DISCOVERING THE ART OF MATHEMATICS

NUMBER THEORY

MATHEMATICAL INQUIRY IN THE LIBERAL ARTS

Julian F. Fleron,
with Volker Ecke, Philip K. Hotchkiss and Christine von Renesse

Discovering the Art of Mathematics

Number Theory

by Julian Fleron

with Philip K. Hotchkiss, Volker Ecke and Christine von Renesse

(Rev.: 2015-9-03)

Acknowledgements

This work has been supported by the National Science Foundation under awards NSF0836943 and NSF1229515. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

These materials are also based on work supported by Project PRIME which was made possible by a generous gift from Mr. Harry Lucas.

These materials were originally developed for use in the course Mathematical Explorations at Westfield State. They are now part of the curriculum library for Discovering the Art of Mathematics, all of whose volumes are freely available at http://artofmathematics.org .

Many fine students at Westfield State have provided insight, feedback, and inspiration for this work. In particular, I would like to thank the great students in MA110 - Mathematical Explorations and MA116 - Introduction to Mathematical Systems who played an active role in the genesis of this materials and patiently worked through early drafts of this work.

As an undergraduate student Brandt Kronholm, now a Ph.D. and leading expert in partition theory, sparked my interest in partitions. He is one of those great students who you learn from more than you teach.

Thanks to Gina Kennedy and Sarah Lewison who carefully helped me revise and edit the first major draft of this work and to Jennifer Roy and Jillian Bates who helped convert the draft into LaTeX.

The Department of Mathematics at Westfield State has provided fertile ground and enthusiastic support for pedagogical innovation, scholarship on teaching and learning in mathematics, and classroom experimentation. Under the direction of Chairs Karin Vorwerk and previously John Judge, and the organization of Deb Samwell, the department continues to be deeply committed to student learning - including in its many required core courses. We are thankful to all departmental faculty, current and past, for their support of Discovering the Art of Mathematics. Colleagues that provided particular guidance, support and feedback of this volume include Marcus Jaiclin, Robert McGuigan, James Robertson, and Larry Griffith. We are grateful for the support of many at our institution over many years. In particular we thank those in Academic Affairs, our fine library faculty, Robert Martin, William Lopes, Louann D'Angelo, Elizabeth Preston, and Andrew Bonacci.

We are grateful for the support our our Advisory Board: Jere Confrey, David Farmer, Sandra Laursen, Carmel Schettino, Deborah Schifter and Dorothy Wallace. We thank Lee Zia for his guidance and encouragement.

Student interns Jillian Bates, Chelsea Baker, Joey Grabowski, Jen Roy, Rachel Cloutier, Zach Lancto, Alyssa Danilow, and Barbara Mulvaney helped with many tasks that supported the project.

Thanks to Sage Fox Consulting, Ken Rath and Emily DeHaro-Otero in particular, for their work on assessment and evaluation.

A great debt of gratitude to Tom Hoogendyk who designed and keeps running our Discovering the Art of Mathematics website.

In different incarnations, this work was reviewed and/or beta tested by George Andrews, Underwood Dudley, David Farmer, Charles Rocca, and Ethan Berkove. The author is grateful for their many insights and detailed work. Any and all imperfections remain with the author.

Of course, many other cherished people deserve thanks for helping me to develop into the mathematics teacher that I am. Many fine mathematics teachers and mathematicians enabled this work by helping inspire my own mathematical exploration. My parents Frederic and Lou Jean, step-parents Kim and Jack, my sister Ingeri, my niece K.C., and many other fine teachers helped nurture not only my intellectual curiosity, but my passion for sharing this curiosity through teaching.

Lastly, I would like to thank my partner Kris Hedblom and my kids, Addie and Jacob, great teachers who constantly remind me of the potential of all learners and the playful forms of exploration in which the best learning naturally takes.

Contents

Preface

This book is a very different type of mathematics textbook. Because of this, users new to it, and its companion books that form the Discovering the Art of Mathematics library[1], need context for the book's purpose and what it will ask of those that use it. This preface sets this context, addressing first the Explorers (students), then both Explorers and Guides (teachers) and finishing with important information for the Guides.

