text{with } p, 2, \alpha, w \in \mathbb{Z}, \quad \min(\alpha, w) > 1, \quad \text{and } w \text{ even}$$

However, this is not possible if $\alpha > 1$ because this is a case of

Catalan's equation with w even, which Lebesgue proved impossible

(Luca, 47). Therefore, $\alpha = 1$ and we have $p = 2^{2(\beta-2)} + 1$, which we

know must be a Fermat prime (theorem 2.10). Furthermore, we

know $2(\beta - 1) > 1$ (since $\beta > 2$), so $p = 2^{2(\beta-2)} + 1$ is a Fermat prime

for some $m \geq 1$, and it follows that we have:

$$2(\beta - 2) = 2^m \rightarrow \beta - 2 = 2^{m-1} \rightarrow \beta = 2^{m-1} + 2$$

and:

$$c = 2^\beta = 2^{2^{m-1}+2} = 2^2(2^{2^{m-1}} + 1 - 1) = 4(F_{m-1} - 1)$$

Therefore, if the triangle is isosceles, with $a = b$, we have shown that $(a, b, c) = (F_m, F_m, 4(F_{m-1} - 1))$.

Case 2: Let the triangle be non-isosceles. Then at least one of a , b , or c is even, so

let $c = 2^\gamma$ be even (we can do so without loss of generality), and let

$a = p^\alpha$ and $b = q^\beta$ for some $\alpha, \beta \in \mathbb{Z}^+$ and some primes $p, q \in \mathbb{Z}^+$. Now, p and q must have the same parity.

Both even: If both are even, then $p = q = 2$, and α, β , and γ must all be distinct (since non-isosceles). Without loss of generality, let $\gamma > \beta > \alpha$.

Then by the Triangle Inequality, we have:

$$\begin{aligned} b - a < c < b + a &\rightarrow 2^\beta - 2^\alpha < 2^\gamma < 2^\beta + 2^\alpha \\ &\rightarrow 2^\alpha(2^{\beta-\alpha} - 1) < 2^\gamma < 2^\alpha(2^{\beta-\alpha} + 1) \\ &\rightarrow 2^{\beta-\alpha} - 1 < 2^{\gamma-\alpha} < 2^{\beta-\alpha} + 1 \\ &\rightarrow -1 < 2^{\gamma-\alpha} - 2^{\beta-\alpha} < 1 \\ &\rightarrow 0 < 2^{\gamma-\alpha} - 2^{\beta-\alpha} < 1 \text{ (since } \gamma - \alpha > \beta - \alpha > 0) \\ &\rightarrow 2^{\gamma-\alpha} - 2^{\beta-\alpha} \notin \mathbb{Z} \rightarrow \leftarrow (2^{\gamma-\alpha}, 2^{\beta-\alpha} \in \mathbb{Z}) \end{aligned}$$

Therefore, p and q must both be odd primes.

Both odd: Let p and q be odd primes. Then notice that since $c = 2^r$, $2^r \parallel c$, and since the prime involved is 2, we have (by lemma 2.1):

$$2^{r+1} \mid a^2 - b^2 \text{ and } 2^{r+1} \mid 4A$$

which leads to:

$$2^{r+1} \mid 4A \rightarrow 2 \cdot 2^r \mid 2 \cdot 2A \rightarrow c = 2^r \mid 2A$$

and:

$$2c = 2^{r+1} \mid a^2 - b^2 = (a+b)(a-b)$$

Now, if $2 \mid a+b$ and $2 \mid a-b$, then we can factor all of the factors of 2 from each. Let $2^m \parallel a+b$ and $2^n \parallel a-b$ for some $m, n \in \mathbb{Z}^*$ with $m, n \geq 1$. Then:

$$a+b = 2^m k_1 \text{ and}$$

$$a-b = 2^n k_2 \text{ for some } k_1, k_2 \in \mathbb{Z} \text{ where } \gcd(2, k_1) = \gcd(2, k_2) = 1$$

Now, by adding we obtain:

$$2a = 2^m k_1 + 2^n k_2 \rightarrow a = 2^{m-1} k_1 + 2^{n-1} k_2 = p^\alpha$$

Since a is odd, exactly one of $2^{m-1} k_1$ and $2^{n-1} k_2$ is odd and one is even:

$$2^{m-1} k_1 \text{ odd and } 2^{n-1} k_2 \text{ even} \rightarrow m = 1, n > 1$$

$$2^{m-1} k_1 \text{ even and } 2^{n-1} k_2 \text{ odd} \rightarrow m > 1, n = 1$$

Now, it follows that: (recall $\gcd(2, k_1) = \gcd(2, k_2) = 1$)

$$m = 1: 2c = 2^{r+1} \mid (2k_1)(2^n k_2) \rightarrow c = 2^r \mid k_1(2^n k_2) \rightarrow c = 2^r \mid 2^n k_2 = a-b$$

$$n = 1: 2c = 2^{r+1} \mid (2^m k_1)(2k_2) \rightarrow c = 2^r \mid (2^m k_1)k_2 \rightarrow c = 2^r \mid 2^m k_1 = a+b$$

Therefore, if $2c \mid (a+b)(a-b)$, then either $c \mid a+b$ or $c \mid a-b$. Notice that $c \nmid a-b$ (since by the Triangle inequality, $0 < |a-b| < c$), so it must be that $c \mid a+b$. This observation enables us to examine the nature of a and b . Since a and b are both odd, we know that either both are congruent to 1 modulo 4, both are congruent to 3 modulo 4, or exactly one is congruent to 1 modulo 4. Since $\gamma \geq 2$ and $c \mid a+b$, the first two cases are easily eliminated.

Case 1: Let $a \equiv_4 1$ and $b \equiv_4 1$. Then we have $a = p^\alpha = 1 + 4k_1$ and $b = q^\beta = 1 + 4k_2$ for some $k_1, k_2 \in \mathbb{Z}$, and it follows that:

$$c = 2^\gamma \mid a+b = 2 + 4(k_1 + k_2) \rightarrow 2(1 + 2(k_1 + k_2)) = 2^\gamma k_3$$

for some $k_3 \in \mathbb{Z}$. But this is not possible since $\gamma \geq 2$.

Case 2: Let $a \equiv_4 3$ and $b \equiv_4 3$ (this case is similar to above). Then we have

$a = p^\alpha = 3 + 4k_1$ and $b = q^\beta = 3 + 4k_2$ for some $k_1, k_2 \in \mathbb{Z}$, whence:

$$c = 2^\gamma \mid a+b = 6 + 4(k_1 + k_2) \rightarrow 2(3 + 2(k_1 + k_2)) = 2^\gamma k_3$$

for some $k_3 \in \mathbb{Z}$. But, again, this is not possible since $\gamma \geq 2$.

Case 3: Therefore, it must be that exactly one of a and b is congruent to 1 modulo 4.

Without loss of generality, let $a \equiv_4 1$ and $b \equiv_4 3$. Notice, then, that

$b = q^\beta \equiv_4 3$ implies that $q \equiv_4 3$ since if $q \equiv_4 1$, then $q = 1 + 4k_1$ for some $k_1 \in \mathbb{Z}$, and we have:

$$q^\beta = (1 + 4k_1)^\beta = 1 + \binom{\beta}{1}(4k_1) + \binom{\beta}{2}(4k_1)^2 + \dots + (4k_1)^\beta \equiv_4 1 \rightarrow \leftarrow$$

Furthermore, β must be odd since if β is even, then $\beta = 2k_2$ for some $k_2 \in \mathbb{Z}$, and we have:

$$q^\beta = (3 + 4k_1)^{2k_2} = 3^{2k_2} + \binom{2k_2}{1}3^{2k_2-1}(4k_1) + \dots + (4k_1)^{2k_2} \equiv_4 1 \rightarrow \leftarrow$$

Now, since $b = q^\beta$, we have $q^\beta \parallel b$, and since $q \equiv_4 3$, we know $b = q^\beta \mid A$ (by lemma 2.1), whence $b \mid 2A$. We have already seen that $c \mid 2A$, so since

$\gcd(b, c) = 1$, clearly $bc \mid 2A$. Therefore, it follows that $\frac{2A}{bc} \geq 1$ (since

$2A = bck$ for some $k \in \mathbb{Z}$ with $k \geq 1$). Putting this together with the fact

that $A = \frac{(bc \sin \theta)}{2}$, where θ is the angle opposite side a , we see that

$\sin \theta \geq 1$, whence $\sin \theta = 1$ and $\theta = \pi/2$, forcing (a, b, c) to be a

Pythagorean triple. Thus we have:

$$a^2 = b^2 + c^2 \rightarrow p^{2\alpha} = q^{2\beta} + 2^{2\gamma}$$

Furthermore, this triple is a primitive Pythagorean triple since

$\gcd(a, b, c) = 1$, whence we may appeal to the standard parameterization of

all such triples yet again; we know there exists $m, n \in \mathbb{Z}$, with $m > n$ and

$\gcd(m, n) = 1$, exactly one of which is odd, such that:

$$p^\alpha = m^2 + n^2, q^\beta = m^2 - n^2, \text{ and } 2^\gamma = 2mn$$

But then:

$$2^\gamma = 2mn \rightarrow m = 2^{\gamma-1} \text{ and } n = 1 \text{ (since } \gcd(m, n) = 1 \text{ and } m > n \text{)}$$

and:

$$q^\beta = m^2 - n^2 \rightarrow q^\beta = m^2 - 1 = (m+1)(m-1)$$

Since $\gcd(m+1, m-1) = 1$ (consecutive odd integers), and their product is a power of a prime, it must be that $m-1 = 1$ (since $m+1 \neq 1$), whence $m = 2$.