0.1 Notes to the Explorer

"Explorer?"

Yes, that's you - an Explorer. And these notes are for you.

We could have addressed you as "reader," but this is not a book intended to be read like a traditional book. This book is really a guide. It is a map. It is a route of trail markers along a path through part of the vast world of mathematics. This book provides you, our explorer, our heroine or hero, with a unique opportunity to explore - to take a surprising, exciting, and beautiful journey along a meandering path through a great mathematical continent.

"Surprising?" Yes, surprising. You will be surprised to be doing real mathematics. You will not be following rules or algorithms, nor will you be parroting what you have been dutifully shown in class or by the text. Unlike most mathematics textbooks, this book is not a transcribed lecture followed by exercises that mimic examples laid out for you to ape. Rather, the majority of each chapter is made up of Investigations. Each chapter has an introduction as well as brief surveys and narratives as accompaniment, but the Investigations form the heart of this book. They are landmarks for your expedition. In the form of a Socratic dialogue, the Investigations ask you to explore. They ask you to discover mathematics. This is not a sightseeing tour, you will be the active one here. You will see mathematics the only way it can be seen, with the eyes of the mind - your mind. You are the mathematician on this voyage.

"Exciting?" Yes, exciting. Mathematics is captivating, curious, and intellectually compelling if you are not forced to approach it in a mindless, stress-invoking and mechanical manner. In this journey you will find the mathematical world to be quite different from the static barren landscape most textbooks paint it to be. Mathematics is in the midst of a golden age - more mathematics is being discovered now than at any time in its long history. Each year there are 50,000 mathematical papers and books that are reviewed for *Mathematical Reviews*! Fundamental questions in mathematics - some hundreds of years old and others with $ 1 Million prizes - are

[1] All available freely online at `http://artofmathematics.org/books`.

being solved. In the time period between when these words were written and when you read them important new discoveries adjacent to the path laid out here have been made.

"Beautiful?" Yes, beautiful. Mathematics is beautiful. It is a shame, but most people finish high school after 10 - 12 years of mathematics *instruction* and have no idea that mathematics is beautiful. How can this happen? Well, they were busy learning arithmetical and quantitative skills, statistical reasoning, and applications of mathematics. These are important, to be sure. But there is more to mathematics than its usefulness and utility. There is its beauty. And the beauty of mathematics is perhaps its most powerful, driving force. As the famous **Henri Poincaré** (French mathematician; 1854 - 1912) said:

> The mathematician does not study pure mathematics because it is useful; [s]he studies it because [s]he delights in it and [s]he delights in it because it is beautiful.

Mathematics plays a dual role as a liberal art and as a science. As a powerful science, it shapes our technological society and serves as an indispensable tool and as a language in many fields. But it is not our purpose to explore these roles of mathematics here. This has been done in other fine, accessible books. Instead, our purpose is to journey down a path that values mathematics for its long tradition as a cornerstone of the liberal arts.

Mathematics was the organizing principle of the *Pythagorean society* (ca. 500 B.C.). It was a central concern of the great Greek philosophers like **Plato** (Greek philosopher; 427 - 347 B.C.). During the Dark Ages, classical knowledge was preserved in monasteries. The classical **liberal arts** organized knowledge in two components: the ***quadrivium*** (arithmetic, music, geometry, and astronomy) and the ***trivium*** (grammar, logic, and rhetoric) which were united by philosophy. Notice the central role of mathematics in both components. During the Renaissance and the Scientific Revolution the importance of mathematics as a science increased dramatically. Nonetheless, it also remained a central component of the liberal arts during these periods. Indeed, mathematics has never lost its place within the liberal arts except in contemporary classrooms and textbooks where the focus of attention has shifted solely to its utilitarian aspects. If you are a student of the liberal arts or if you want to study mathematics for its own sake, you should feel more at home on this expedition than in other mathematics classes.

"Surprise, excitement, and beauty? Liberal arts? In a mathematics textbook?" Yes. And more!

In your exploration here you will see that mathematics is a human endeavor with its own rich history of struggle and accomplishment. You will see many of the other arts in non-trivial roles: art, music, dance and literature. There is also philosophy and history. Students in the humanities and social sciences, you should feel at home here too. There are places in mathematics for anyone to explore, no matter their area of interest.

The great **Betrand Russell** (English mathematician and philosopher; 1872 - 1970) eloquently observed:

> Mathematics, rightly viewed, possesses not only truth, but supreme beauty - a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of paintings or music, yet sublimely pure and capable of a stern perfection such as only the greatest art can show.

We hope that your discoveries and explorations along this mathematical path will help you glimpse some of this beauty. And we hope they will help you appreciate Russell's claim:

> ... The true spirit of delight, the exultation, the sense of being more than [hu]man, which is the touchstone of the highest excellence, is to be found in mathematics as surely as in poetry.

Finally, we hope that your discoveries and explorations enable you to make mathematics a part of your lifelong educational journey. For, in Russell's words once again:

> ... What is best in mathematics deserves not merely to be learned as a task but to be assimilated as a part of daily thought, and brought again and again before the mind with ever-renewed encouragement.

Bon voyage. May your journey be as fulfilling and enlightening as those that have beaconed people to explore the many continents of mathematics throughout humankind's history.

0.2 Navigating This Book

Intrepid Explorer, as you ready to begin your journey, it may be helpful for us to briefly describe basic customs used throughout this book.

As noted in the Preface, the central focus of this book is the **Investigations**. They are the sequences of problems that will help guide you on your active exploration of mathematics. In each chapter the Investigations are numbered sequentially in bold. Your role will be to work on these Investigation individually or cooperatively in groups, to consider them as part of homework assignments, to consider solutions to selected Investigations that are modeled by your fellow explorers - peers or your teacher - but always with you in an active role.

If you are stuck on an Investigation remember what **Frederick Douglass** (American slave, abolitionist, and writer; 1818 - 1895) told us:

> If there is no struggle, there is no progress.

Or what **Shelia Tobias** (American mathematics educator; 1935 -) tells us:

> There's a difference between not knowing and not knowing *yet*.

Keep thinking about the problem at hand, or let it ruminate a bit in your subconscious, think about it a different way, talk to peers, or ask your teacher for help. If you want you can temporarily put it aside and move on to the next section of the chapter. The sections are often somewhat independent.

Independent Investigations are so-called to point out that the task is more involved than the typical Investigations. They may require more significant mathematical epiphanies, additional research outside of class, or a significant writing component. They may also signify an opportunity for class discussion or group reporting once work has reached a certain stage of completion.

The **Connections** sections are meant to provide illustrations of the important connections between the mathematics you're exploring and other fields - especially in the liberal arts. Whether you complete a few of the Connections of your choice, all of the Connections in each section, or are asked to find your own Connections is up to your teacher. We hope that these Connections sections will help you see how rich mathematics' connections are to the liberal arts, the fine arts, culture, and the human experience.

Further Investigations, when included, are meant to continue the Investigations of the mathematical territory but with trails to significantly higher ground. Often the level of sophistication of these investigations will be higher. Additionally, our guidance will be more cursory - you are bushwhacking on less well-traveled trails.

In mathematics, proof plays an essential role. Proof is the arbiter for establishing truth and should be a central aspect of the sense-making at the heart of your exploration. Proof is reliant on logical deductions from agreed upon definitions and axioms. However, different contexts suggest different degrees of formality. In this book we use the following conventions regarding **definitions**:

- An *Undefined Term* is italicized the first time it is used. This signifies that the term is: a standard technical term which will not be defined and may be new to the reader; a term that will be defined a bit later; or an important non-technical term that may be new to the reader, suggesting a dictionary consultation may be helpful.
- An ***Informal Definition*** is italicized and bold- faced the first time it is used. This signifies that an implicit, non-technical, and/or intuitive definition should be clear from context. Often this means that a formal definition at this point would take the discussion too far afield or be overly pedantic.
- A **Formal Definition** is bolded the first time it is used. This is a formal definition that is suitably precise for logical, rigorous proofs to be developed from the definition.

In each chapter the first time a **Biographical Name** appears it is bolded and basic biographical information is included parenthetically to provide historical, cultural, and human connections.