Therefore:

$$q^\beta = m^2 - 1 = 3 \rightarrow q = 3 \text{ and } \beta = 1$$

Furthermore:

$$m = 2^{\gamma-1} \rightarrow 2 = 2^{\gamma-1} \rightarrow \gamma = 2$$

and:

$$p^\alpha = m^2 + n^2 = 2^2 + 1 = 5 \rightarrow p = 5 \text{ and } \alpha = 1$$

Finally, we have shown $(a, b, c) = (p^\alpha, q^\beta, 2^\gamma) = (5, 4, 3)$. \square *

Application Three: Finite Minimal POS Groups

A. Introduction

During a typical undergraduate abstract algebra course, the revelation that the order of various entities (an element, a coset, and a subgroup for example) divides the

order of the group (when the group is finite) tempts many students to conclude that the converse is also true; if a number divides the order of the group, then there must be an entity of that particular order within the group. While this is false in general, finite abelian groups frequently cooperate as desired, making them very intuition friendly. In this section, we define a different type of subset (perfect order subsets) whose order divides the order of the group and investigate resulting properties of finite abelian groups that contain these special subsets. The culminating theorem due to Finch and Jones, whose proof enlists the aid of Fermat primes, classifies all finite abelian groups satisfying our given conditions. While the reader should be familiar with cyclic groups and Sylow p -subgroups, we begin with a short review of key ideas from these topics before setting the stage with new definitions. Immediate consequences presented by Finch and Jones are then examined, followed by crucial facts used in proving the culminating theorem. The author has followed the approach presented in the original journal article, supplying additional information, proofs, and examples for the reader.

B. Reviewing Key Ideas

Since we will be dealing exclusively with finite abelian groups, let G always be a finite abelian group. In addition, to make dealing with repeated factors less cumbersome, let $(\mathbb{Z}_n)^t$ be the Cartesian product of t factors of \mathbb{Z}_n . We now give a brief list of key ideas from undergraduate algebra (see, for instance, Fraleigh).

- a. Every finitely generated abelian group, G , is isomorphic to a direct product of cyclic groups. If G is finite, then we know there are no factors of \mathbb{Z} , so $G \cong \mathbb{Z}_{(p_1)^{a_1}} \times \mathbb{Z}_{(p_2)^{a_2}} \times \cdots \times \mathbb{Z}_{(p_r)^{a_r}}$, where each p_i is prime (not necessarily distinct), and the factorization is unique (up to the order of the factors).
- b. The order of an element in a finite group must divide the order of the group.
- c. The order of $a \in \mathbb{Z}_m$ is $\frac{m}{\gcd(m, a)}$, the number of elements in $\langle a \rangle$.
- d. The order of $(a_1, a_2, \dots, a_n) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ is the least common multiple of the respective orders of each a_i .
- e. If a generates a finite cyclic group G , where $|G| = n$, then a^r also generates G provided $\gcd(r, n) = 1$.
- f. The number of elements of a given order in a cyclic group is the same as the number of generators for the subgroup of that order (recall that each such subgroup is unique). For example, the number of elements of order 4 in \mathbb{Z}_8 is 2 ($\langle 2 \rangle = \{2, 4, 6, 0\} = \langle 6 \rangle$). Therefore, the number of elements of order p^b in \mathbb{Z}_{p^a} is $\phi(p^b) = p^{b-1}(p-1)$.
- g. Consequently, for any prime p , there are $p-1$ elements of order p in \mathbb{Z}_p .
- h. If G is a finite group such that $|G| = p^n m$ where $n \geq 1$ and $p \nmid m$, then G contains a subgroup of order p^i for each $1 \leq i \leq n$, and every subgroup of order p^i is a normal subgroup of a subgroup of order p^{i+1} where $1 \leq i \leq n-1$.

C. Setting the Stage: New Ideas and Definitions

Now that we have reviewed the order properties for elements and subgroups of finite abelian groups, we are ready to put the ideas to use in a new way. To begin, consider all the elements that have the same order in a given group. Placing these elements (of the same order) into a set, called an *order subset*, introduces the first restriction for the groups we want to work with (note that we will only consider nonempty subsets). We wish to look only at groups where the cardinalities of all the order subsets divide the order of the group. Such groups will be said to have *perfect order subsets*. For instance, if we look at \mathbb{Z}_3 , there are two order subsets: $\{0\}$ and $\{1, 2\}$ (the elements of order one and three). However, while $|\{0\}| = 1$ divides $|\mathbb{Z}_3| = 3$, $|\{1, 2\}| = 2$ does not divide 3, so while this group has order subsets, it does not have perfect order subsets (similarly, any \mathbb{Z}_p for an odd prime p will not have perfect order subsets). On the other hand, consider $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$. Notice that $|G| = 24$. Since \mathbb{Z}_2 , \mathbb{Z}_4 , and \mathbb{Z}_3 have elements of order 1, 2, 3 and 4, there are elements of order 1, 2, 3, 4, 6, and 12 in G as table 1 illustrates. Clearly 1, 2, 3, 4, 6, and 8 all divide 24, so G has perfect order subsets (notice that while $12|24$, there is not an order subset with 12 elements, whence having perfect order subsets does not imply that there is an order subset for every divisor of the order of the group, even though we are in an abelian group). Notice that the property of having perfect order subsets is not necessarily passed on to subgroups (since $\{0\} \times \{0\} \times \mathbb{Z}_3 \cong \mathbb{Z}_3 \leq G$).

Table 1. Number of elements of given orders in $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$.

Element Order	Number of Elements	Elements
1	1	(0,0,0)
2	3	(0,2,0), (1,0,0), (1,2,0)
3	2	(0,0,1), (0,0,2)
4	4	((0,1,0), (0,3,0), (2,1,0), (2,3,0)
6	6	(0,2,1), (0,2,2), (1,0,1), (1,0,2), (1,2,1), (1,2,2)
12	8	(0,1,1), (0,1,2), (0,3,1), (0,3,2), (1,1,1), (1,1,2), (1,3,1), (1,3,2)

Before moving to the immediate consequences for groups with perfect order subsets, we give one more example in order to illustrate the counting arguments a little more clearly. Let $H \cong (\mathbb{Z}_2)^2 \times \mathbb{Z}_9$. Clearly, $|H| = 36$, and elements of H are triples where the first two elements have order 1 or 2 and the third element has order 1, 3 or 9 in their respective groups. Considering \mathbb{Z}_9 , the number of elements of order 1, 3, and 9 are 1, 2 and 6 respectively (using $\phi(p^b)$). Therefore, if we wish to consider how many elements there are of order eighteen in H (for a more complex example), we must have an element of order one or two in the first two positions followed by an element of order nine in the third position (as long as the first two elements do not have order one simultaneously). Since there are two choices for the first two positions and six choices for the third position, excluding the case where both of the first two elements have order one, there are $2(2)(6) - 1(1)(6) = 24 - 6 = 18$ elements of order eighteen. Performing similar calculations shows that the number of elements of order 1, 2, 3, 6, 9, and 18 in H

are 1, 3, 2, 6, 6, and 18 respectively, each of which divide $|H|$, whence H has perfect order subsets.