In mapping out trails for your explorations of this fine mathematical continent we have tried to uphold the adage of **George Bernard Shaw** (Irish playwright and essayist; 1856 - 1950):

> I am not a teacher: only a fellow-traveler of whom you asked the way. I pointed ahead – ahead of myself as well as you.

We wish you wonderful explorations. May you make great discoveries, well beyond those we could imagine.

0.3 Directions for the Guides

Faithful Guide, you have already discovered great surprise, beauty and excitement in mathematics. This is why you are here. You are embarking on a wonderful journey with many explorers looking to you for bearings. You're being asked to lead, but in a way that seems new to many.

We believe telling is not teaching. Please don't tell them. Answer their questions with questions. They may protest, thinking that listening is learning. But we believe it is not.

This textbook is very different from typical mathematics textbooks in terms of structure (only questions, no explanations) and also of expectations it places on the students. They will likely protest, "We're supposed to figure this out? But you haven't explained anything yet!" It is important to communicate this shift in expectations to the students and explain some of the reasons. That's why we have written the earlier sections of this preface, which can help do the explaining for us (and for you).

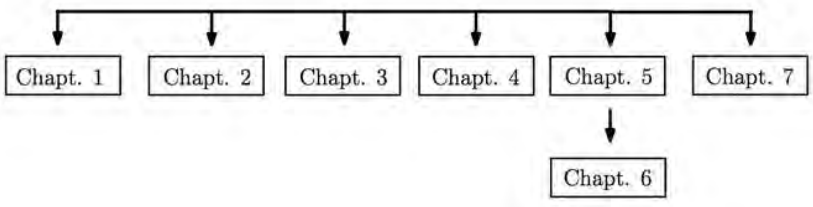
You need support as well. A shift in pedagogy to a more inquiry-based approach may be subtle for some, but for many it is a great leap. Understanding this we have assembled an online resource to support teachers in the creation and nurturing of successful inquiry-based mathematics classrooms. Available online at `http://artofmathematics.org/classroom` it contains a wealth of information - in many different forms including text, data, videos, sample student work - on many critical topics:

- Why inquiry-based learning?
- How to get started using our books...
- A culture of curiosity
- Learning contracts
- Grouping students
- Choosing materials - Mixing It Up
- Asking good questions
- Creating inquiry-based activities
- Making mistakes
- Cool things
- Proof as sense-making
- Homework stories
- Exams
- Posters
- Assessment: Student Solution Sets
- Evaluating the effectiveness of inquiry-based learning
- ... and much more ...

We wrote the books that make up the Discovering the Art of Mathematics library because they have helped us have the most extraordinary experiences exploring mathematics with students who thought they hated mathematics and had been disenfranchised from the mathematical experience by their past experiences. We are encouraged that others have had similar experiences with these materials. We love to hear success stories and are also interested in hearing about things that might need to be changed or did not work so well. Please feel free to share your stories and suggestions with us: `http://artofmathematics.org/contact`.

0.3.1 Chapter Dependencies

Guides are encouraged to pick and choose topics freely, from this book and others in the Discovering the Art of Mathematics series, depending on their interests and those of their students. The chapter dependencies in this book, with first level chapters independent and arrows emanating from them indicating which chapters are dependent, are as follow:



Chapter 1

Introducing Number Theory

> Mathematics is the queen of the sciences and number theory the queen of mathematics.
>
> **Carl Friedrich Gauss** (German Mathematician; 1777 - 1855)

> ...number theory. It is a field of almost pristine irrelevance to everything except the wondrous demonstration that pure numbers, no more substantial than Plato's shadows, conceal magical laws and orders that the mind can discover after all.
>
> **Newsweek Magazine** (New Answer for An Old Problem; 5 July - 1993)

Number theory is the name given by mathematicians to the study of whole numbers and the patterns, relationships, laws, and properties that govern these numbers. Our school experiences with whole numbers were often characterized by memorizing multiplication tables, learning long division algorithms, computing mysterious *greatest common divisors*, and the like, so you might not agree with **Carl Freidrich Gauss** (German Mathematician; 1777 - 1855) that this is a very regal area. And you might be hesitant to give it another look. Might $1 million change your mind?