D. Immediate Consequences

Now that we have shown that finite abelian groups with perfect order subsets exist, we will restrict our examination to the consequences of our definitions on these groups. Accordingly, let G be a finite abelian group with perfect order subsets from now on. Keeping in mind that our main (culminating) goal is to classify all finite abelian groups with perfect order subsets, we begin our investigation by looking at $|G|$ and the number of elements of a given order in G , subsequently inspecting any ability to expand or contract our group. The reader is advised that all of the observations, lemmas and theorems in this section are found in the original article; the author has renamed the theorems, added details to the proofs, and provided examples to illustrate the ideas.

As a first observation, notice that if p is any prime divisor of $|G|$, then $p-1$ must divide $|G|$. To see this, let $G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_r}} \times \mathbb{Z}_m$ where $p \nmid m$. Then for $x = (x_1, x_2, \dots, x_r, x_m) \in G$ to have order p , each x_i , $1 \leq i \leq r$, must have order at most p in its respective group (with the identity in the last spot). Since there is one element of order one and there are $p-1$ elements of order p in each $\mathbb{Z}_{p^{a_i}}$, there are p choices for each x_i . However, we cannot let each x_i have order one, so there are $p^r - 1$ elements of order p in G . Since G has perfect order subsets, this shows that

$p^r - 1 = (p-1)(p^{r-1} + p^{r-2} + \dots + 1)$ divides $|G|$, whence $p-1$ divides $|G|$. From this it follows that if G has perfect order subsets, then $|G|$ must be even.

We now turn our attention to the number of elements of a given order within G .

To begin, we consider $(\mathbb{Z}_{p^a})^t$ and then build onto this.

Lemma 3.1: Let a , b and t be positive integers with $b \leq a$, and let $G \cong (\mathbb{Z}_{p^a})^t$ for a prime p . Then the number of elements in G of order p^b is $(p^{b-1})^t(p^t - 1)$.

Proof: Let G be as described, and let $x = (x_1, x_2, \dots, x_t) \in G$. If the order of x is p^b , then

the order of each x_i , $1 \leq i \leq t$, is $1, p, p^2, \dots$, or p^b with the order of at least one x_i being p^b . Counting such elements systematically, we count all the tuples whose first occurrence of an element of order p^b is in the first spot. We then count the tuples whose first occurrence of an element of order p^b is in the second spot, and so forth. Continuing in this manner will exhaust all possible arrangements for elements of order p^b without over counting the tuples. To make this process easier, note that the number of elements of order p^b in \mathbb{Z}_{p^a} is

$\phi(p^b) = p^{b-1}(p-1) = p^b - p^{b-1}$ (see part C). Furthermore, the number of choices

for each of the x_i with order less than or equal to p^b is $1 + \phi(p) + \phi(p^2) + \dots + \phi(p^b)$

(the number of elements for each successive order in \mathbb{Z}_{p^a}). This leads to

$1 + (p-1) + (p^2 - p) + \dots + (p^{b-1} - p^{b-2}) + (p^b - p^{b-1}) = p^b$ choices. Similarly, there

are p^{b-1} elements of order p^j , $0 \leq j < b$ ($1 + \phi(p) + \phi(p^2) + \dots + \phi(p^{b-1}) = p^{b-1}$). We are now ready to begin counting.

For the first arrangement, there are $\phi(p^b)$ choices for the first position with p^b choices for each of the following $t - 1$ positions, whence there are $\phi(p^b)(p^b)^{t-1}$ elements with the order of the first entry being p^b and the remaining orders less than or equal to p^b . Moving on, we let x_1 be an element of order strictly less than p^b and x_2 be an element of order p^b , followed by elements of order p^j , $0 \leq j \leq b$. This gives p^{b-1} choices for the first position, $\phi(p^b)$ choices for the second position, and p^b choices for the remaining $t - 2$ positions (as before). Thus there are $p^{b-1}\phi(p^b)(p^b)^{t-2}$ elements in this configuration. Continuing in this manner and summing the results, we obtain the number of elements in G of the desired order, p^b :

$$\phi(p^b)(p^b)^{t-1} + p^{b-1}\phi(p^b)(p^b)^{t-2} + \dots + (p^{b-1})^{t-2}\phi(p^b)(p^b) + (p^{b-1})^{t-1}\phi(p^b)$$

Now, looking at the exponents of p in the first and $t - 1^{\text{st}}$ terms, we see that

$$(t-1)b = (t-1)(b+1-1) = (b-1)(t-1) + t-1 \text{ and}$$

$$(b-1)(t-2) + b = (bt - t - 2b + 2) + b = bt - t - b + 2 = (b-1)(t-1) + 1$$

(with similar calculations for exponents of p in between), so we have:

$$\begin{aligned} & \phi(p^b)(p^b)^{t-1} + p^{b-1}\phi(p^b)(p^b)^{t-2} + \dots + (p^{b-1})^{t-2}\phi(p^b)(p^b) + (p^{b-1})^{t-1}\phi(p^b) \\ &= \phi(p^b)(p^{b-1})^{t-1}(p^{t-1} + p^{t-2} + \dots + p + 1) \\ &= p^{b-1}(p-1)(p^{b-1})^{t-1} \left(\frac{p^t - 1}{p-1} \right) \\ &= (p^{b-1})^t (p^t - 1) \quad \square \end{aligned}$$

Lemma 3.2: Let a and t be positive integers and p be prime. Let $G \cong (\mathbb{Z}_{p^a})^t \times M$ and

$\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^t \times M$ such that p does not divide $|M|$. If d is the order of an element in \hat{G} , and $p^{a+1} \nmid d$, then G and \hat{G} both contain the same number of elements of order d .

Proof: Let G and \hat{G} be as described, and let $x = (x_1, x_2) \in \hat{G}$ where $x_1 \in (\mathbb{Z}_{p^{a+1}})^t$ and $x_2 \in M$. Since p does not divide $|M|$, p does not divide the order of x_2 , so the order of x is the product of the orders of x_1 and x_2 . If d is the order of x , and $p^{a+1} \nmid d$, then we know $d = p^b m$ for some $0 \leq b < a+1$, where p^b is the order of x_1 and m is the order of x_2 . Then, by Lemma 3.1, the number of elements of order p^b in $(\mathbb{Z}_{p^{a+1}})^t$ is $(p^{b-1})^t (p^t - 1)$, but this is the same as the number of elements of order p^b in $(\mathbb{Z}_{p^a})^t$, whence it follows that there are the same number of elements of order d in G and \hat{G} . \square

Since groups satisfying the conditions of lemma 3.2 share elements of the same order, a natural question arises. May we use this information to expand a group known to have perfect order subsets and preserve the property of having perfect order subsets? The answer is yes; we may do so by increasing the exponent on the primes.

Expansion Theorem: Let a and t be positive integers, p be prime, $G \cong (\mathbb{Z}_{p^a})^t \times M$ and

$\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^t \times M$ such that p does not divide $|M|$. If G has perfect order subsets, then \hat{G} has perfect order subsets.

Proof: Let G and \hat{G} be as described, and let $x = (x_1, x_2) \in \hat{G}$ where $x_1 \in (\mathbb{Z}_{p^{a+1}})^t$,

$x_2 \in M$, and the order of x is d . If $p^{a+1} \nmid d$, then lemma 3.2 clearly shows that the order subset determined by x divides $|\hat{G}|$ (since it's order divides $|G|$ which in turn divides $|\hat{G}|$). Now, if $p^{a+1} \mid d$, then the order of x_1 is p^{a+1} (it can not have order greater than this), so $d = p^{a+1}m$ where m is the order of x_2 . By lemma 3.1 there are $(p^{(a+1)-1})^t(p^t - 1) = p^{at}(p^t - 1)$ choices for x_1 . Thus, if there are n elements of order m in \hat{G} , then there are $p^{at}(p^t - 1)n$ elements of order d in \hat{G} . Since there are $(p^{a-1})^t(p^t - 1)n$ elements of order p^am in G , and G has perfect order subsets, we know $k = (p^{a-1})^t(p^t - 1)n$ divides $|G|$. Furthermore,

$$p^t \mid |G| = |\hat{G}|, \text{ so } p^t k = p^t (p^{a-1})^t (p^t - 1)n = p^{at} (p^t - 1)n \text{ divides } |\hat{G}|$$

$$(a \mid b \rightarrow ap^t \mid bp^t). \quad \square$$

Before proceeding, we pause to illustrate this theorem. Let $G = (\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$,

which has perfect order subsets as illustrated in table 2 (using established counting procedures).

Table 2. Number of elements of given orders in $G = (\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Element Order	Individual Orders (within the triple)	Number of Elements (within G)
1	1, 1, 1	1
2	2, 1, 1	$2^4 - 1 = 15$
3	1, 3, 1	2
5	1, 1, 5	4
6	2, 3, 1	$(2^4 - 1)(2) = 30$
10	2, 1, 5	$(2^4 - 1)(4) = 60$
15	1, 3, 5	$2(4) = 8$
30	2, 3, 5	$(2^4 - 1)(2)(4) = 120$

Clearly 1, 2, 4, 8, 15, 30, 60 and 120 all divide $|G| = 240$. Now, according to the expansion theorem, we may increase the exponent on any of the primes. Thus, $G_1 = (\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ also has perfect order subsets. To verify this, note that there are $2^4 - 1 = 15$ elements of order 2 in $(\mathbb{Z}_2)^4$, 2 elements of order 3 and 6 elements of order 9 in \mathbb{Z}_9 , and 4 elements of order 5 in \mathbb{Z}_5 . Putting this together, we obtain elements of order 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45 and 90. The number of elements of these orders divides the order of our group, as is seen in table 3 since 1, 2, 4, 6, 8, 15, 24, 30, 60, 90, 120, and 360 all divide $|G_1| = 720$ (let the elements of $(\mathbb{Z}_2)^4$ be represented by a single place holder to simplify expressions; the reader should be able to separate the cases involved).

Table 3. Number of elements of given orders in $G_1 = (\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

Element Order	Individual Orders (within the tuple)	Number of Elements (within G)
1	1, 1, 1	1
2	1 or 2, 1, 1	15
3	1, 3, 5	2
5	1, 1, 5	4
6	1 or 2, 3, 1	$15(2) = 30$
9	1, 9, 1	6
10	1 or 2, 1, 5	$15(4) = 60$
15	1, 3, 5	$2(4) = 8$
18	1 or 2, 9, 1	$15(6) = 90$
30	1 or 2, 3, 5	$15(2)(4) = 120$
45	1, 9, 5	$6(4) = 24$
90	1 or 2, 3, 5	$15(6)(4) = 360$

Similar computations reveal groups such as $G_2 = (\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$, $G_3 = (\mathbb{Z}_8)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, and $G_4 = (\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_{125}$ also have perfect order subsets, which leads to another natural question. Given a group such as $G_4 = (\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_{125}$, can we reduce it to a group such as G that also has perfect order subsets and, if so, is there a minimal such group? In other words, is there a subgroup that also has perfect order subsets and, if there is more than one, is there a minimal such subgroup? Again, the answer is yes, but we look at special subgroups that arise by excluding factors (in a special way) or by decreasing the exponent on the prime(s). The details are given in the following theorems.

Exclusion Theorem: If $G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_{s-1}}} \times \left(\mathbb{Z}_{p^{a_s}}\right)^t \times M$ has perfect order

subsets, where $0 < a_1 \leq a_2 \leq \cdots \leq a_{s-1} < a_s$ are integers, and p is a prime such that p

does not divide $|M|$, then $\hat{G} \cong \left(\mathbb{Z}_{p^{a_s}}\right)^t \times M$ also has perfect order subsets.

Proof: Let G and \hat{G} be as described, and let $x = (x_1, x_2) \in \hat{G}$ where $x_1 \in \left(\mathbb{Z}_{p^{a_s}}\right)^t$. As

before, the order of x is $p^b m$ for some $0 \leq b \leq a_s$ (p^b is the order of x_1 and m is

the order x_2). Now, if $n = p^c k$ is the number of elements of order m in M , then by

lemma 3.1, the number of elements of order $p^b m$ in \hat{G} is $(p^{b-1})^t (p^t - 1) p^c k$,

which we must show divides $|\hat{G}|$. In order to show $(p^{b-1})^t (p^t - 1) p^c k$ divides

$|\hat{G}|$, we will show that $(p^{d-1})^t (p^t - 1) p^c k$ divides $|\hat{G}|$ for some $d \geq b$, from

which our conclusion easily follows by transitivity. Now, there are no elements

of order p^{a_i} in $\mathbb{Z}_{p^{a_i}}$ for $1 \leq i \leq s-1$, so an element of order $p^{a_s} m$ in G must have

an element of order p^{a_s} in the s -th position. Since $1, p^2, \dots, p^{a_{s-1}}$ all have p^{a_s} as

a common multiple, there are p^{a_1} choices for the first entry, p^{a_2} choices for the

second entry, and so forth, followed by elements of order p^{a_s} in $\left(\mathbb{Z}_{p^{a_s}}\right)^t$ and

elements of order m in M . By lemma 3.1, there are $(p^{a_s-1})^t (p^t - 1)$ elements of

order p^{a_s} in $\left(\mathbb{Z}_{p^{a_s}}\right)^t$, so we have $p^{a_1} p^{a_2} \cdots p^{a_{s-1}} (p^{a_s-1})^t (p^t - 1) p^c k$ elements of

order $p^{a_s} m$ in G . Notice that since $p^{a_1+a_2+\dots+a_{s-1}+a_s t-t+c} (p^t - 1) k$ divides $|G|$, we

must have $-t + c \leq 0$, or $c \leq t$ (otherwise we will have too many factors of p).

Furthermore, $(p^t - 1)k$ must divide $|M|$. Finally, since $|G| = p^{a_1 + a_2 + \dots + a_{s-1}} |\hat{G}|$, we have:

$$p^{a_1} p^{a_2} \dots p^{a_{s-1}} (p^{a_s - 1})^t (p^t - 1) p^c k \text{ divides } |G| \text{ implies}$$

$$p^{a_1 + a_2 + \dots + a_{s-1}} (p^{a_s - 1})^t (p^t - 1) p^c k \text{ divides } |G| = p^{a_1 + a_2 + \dots + a_{s-1}} |\hat{G}|$$

From which it follows that $(p^{a_s - 1})^t (p^t - 1) p^c k$ divides $|\hat{G}|$. Since $b \leq a_s$, it

follows that $(p^{b-1})^t (p^t - 1) p^c k$ also divides $|\hat{G}|$. Thus \hat{G} also has perfect order subsets. \square

Notice that the converse of this theorem is not necessarily true. For instance, $\mathbb{Z}_8 \times \{0\}$ has perfect order subsets (the number of elements of order 1, 4, and 8 are 1, 2, and 4 respectively), but neither $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \{0\}$ nor $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \{0\}$ has perfect order subsets (there are 3 elements and 7 elements of order 2 respectively, neither of which divide the orders of the groups). Lest the reader think this only happens for groups with $M = \{0\}$, notice that while $H \cong \mathbb{Z}_9 \times (\mathbb{Z}_2)^2$ has perfect order subsets (as seen in part C), $H_1 \cong \mathbb{Z}_3 \times \mathbb{Z}_9 \times (\mathbb{Z}_2)^2$ does not (there are 8 elements of order 3).

Reduction Theorem: If $G \cong (\mathbb{Z}_{p^a})^t \times M$ has perfect order subsets and p is a prime such

that p does not divide $|M|$, then $\hat{G} \cong (\mathbb{Z}_p)^t \times M$ also has perfect order subsets.

(The proof of this theorem is similar to that for the previous theorem.)

Putting these facts together, we see that if we are given a group with perfect order subsets, we may exclude factors with lesser powers of repeated primes, and we may decrease the powers of the remaining primes involved all the way to one (so we have a group with Sylow p -subgroups that are square-free). In addition, the order of any group with perfect order subsets must be even, whence we always have at least one factor of \mathbb{Z}_2 . Therefore, we define a *minimal POS group* as a group $G \cong (\mathbb{Z}_2)^t \times M$ such that G has perfect order subsets, $|M|$ is odd and square-free, and that no group $\hat{G} \cong (\mathbb{Z}_2)^t \times \hat{M}$, where \hat{M} is a proper subgroup of M , has perfect order subsets. For example, we saw in part C that $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ and $H \cong (\mathbb{Z}_2)^2 \times \mathbb{Z}_9$ have perfect order subsets. By the exclusion and reduction theorems, it follows that $G_1 = \mathbb{Z}_4 \times \mathbb{Z}_3$ and $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_3$ have perfect order subsets; however, G_2 is not minimal since $\mathbb{Z}_2 \times \{0\} \cong \mathbb{Z}_2$ also has perfect order subsets (while $\{0\}$ is a trivial subgroup of \mathbb{Z}_3 , it is still a proper subgroup). Therefore, \mathbb{Z}_2 is the minimal POS group that we seek inside G . Lest the reader think we can always reduce to \mathbb{Z}_2 , consider $H \cong (\mathbb{Z}_2)^2 \times \mathbb{Z}_9$, which is not minimal. Notice that there is a subgroup of \mathbb{Z}_9 that is isomorphic to \mathbb{Z}_3 , and $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ has perfect order

subsets; however, $(\mathbb{Z}_2)^2 \times \{0\}$ does not have perfect order subsets, whence $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ is a minimal POS group. Notice that H also has a subgroup isomorphic to \mathbb{Z}_2 , which is a POS group, yet this is not a minimal POS group corresponding to H since neither the exclusion nor the reduction theorem allows us to exclude a factor of \mathbb{Z}_2 (reducing H to G_2). In other words, one must use care when reducing a given POS group.