1.1 $1 Million Dollar Problems

You will probably remember that a **prime number** is a positive integer whose only divisors are 1 and itself. So, for example, the numbers 2, 3, 5, 7, and 11 are the first five primes. (Contemporary mathematicians do not consider the number 1 a prime.[1] In a letter dated 7 June, 1742[2], **Christian Goldbach** (Prussian Mathematician; 1690 - 1764), a mathematician of little renown outside of this letter, wrote to **Leonhard Euler** (Swiss Mathematician; 1707 - 1783), who we meet often across many areas of mathematics, that he had observed the following pattern:

[1] Otherwise it would complicate the *fundamental theorem of arithmetic* whose name you may not recognize, but who you have seen and will see again later in this book.

[2] A copy of the letter is available at `http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf`.

$$
\begin{array}{cc}
2 = 1 + 1 & 3 = 1 + 1 + 1 \\
4 = 1 + 3 & 5 = 1 + 1 + 3 \\
6 = 3 + 3 & 7 = 1 + 3 + 3 \\
8 = 3 + 5 & 9 = 3 + 3 + 3 \\
10 = 5 + 5 & 11 = 3 + 3 + 5 \\
12 = 5 + 7 & 13 = 3 + 5 + 5 \\
14 = 7 + 7 & 15 = 5 + 5 + 5 \\
16 = 5 + 11 & 17 = 5 + 5 + 7 \\
18 = 5 + 13 & 19 = 5 + 7 + 7 \\
20 = 7 + 13 & 21 = 7 + 7 + 7 \\
22 = 11 + 11 & 23 = 5 + 5 + 13 \\
24 = 11 + 13 & 25 = 3 + 11 + 11 \\
26 = 13 + 13 & 27 = 5 + 11 + 11 \\
\vdots & \vdots
\end{array}
$$

On the basis of this *inductive* evidence, Goldbach surmised, or, as mathematicians would say, ***conjectured***, that any even positive integer could be written as the sum of two primes and any odd positive integer could be written as the sum of three primes.[3] These conjectures are known, appropriately, as **Goldbach's two-prime conjecture** and **Goldbach's three-prime conjecture**.

Progress has been made on the three-prime result since breakthrough work of **Ivan Matveevich Vinogradov** (Soviet mathematician; 1891 - 1983) in the 1930's. In fact, a 14 June, 2013 paper by **Harald Helfgott** (Peruvian mathematician; 1977 -), which he posted online at the electronic database ***arXiv***[4], claims a proof of this result. In other words, finally, after more than 250 years, the "easier" problem may have been solved.

What about the harder, more important two-prime result? The problem is so compelling it played a central role in the notable novel Uncle Petros and Goldbach's Conjecture by **Apostolos Doxiadis** (Greek author; 1953 -). When this 1992 novel was translated and published in English in 2000 its publisher offered a $1 million dollar prize to anybody who could definitively resolve Goldbach's two-prime conjecture! The prize was not claimed. In other words, the problem remains unresolved to this day despite tremendous efforts of mathematicians world-wide for two and one-half centuries and a 1$ million dollar prize.

In Chapter 5 you will investigate two other $1 Million problems, the *Riemann hypothesis* and the *Birch and Swinnerton-Dyer* conjecture.

1.2 High Drama

Intrigued? Many are. In fact, number theory has recently served as the vehicle for several major theatrical productions. The Tony Award and Pulitzer Prize winning Broadway play Proof[5] by

[3] In the time of Goldbach it was typical for mathematicians to consider 1 to be prime. Contemporary mathematicians limit the conjectures to even numbers greater than 4 and odd numbers greater than 7 as 1 is no longer considered a prime. See **??** for the rationale for this distinction.

[4] Available at the `http://arxiv.org/abs/1305.2897`.

[5] This play was subsequently made into a full-length movie starring Gwyneth Paltrow, Anthony Hopkins, and Jake Gyllenhaal.

David Auburn (American playwright; 1969 -), revolves around the obsessions of an aging mathematician and his daughter, a mathematical prodigy who cares for her psychologically unstable father, with number theoretic questions. While the open mathematical question whose "proof" serves as a metaphor for this moving drama is never revealed, it could very well be Goldbach's conjecture.