The astute reader may now be thinking that due to the restrictions we have put in place, is it possible to list all the minimal POS groups? Once more the answer is yes, up to isomorphism, and we are now ready to classify all the minimal POS groups; however, to aid the reader, we give two crucial facts before stating the culminating theorem.

E. Crucial Facts Used in the Proof of the Culminating Theorem

The following theorem and lemma play key roles in the proof of the main theorem to follow. They are presented here to ease the proof of the theorem. While theorem 3.1 was not proved in the original article, lemma 3.3 was (details have been added by author).

Theorem 3.1: If p is an odd prime such that $p|t$, then $2^p - 1|2^t - 1$.

Proof: If $p = t$, then the result is clear. Let $p < t$. Then since $p|t$, we know $t = pk$ for

some $k \in \mathbb{Z}^+$, from which it follows that $2^p - 1|2^t - 1$ since:

$$2^t - 1 = 2^{pk} - 1 = (2^p)^k - 1 = (2^p - 1)[(2^p)^{k-1} + (2^p)^{k-2} + \dots + (2^p) + 1]. \quad \square$$

Lemma 3.3: If p is a prime, $a \in \mathbb{Z}^+$, and q is a prime divisor of $2^{p^a} - 1$, then $p \mid q - 1$.

Proof: Let p be a prime, $a \in \mathbb{Z}^+$, and q a prime divisor of $2^{p^a} - 1$. Then $2^{p^a} \equiv_q 1$, from which it follows that 2^{p^a} is the identity element of the group $(\mathbb{Z}_q)^*$. Therefore, $\text{ord}_{(\mathbb{Z}_q)^*} 2 = d \mid p^a$, or $p^a = dk$ for some $k \in \mathbb{Z}^+$. Thus $d = p^\alpha$ and $k = p^\beta$ where $\alpha + \beta = a$, so $p(p^{\alpha-\beta-1}) = d \rightarrow p \mid d$. Now, the order of an element in a finite group divides the order of the group (Lagrange's Theorem), so we know d divides $|(\mathbb{Z}_q)^*|$, or $d \mid q - 1$, whence we have $p \mid d$ and $d \mid q - 1$ implies $p \mid q - 1$. \square

F. Proving The Main Theorem

We are now ready to classify all minimal POS groups (for finite abelian groups). Before doing so, however, the reader should take a moment to reflect upon the potential consequences of creating a minimal POS group. For instance, if we start with $(\mathbb{Z}_2)^t$, where t is a known value, and we wish to attach cyclic groups (of odd order) to $(\mathbb{Z}_2)^t$ in order to make $G \cong (\mathbb{Z}_2)^t \times H$ a minimal POS group, where the order of H is odd and square free, then $2^t - 1$ must divide the order of G (since there are $2^t - 1$ elements of order 2 in G) whence $2^t - 1$ must divide the order of H (since $2^t - 1$ is odd). Furthermore, for each prime p dividing $2^t - 1$, our group must contain a Sylow p -

subgroup of that order. However, if we attach a cyclic group of order p , then we introduce elements of order $p-1$, which in turn must divide the order of G (to ensure G is still a POS group). This requirement might force us to add more cyclic groups. For instance if we start with $(\mathbb{Z}_2)^3$ and attach \mathbb{Z}_7 , then we will be required to attach \mathbb{Z}_3 as well so that we can have an element of order 6. For higher values of t , this process might lead to non-desirable conditions, such as requiring factors which lead to groups with Sylow p -subgroups which are not square free (violating our search for a minimal POS group). For instance, if we begin with $(\mathbb{Z}_2)^7$, then we must attach \mathbb{Z}_{127} , opening the door to elements of order 9 (since $9|126$). We must then attach \mathbb{Z}_9 , causing the order of H to have a power of a prime, which we wish to avoid (since we will then have a Sylow 9-subgroup). Although the situation seems hopelessly complex, there are a finite number of values of t that will work nicely within our constraints, which the following theorem due to Finch and Jones spells out.

Theorem 3.2: Let G be a finite abelian group of even order whose Sylow p -subgroup is a cyclic group of order p for each prime p dividing the order of G . If G is a minimal POS group, then G is isomorphic to one of the following groups:

- a. \mathbb{Z}_2
- b. $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$
- c. $(\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$
- d. $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- e. $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$
- f. $(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$

- g. $(\mathbb{Z}_2)^{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$
- h. $(\mathbb{Z}_2)^{17} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{131071}$
- i. $(\mathbb{Z}_2)^{32} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{65537}$

Proof: (The original proof has been reorganized and important details have been added.)

We will prove the theorem in two stages: verifying that the above are minimal POS groups and showing that these are the only nine such groups.

I. Verifying:

To begin, \mathbb{Z}_2 has already been shown to be a minimal POS group (group b was mentioned to be minimal in part D, but it was not proved, so we will consider it as needing to be verified). As it turns out, we can split the remaining eight groups into two sets corresponding to the verification process involved in showing the group in question is a minimal POS group (there are two main concepts involved, one for each set). Coincidentally, there are four groups within each of these sets. We shall show one of the groups in each set is a minimal POS group, leaving the remaining verifications to the reader. Before doing so, however, we note that the reader should be familiar with finding the order of an element, as well as the number of elements of a given order, at this point. For sake of completeness, we include a column in our tables verifying the divisibility check, although this is a trivial process.

The first set we consider is $A = \{b, f, g, h\}$. From this set, we will show that group $f, (\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$, is a minimal POS group. Notice that $|f| = 65280$. Table 4 then shows that f is a POS group.

Table 4. Number of elements of given orders in $(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$.

Element Order	Relevant Orders (within the tuple)	Number of Elements (within the group in question)	Divisibility Check (product is 65280)
1	1	1	1(65280)
2	2	$2^8 - 1 = 255$	255(256)
3	3	2	2(32640)
5	5	4	4(16320)
6	2, 3	$(2^8 - 1)(2) = 510$	510(128)
10	2, 5	$(2^8 - 1)(4) = 1020$	1020(64)
15	3, 5	$2(4) = 8$	8(8160)
17	17	16	16(4080)
30	2, 3, 5	$(2^8 - 1)(2)(4) = 2040$	2040(32)
34	2, 17	$(2^8 - 1)(16) = 4080$	4080(16)
51	3, 17	$2(16) = 32$	32(2040)
85	5, 17	$4(16) = 64$	64(1020)
102	2, 3, 17	$(2^8 - 1)(2)(16) = 8160$	8160(8)
170	2, 5, 17	$(2^8 - 1)(4)(16) = 16320$	16320(4)
255	3, 5, 17	$2(4)(16) = 128$	128(510)
510	2, 3, 5, 17	$(2^8 - 1)(2)(4)(16) = 32640$	32640(2)

We must now verify that f is a minimal POS group. This is fairly straightforward. Notice that $2^8 - 1 = 255 = 3(5)(17)$. Since it is essential for $2^8 - 1$ to divide $|G|$ (since there are $2^8 - 1$ elements of order 2, and we want G to be a POS group), every prime that divides $2^8 - 1$ is required to be present in $|G|$ (in order to make $|G|$ divisible by 255). Hence, we may not leave off any of the odd cyclic groups without disrupting the POS quality of our group, and f is a minimal POS group.

The second set we consider is $B = \{c, d, e, i\}$. From this set we consider group e , $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$, which has order 14880. Table 5 then shows that e is a POS group. Verifying that e is a minimal POS group is a little trickier in this case since $2^5 - 1 = 31$ is prime. On the surface it looks as though we could reduce the group to $(\mathbb{Z}_2)^5 \times \mathbb{Z}_{31}$, but a moment's thought shows that \mathbb{Z}_{31} introduces elements of order 30. In order for 30 to divide $|G|$, we must have all the primes that divide 30 involved in $|G|$. We are missing 3 and 5, hence we must include \mathbb{Z}_3 and \mathbb{Z}_5 , bringing us back to the original group. All of the groups in this set have this "capturing" quality, as is easily checked.

Table 5. Number of elements of given orders in $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$.

Element Order	Relevant Orders (within the tuple)	Number of Elements (within the group in question)	Divisibility Check (product is 14880)
1	1	1	1(14880)
2	2	$2^5 - 1 = 31$	31(480)
3	3	2	2(7440)
5	5	4	4(3720)
6	2, 3	$(2^5 - 1)(2) = 62$	62(240)
10	2, 5	$(2^5 - 1)(4) = 124$	124(120)
15	3, 5	$2(4) = 8$	8(1860)
30	2, 3, 5	$(2^5 - 1)(2)(4) = 248$	248(60)
31	31	30	30(496)
62	2, 31	$(2^5 - 1)(30) = 930$	930(16)
93	3, 31	$2(30) = 60$	60(248)
155	5, 31	$4(30) = 120$	120(124)
186	2, 3, 31	$(2^5 - 1)(2)(30) = 1860$	1860(8)
310	2, 5, 31	$(2^5 - 1)(4)(30) = 3720$	3720(4)
465	3, 5, 31	$2(4)(30) = 240$	240(62)
930	2, 3, 5, 31	$(2^5 - 1)(2)(4)(30) = 7440$	7440(2)

II. Isolating the minimal POS groups:

Now that we have described typical verifications that each of the nine groups on the list is a minimal POS group, we switch our focus to finding all such minimal POS groups. Let G be a finite abelian minimal POS group of

even order whose Sylow p -subgroup is a cyclic group of order p for each prime p dividing the order of G . Then $G \cong (Z_2)^t \times H$ where the order of H is odd (by definition of minimal POS group) and square free (since each Sylow p -subgroup is cyclic of order p). Furthermore, $t \geq 1$ since G is of even order; however, $t = 1$ leads to Z_2 , so we consider $t > 1$. As the comments preceding the theorem indicate, t determines the order of H , and H in turn heavily influences the value we can use for t . As we shall see, this interdependence forces t to be a power of a single prime.

Before we can see this result, we need to establish a few useful facts. Recall that $2^t - 1$ (the number of elements of order 2) divides $|H|$, whence $2^t - 1$ is square free (since $|H|$ is square free). Now if p is an odd prime such that $p | t$, then $2^p - 1 | 2^t - 1$ (by Theorem 3.1), whence $2^p - 1$ is square free (since $2^t - 1$ is square free). Furthermore, $2^p - 1$ is prime since if q_1 and q_2 are two distinct primes dividing $2^p - 1$, then $p | q_1 - 1$ and $p | q_2 - 1$ (by Lemma 3.3), whence $p^2 | (q_1 - 1)(q_2 - 1)$. However, $(q_1 - 1)(q_2 - 1)$ is the number of elements of order $q_1 q_2$ in G , so p^2 divides $|G|$, and since p is odd, it follows that p^2 divides $|H|$. $\rightarrow\leftarrow$ Therefore $2^p - 1$ is a square-free prime such that $2^p - 1$ divides $|G|$, from which it follows that there are $2^p - 2$ elements of order $2^p - 1$ in G (by the hypothesis of the theorem). The final observation we make here is that since p is odd, $p = 2k + 1$ for some $k \in \mathbb{Z}$,

and $2^p \equiv_3 2^{2k+1} = (2^2)^k 2 \equiv_3 2$, whence $3 \mid 2^p - 2$. We are now ready to see that t must be a power of a single prime.

Assume that t is not a power of a single prime. Let p_1 and p_2 be two distinct odd primes dividing t . Then it follows that $3 \mid 2^{p_1} - 2$ and $3 \mid 2^{p_2} - 2$, whence $9 \mid (2^{p_1} - 2)(2^{p_2} - 2)$. Since $(2^{p_1} - 2)(2^{p_2} - 2)$ is the number of elements of order $(2^{p_1} - 1)(2^{p_2} - 1)$, this shows that 9 divides $|G|$, hence $|H|$, a contradiction. Similarly, if 2 and an odd prime p divide t , then $t = 2k$ for some $k \in \mathbb{Z}$, whence $2^t = (2^2)^k \equiv_3 1$, and we have $3 \mid 2^t - 1$ and $3 \mid 2^p - 2$ leading to $9 \mid (2^t - 1)(2^p - 2)$, the number of elements of order $2(2^p - 1)$ in G , again contradicting the square free property of H . Therefore t must be a power of a single prime. We are now ready to narrow the focus even more, isolating which primes can play in the game with t , and it is at this point the friendly Fermat primes lend a hand.

Clearly if t is a power of 2, then $t = 2^a$ for some $a \geq 1$. On the other hand, if t is a power of an odd prime, then t must be a Fermat prime. To see this, let $t = p^a$ with p an odd prime and $a \geq 2$ (we shall see that this is not possible, forcing $a = 1$). Recall that $2^p - 1 \mid 2^t - 1$, so we now have $2^p - 1 \mid 2^{p^a} - 1$. Furthermore, since $2^t - 1 = 2^{p^a} - 1$ is square free, and $2^p - 1 \neq 2^{p^a} - 1$, we know there exists another odd prime $q \neq 2^p - 1$ such that $q \mid 2^{p^a} - 1$. Now, by Lemma 3.3, it follows that $p \mid q - 1$. Furthermore, $2^p \equiv_p 2$ for any odd prime,

so we have $p|q-1$ and $p|2^p-2$, whence $p^2|(q-1)(2^p-2)$, the number of elements of order $q(2^p-1)$ in G , whence p^2 divides $|H|$ ($\rightarrow\leftarrow$). Therefore, $a \leq 1$, but since $a \geq 1$, we have $a=1$, whence $t=p$. Notice that $2(2^{p-1}-1)=2^p-2$ divides $|G|$ implies that $2^{p-1}-1$ divides $|G|$, allowing us to perform an identical analysis of $p-1$ that we applied to t in the previous paragraph. In short, $p-1$ must be a power of a single prime, and since $p-1$ is even, that prime must be 2. This shows that if t is a power of an odd prime, then $t=p$ where $p-1=2^a$, or $t=2^a+1$. As seen in previous sections, the only primes of this form are Fermat primes (see theorem 2.10).

We have now narrowed the form of t to $t=2^a$, or $t=2^{2^a}+1$ (a Fermat prime) where $2^{t-1}-1$ divides $|G|$, with $a \geq 1$ in either case. If $t=2^a$, then $2^t-1=2^{2^a}-1$ divides $|G|$, and if $t=2^{2^a}+1$, then $2^{t-1}-1=2^{2^b}-1$, where $b=2^a$, divides $|G|$, both of which are of the form $2^{2^m}-1$. One final observation will now allow us to restrict the values for t one last time. Notice

that $2^{2^m}-1 = \prod_{n=0}^{m-1} (2^{2^n}+1)$:

This is clearly true for $m=1$: $2^2-1=2+1=3$. Suppose it is true for

$m=k$. Then $2^{2^k}-1 = \prod_{n=0}^{k-1} (2^{2^n}+1)$, and we have:

$$2^{2^{k+1}}-1 = 2^{(2^k)^2}-1 = \left(2^{2^k}\right)^2-1 = \left(2^{2^k}+1\right)\left(2^{2^k}-1\right)$$

$$= \left(\prod_{n=0}^{k-1} (2^{2^n} + 1) \right) (2^{2^k} + 1) = \prod_{n=0}^k (2^{2^n} + 1)$$

Therefore the formula is true by induction on m .

Now, since $2^{2^m} - 1 = \prod_{n=0}^{m-1} (2^{2^n} + 1) = \prod_{n=0}^{m-1} F_n$, we see that $F_5 \mid 2^{2^m} - 1$ when $m \geq 6$.

We argue that $m \geq 6$ is not possible. One of the prime factors of F_5 is

6700417, whence $6700417 \mid F_5$, $F_5 \mid 2^{2^m} - 1$, and $2^{2^m} - 1 \mid |G|$ imply 6700417

divides $|G|$. Therefore G has elements of order 6700417 (by hypothesis).