> Proof depicts the study of mathematics as a painful joy, not as the geek-making obsession of stereotype, but as human labor, both ennobling and humbling, by people who, like musicians or painters (or playwrights), can envision an elusive beauty in the universe and are therefore both enlivened by its pursuit and daunted by the commitment. It does this not by showing them at work but by showing them trying to live or cope when they can't, won't or simply aren't, and in doing so makes the argument that mathematics is a business for the common heart as well as the uncommon brain.[6]

In the Golden Globe winning and Oscar nominated movie A Beautiful Mind, the mathematical insights of Nobel prize-winning mathematician **John Nash** (American Mathematician; 1928 -) are portrayed visually through whole number patterns seen in arrays of encrypted messages.[7] Although Nash's insights were extraordinary, an ability to discover patterns and relationships like this are critical to most mathematicians' work.

1.3 What Good is This?

In our exploration of number theory, you might wonder "what good is this?" Some applications of number theory in the first few topics – to art, architecture, biology – are immediate. *Fermat's Last Theorem*, *partition congruences*, and the content of later topics have applications and implications that are beyond the level of this text. But a single example will provide some proper sense of the scope of number theory's applications: secret codes or ***encryption*** as it is more properly known.

Secret messages have a long history, at least as far back as the *Caesar ciphers* named after **Julius Caesar** (Roman general, statesman, and author; 100 BC - 44 BC). In the Second World War the Allies superior encryption and decryption proved critical to their eventual victory. Central to the Allies' efforts were the roles of the Navajo "code talkers" in keeping classified U.S. transmissions secret and of British and Polish mathematicians, led by the brilliant but persecuted **Alan Turing** (English Mathematician; 1912 - 1954), in deciphering the German *Enigma* codes.[8] In contemporary communication information is secured by encryption schemes like the *RSA algorithm* and the *Advanced Encryption Standard*[9] which are based squarely on patterns, methods, and algorithms from number theory. Without the development, testing, refinement and implementation of these algorithms by thousands of mathematicians and engineers we could not: send classified military information, have secure ATM access, have secure credit card transactions, have secure

[6] From the review "A common heart and uncommon brain," by Bruce Weber, *New York Times*, 24 May, 2000, E1,3.

[7] The movie took some dramatic license in these scenes. There is little evidence in the book on which the movie is based, A Beautiful Mind: The Life of Mathematical Genius and Nobel Laureate John Nash by **Sylvia Nasar** (German journalist; 1947 -), that Nash worked with or thought about encryption of this sort.

[8] See the section Additional Investigations for more on the Navajo code talkers and Alan Turing.

[9] Beginning in May, 2002, the National Institute for Standards and Technology specified the Advanced Encryption Scheme for use "by U.S. Government organizations (and others) to protect sensitive information." See `csrc.nist.gov/` for more information.

email or Internet communication and data sharing, and so on. The Information Age in which we live would be a ghost of what it now is. A broad variety of accessible material on encryption is available. (See e.g. [Flan], [Sin], [Gar], [Bur; Ch. 7, Sect. 5], [Kah].)

1.4 Recent Breakthroughs

In addition to the numerous applications of number theory that pervade the Information Age, there have been many stunning breakthroughs on the more theoretical side of number theory during the past few decades. In 1993, **Andrew Wiles** (English Mathematician; 1953 -) shocked the world by discovering/inventing a proof of *Fermat's Last Theorem*, not only the most famous and long-standing problem in number theory, but in all of mathematics. We'll discover more about the mathematical story of Fermat's Last Theorem and its solution, an event that appeared on the front page of the *New York Times*[10] and resulted in Wiles being named as one of *People Magazine's* "25 Most Intriguing People of 1993". We will investigate the surprising extensions made by **Ken Ono** (American mathematician; 1968 -) on the hundred year old work on *partition congruences* by the remarkable **Srinivasa Ramanujan's** (Indian Mathematician; 1887 - 1920). And we will investigate twin primes, learning about **Yitang Zhang** (Chinese mathematician; 1955 -) who shocked the world on April 17, 2013 with his *bounded gaps theorem* which nearly solves a centuries old effort to understand how many twin primes there are.