Furthermore, $3 \mid 2^{2^m} - 1$ and $3 \mid 6700416$, whence $9 \mid 6700416(2^{2^m} - 1)$, the

number of elements of order $2(6700417)$ in G , forcing 9 to divide $|H|$ yet

again. $\rightarrow\leftarrow$ Therefore, $m \leq 5$, giving us the key to unlock the exact values for t .

Considering $t = 2^a > 1$ with $a \leq 5$ first (recall we used $a = m$ in the

formula), we see that $t \in \{2, 4, 8, 16, 32\}$. On the other hand, if $t = 2^{2^a} + 1$, we

must exercise a little caution in unraveling the value for t since we used a

small change of variable, $m = b = 2^a$, whence $2^a \leq 5$. The only values that

will work for a in this inequality are 0, 1, and 2, from which it follows that

$t \in \{3, 5, 17\}$. Putting this together with the trivial case in the beginning of the

proof, we have $t \in \{1, 2, 3, 4, 5, 8, 16, 17, 32\}$.

Finally, recall that the minimal POS groups associated with these values

for t must have Sylow p -subgroups of order p for each prime p such that

$p \mid 2^t - 1$ and that $p - 1$ must divide $|G|$. Introducing the requirement that $|H|$ be square free then forces the existence of exactly one minimal POS group for each value of t that meets these requirements. We have just shown the only values of t that will cooperate, and each value corresponds to one of the nine groups already verified minimal POS groups. \square *

CHAPTER FOUR

CONCLUDING COMMENTS AND OPEN PROBLEMS

As we have seen, Fermat unwittingly changed the course of mathematical history, although he was not blessed to witness the beautiful harmony that his contribution has had within the orchestra of the mathematical framework being constructed. In light of the fact that Fermat did not publish his work but rather pursued mathematics purely for love of the subject, the author feels confident that Fermat did not fully comprehend the vital role that he was playing. To put Fermat's role in perspective, the author notes two significant details: work with prime numbers and advances in algebra and number theory had both been neglected for a significant period of time prior to Fermat's birth. The ancient Greeks had completed extensive work with prime numbers, yet after Eratosthenes introduced his famous prime number sieve in 200 B.C., the world entered a period of silence known as the Dark Ages. This silence was shattered with Fermat's enlightened work (O'Connor, Prime Numbers, 1). Similarly, the reader may be aware that Fibonacci broke a 1000 year stagnation in development in western mathematics, yet it was not for approximately another 300 years that François Viète introduced the notation with letters that Fermat was to follow (Scharlau, 5). The author wonders whether Fermat realized that when he took up this mantle that he would uncover mathematical concepts that were so radically new and important that he would one day be seen as a forerunner in the development of what is now known as modern mathematics. Added to the fact that Fermat was a pioneer in a new mathematical world, Fermat's brilliance was met with stiff jealousy and wounded pride when Fermat carelessly ridiculed Descartes' work with the

law of refraction. In the ensuing controversy that swept the community, Descartes unleashed bitter attacks upon Fermat in an effort to destroy Fermat's reputation.

Although the battle ended on a sociable note, Descartes continued to assault Fermat's reputation. Due to Descartes' prominence, these attacks severely damaged Fermat's reputation (O'Connor, Pierre de Fermat, 3). Certainly, as Fermat suffered these character attacks, and as he later found himself without any colleagues interested in his beloved number theory, he more than likely did not fathom that his responding challenges and raised questions would have far-reaching consequences more than 400 years later.

Today the world is blessed with deep and beautiful theories as a result of Fermat's effort, and the groundwork that Fermat began continues to challenge mathematicians. This gives cause for one to stop and ponder his or her contribution, for the story is far from over. As one question resolves, another one raises its head, and intricate and exciting connections emerge. This paper has illustrated relations between Fermat primes and Geometry as well as Finite Group Theory. How many more connections remain to be discovered? How many seemingly unrelated questions provide the keys to unlocking fundamental truths? We have already seen that the smallest value for $k \in \mathbb{N}$ such that all the numbers in the set $\{k2^n + 1 : n \in \mathbb{N}\}$ are composite remains to be found. Will its discovery help solve any riddles? For instance, will this help to show if there exists an odd $k \geq 3$ such that infinitely many Fermat numbers have a prime factor $k2^n + 1$ for some n (that is, for any fixed k and varying n)? With these thought-provoking questions, the author wishes to alert the reader that there exist many open questions pertaining to Fermat numbers, Fermat primes and composite factorizations, primes in general, and other areas of

investigation involving connections with Fermat primes, each of which may provide the next crucial discovery.

Perhaps the issue which is foremost in the minds of many is the very old question of whether the five known Fermat primes comprise all of the Fermat primes. In the relentless quest to answer this problem over the last several centuries, mathematicians the world over have joined forces to unlock any piece of the puzzle that may give further insight. Several heuristic arguments that the number of Fermat primes is finite have been offered, but the reader is cautioned that these arguments are probabilistic and rely upon random behavior. Since any Fermat number, say $F_m = 2^{2^m} + 1$, can be written in base two as 10000...01 (a one followed by $2^m - 1$ zeroes and a concluding one), the Fermat numbers are highly non-random. As more progress is being made in establishing further composite Fermat numbers, however, it seems likely that the number of Fermat primes is finite, but this remains as a tantalizing question.

Perhaps one way to answer this question is to look into the prime divisors of the composite Fermat numbers. It has been shown that any prime divisor of a Fermat number, F_m , must have the form $k2^{m+1} + 1$ for some $k \in \mathbb{N}$ (Křížek, 38), but these primes seem scarce and difficult to find. Nevertheless, the search has consumed men across the globe for several centuries now. According to one website, between 1640 and 2003, seventy-one men from over sixteen different countries have contributed to the growing list of prime divisors (Morelli)! Interestingly, the top three most frequently mentioned countries are the United States of America, Russia, and France (although not all of the contributors' nationalities are listed). The majority of these contributions have occurred

since 1925 (only eleven contributors between 1640 and 1924). This illustrates a key shift: since the advent of the computer and the mobility of information offered by the Internet, the pursuit in this direction has intensified. If the reader searches the Internet, for example, he or she will find numerous websites that list known factorizations and key discoveries. It is therefore generally known that prior to 1925, only sixteen factors of Fermat primes had been found. Since computers have offered assistance, however, over 234 new factors have been found, giving us a total of more than 250 currently known factors (numbers vary depending on the website). Lest the reader think that interest might begin to lag in this area, the author notes that during the course of writing this thesis, new factors have been discovered, the most recent of which occurred less than a month prior to completion of this paper. Curtis Cooper found that $27 \cdot 2^{672007} + 1$ divides F_{672005} on August 30, 2005. Notice that the index for this Fermat number ends in the year of discovery, a small curiosity to the author. New prime factors which divide F_{83} , F_{1160} , F_{60079} , and F_{960897} have also been discovered recently (since February, 2005) by Vasily Danilov, Maximilian Pacher, and Michael Eton (respectively; the last two by Eton). The most current reported total found by the author was 257 known prime factors with 224 known composite Fermat numbers as of August 30, 2005 (Keller). According to Ivars Peterson, author of “Cracking Fermat Numbers,” part of the excitement in this search is “the race to set the record for the largest Fermat number known to be composite,” the largest of which is currently $F_{2145351}$ (as of 2003). To give the reader an idea of the size of this number, the discoverer, John Cosgrove, noted that “to write out its decimal value – at

four digits per square inch in the horizontal and vertical directions – would require a sheet of paper with side length exceeding 10^{322889} light years” (Peterson). The incredible size of this composite Fermat number is something to ponder!

Another question, which brings us back to Earth for the time being, shifts focus from the prime divisors themselves to the number of divisors involved in the complete factorization of a composite Fermat number. In particular, once a Fermat number is known to be composite, does the number of its prime factors necessarily have to be greater than the number of prime factors of any of the previous composite Fermat numbers? For instance, table 6 lists the number of prime factors of the first thirteen Fermat numbers. Is the resulting sequence of the number of prime factors a nondecreasing sequence?

Table 6. The number of prime factors for the first thirteen Fermat numbers.

Fermat Numbers	Number of Prime Factors
$F_0 - F_4$	1
$F_5 - F_8$	2
F_9	3
F_{10}	4
F_{11}	5
F_{12}	≥ 7

The answer to this question remains a difficult one since only the first twelve Fermat numbers have been completely factored into a product of primes. Thus, the complete

factorizations of the remaining Fermat numbers leaves a lot of playing room for anyone who wishes to explore open problems. Another related quest is finding the smallest prime factor for F_{14} , F_{20} , F_{22} , and F_{24} (Křížek, 159). Interestingly, the known prime factorizations of Fermat numbers are all square free, which leads to a further question of whether all Fermat numbers are square free.

Switching focus slightly to general primes, there are numerous open questions that are similar in nature and whose answers may, therefore, shed light on Fermat factorizations. For instance, if p is a prime, is $2^p - 1$ always square free? Furthermore, are there infinitely many primes of the form $n^n + 1$, $n! + 1$, and / or $n! - 1$ (O'Connor, "Prime Numbers")? While an underlying connection is not very clear to the author, the similarities to the open questions concerning primes and Fermat numbers are appealing.

As a last observation, the reader is reminded that there are other areas of investigation involving connections with Fermat numbers, each of which have resulting open questions. For instance, Finch and Jones offer several open questions relating to their article on finite minimal POS groups, which we present here. The only known example of a minimal POS group containing a cyclic subgroup of odd order is

$(\mathbb{Z}_2)^{11} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times (\mathbb{Z}_{11})^2 \times \mathbb{Z}_{23} \times \mathbb{Z}_{89}$. This leads to the natural question: are there only

finitely many such groups? Furthermore, if G is known to have perfect order subsets, and p is an odd prime that divides $|G|$, is it true that three will divide $|G|$? Finally, since the primary focus to date has been on abelian groups, non-abelian groups provide fertile research ground.

In the introduction to this thesis, the author mentioned that research has also uncovered many interesting connections between Fermat numbers and Pascal's triangle. We can find many open questions here as well. For instance, one of the connections between the Fermat numbers and Pascal's triangle appears when $c = 3$ in the following proposition (see Křížek, 90 – 91):

If c is any fixed integer greater than 2, and $k > 1$ is any integer not divisible by any prime less than or equal to $c^2 - c - 1$, then k is a prime number if and only if

$$n \binom{n}{k-cn} \text{ for all } n \text{ such that } \frac{k}{c+1} \leq n \leq \frac{k}{c}.$$

Now, notice that if we let $K_c = \left\{ n \in \mathbb{Z}^+ \text{ such that } n \binom{n}{k-cn} \text{ for all } \frac{k}{c+1} \leq n \leq \frac{k}{c} \right\}$, then

the previous proposition fails to give any information about members of K_c that are divisible by primes smaller than $c^2 - c - 1$. Furthermore, while the exact structure of these sets has been studied for $c = 4, 5, 6$, nothing is known about the structure when $c > 7$ (93). In addition, it has been shown that $K_3 = \{1, 4, 25, \text{all primes}, 2q: q > 3 \text{ is a Fermat prime}\}$. However, is it true that $2q$, where $q > 3$ is a Fermat prime, will belong to K_c for infinitely many values of c ? If not, what about those c 's divisible by three (93)? The answers to these questions and many more may unlock further connections between Pascal's triangle and Fermat numbers.

While the above questions are more number theoretic in nature, recall that exciting connections exist between Fermat numbers and Geometry as well. Similar to Gauss's theorem, it has been shown that if F_0, F_1, F_2, F_3 , and F_4 are the only Fermat

primes, and $2^n + 1$ is prime, then for $n \neq 1$, there exists a regular polyhedron whose number of faces is $n + 4$ (163). Inserting “vertices” for “faces” or “number of sides” in these two theorems does not change the truth of the theorems, so a natural question arises. Do these two theorems have a deeper governing principle, or do they hold simply because of the restricted set of numbers (164)? Similarly, is there a general theory that would lead to a definitive answer about whether or not F_4 is the largest Fermat prime? The author wonders whether, if such a principle for one question exists and is revealed, would it be related to the underlying theory of the other.

Just as the highlights of the numerous results found during the course of the author’s research were not comprehensively listed in this thesis, the open questions presented herein represent only a small portion of the unanswered questions available for exploration. The reader is invited to ponder the role that he or she may play in the further development of the mathematical framework, whether that be merely contemplating the ideas thus shared, investigating further areas of connection not presented herein, or by asking more questions still.

Works Cited

- Cox, David A. Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. New York: John Wiley & Sons, 1989.
- Finch, Carrie and Lenny Jones. “A Curious Connection Between Fermat Numbers and Finite Groups.” The Mathematical Association of America Monthly 109 (2002): 517–523.
- Fraleigh, John B. A First Course in Abstract Algebra. 6th ed. Reading: Addison-Wesley Publishing Company, Inc., 1999.
- Grillet, Pierre. Algebra. New York: John Wiley & Sons, Inc., 1999.
- Guillemets, Terri. “Quotations About Math.” The Quote Garden. 1998–2005. Gratia WBS Publishing. <<http://www.quote garden.com/math.html>>
- Keller, Wilfrid. “Fermat Factoring Status.” Updated August 30, 2005. <<http://www.prothsearch.net/fermat.html>>
- Křížek, Michael, Florian Luca and Lawrence Somer. 17 Lectures on Fermat Numbers: From Number Theory to Geometry. CMS Books in Mathematics. New York: Springer-Verlag, 2001.
- Long, Calvin. Elementary Introduction to Number Theory. 3rd ed. Prospect Heights: Waveland Press, Inc., 1987.
- Luca, Florian. “Fermat Primes and Heron Triangles with Prime Power Sides.” The Mathematical Association of America Monthly 110 (2003): 46–49.
- _____. “The Anti-Social Fermat Number.” The Mathematical Association of America Monthly 107 (2000): 171–173.
- Morelli, Luigi. “Distributed Search for Fermat Number Divisors: History.” Updated May 26, 2005. <<http://www.fermatsearch.org>>
- O'Connor, J J and E F Robertson. “Fermat’s Last Theorem.” Accessed August 18, 2005. <http://www-groups.dcs.st-and.ac.uk/~history/PrintHT/Fermat's_last_theorem.html>
- _____. “Pierre de Fermat.” Accessed August 18, 2005. <<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html>>
- _____. “Prime Numbers.” Accessed September 18, 2005. <http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html>

Peterson, Ivars. "Cracking Fermat Numbers." Science News Online. Volume 163, No. 9. March 1, 2003. <<http://www.sciencenews.org/articles/20030301/mathtrek.asp>>

Scharlau, Winfried and Hans Opolka. From Fermat to Minkowski: Lectures on the Theory of Numbers and Its Historical Development. New York: Springer-Verlag, 1985.

Works Referenced

Ball, W. W. Rouse. "Pierre de Fermat." A Short Account of the History of Mathematics. 4th edition, 1908. Accessed August 18, 2005.
<http://www.maths.tcd.ie/pub/HistMath/People/Fermat/RouseBall/RB_Fermat.html>

Basaldúa, Jacques. "All Fermat and Mersenne Numbers are Squarefree." 2001.
<<http://www.dybot.com/numbers/sqfree.htm>>

Caldwell, Chris. "Prime Conjectures and Open Questions." Accessed September 24, 2005. <<http://primes.utm.edu/notes/conjectures/>>

Chellani, Yogita. "Pierre de Fermat." Term Paper. Accessed August 18, 2005.
<<http://www.math.rutgers.edu/~cherlin/History/Papers1999/chellani.html>>

"Fermat Number." Wikipedia: The Free Encyclopedia. Updated September 21, 2005.
<http://en.wikipedia.org/wiki/Fermat_prime>

Hungerford, Thomas W. Algebra. Graduate Texts in Mathematics, 73. New York: Springer-Verlag, 1974.

"Pierre de Fermat." Wikipedia: The Free Encyclopedia. Updated September 10, 2005.
<http://en.wikipedia.org/wiki/Pierre_de_Fermat>

"Prime Number." Wikipedia: The Free Encyclopedia. Updated September 23, 2005.
<http://en.wikipedia.org/wiki/Prime_number>

Weisstein, Eric W. "Fermat Number." MathWorld. A Wolfram Web Resource. 1995-2005. <<http://mathworld.wolfram.com/FermatNumber.html>>

_____. "Fermat Prime." MathWorld. A Wolfram Web Resource. 1995-2005.
<<http://mathworld.wolfram.com/FermatPrime.html>>

_____. "Pierre de Fermat." Accessed August 18, 2005.
<<http://scienceworld.wolfram.com/biography/Fermat.html>>