Each of these events of the last 25 years will be remembered as key chapters in the history of mathematics even 1000 years from now. These offer strong challenges to the widespread misperceptions of mathematics as a static, completed, archaic field, don't they?

1.5 Yeah, But Can *We* Do It?

Assuming you are now intrigued by these historical, humanistic, and utilitarian aspects of number theory, you might wonder whether we can actually explore any significant number theory. They're offering million dollar prizes and people get their picture on the front page of the *New York Times* for solving these problems. It sounds daunting. **Godfrey H. Hardy** (English Mathematician; 1877 - 1947), one of the foremost number theorists of all times, offers enthusiastic encouragement:

> The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and at least ten times as entertaining as the same amount of "calculus for engineers."

Indeed, despite its tantalizing, centuries-old problems and the extreme importance of its applications, there are great stories of number theory's accessibility. Later we will meet **Rhiannon L. Weaver** (American student; -), a Penn State undergraduate who contributed a critical sequel to Ken Ono's work on partition congruences. And there is **Sarah Flannery** (Irish student; 1982 -),

[10] 24 June, 1993; the day after Wiles announced his proof at the end of three lectures he gave at a conference in Cambridge, England.

a high school student who gained international acclaim by developing an encryption algorithm that originally was thought to have been a dramatic improvement over the universal encryption standard set by the RSA algorithm. She was awarded Ireland's Young Scientist of the Year Award, awarded Europe's Young Scientist of the Year Award, and was featured in news media reports worldwide. Her memoir, In Code: A Mathematical Journey, is a wonderful account of the fascination that can be found in mathematics if given the opportunity and encouragement to explore rather than the mundane tasks of memorizing and regurgitating. And we'll investigate some of the mathematics of *partitions* which is the area that **Kaavya Jayram** (Indian student; 1998 -) investigates. At age 12 she had a paper on this topic published in the prestigious *International Journal of Number Theory*.

So here's your opportunity.

Chapter 2

Fibonacci Numbers

> All is number.
>
> **The Pythagoreans** (Greek sect/cult; 500 BC - 200 BC)

> In mathematics, if a pattern occurs, we can go on to ask, Why does it occur? What does it signify? And we can find answers to these questions. In fact, for every pattern that appears, a mathematician feels [s]he ought to know why it appears.
>
> **W. W. Sawyer** (English mathematician and author; 1911 - 2008)

> Music is a hidden arithmetic exercise of the soul, which does not know that it is counting.[1]
>
> **G.W. Leibniz** (German mathematician; 1646 - 1716)

To everything there is a number. There is one you. Two eyes looking at this page. Three figures in the Christian trinity. Four legs on a chair. Five petals on the columbine flower. Six legs on insects. Seven is lucky. Eight counter-clockwise spirals of seeds on some pinecones. So many things to count. And from such counting, remarkable relationships and connections can emerge. Some are spurious, curiosities to the ***numerologists*** who use number mysticism as astrologers use the signs of the Zodiac. The ***Pythagoreans***, the important sixth century B.C. sect of Greek mathematicians, and other important mathematicians have dabbled in numerology. Yet it is a subject short on substance, long on coincidence and happenstance.[2] When mathematicians see relationships and connections among numbers they seek to discover underlying causal patterns and mechanisms. For mathematics is the science of patterns.[3]

2.1 A Remarkable Sequence of Numbers

In botany a particularly compelling pattern of numbers emerges. When we count the number of petals on many different types of flowers, the number of spirals that appear on the surface textures of many fruits, and the arrangement of leaves on tree branches they usually do not find a random

[1] Written on 17 April, 1712 in a letter to Christian Goldbach who we have already met.

[2] See the wonderful book Numerology, or, What Pythagoras Wrought by Underwood Dudley, Mathematical Association of America, 1997 for a vigorous debunking of numerology.

[3] While the statement "Mathematics is the science of patterns" is a bit of an oversimplification, contemporary mathematicians generally agree this is about as good as can be done in a single sentence. See the book Mathematics: The Science of Patterns by Keith Devlin for a comprehensive discussion.

collection of numbers. Rather, the numbers $5, 89, 13, 34, 8, 21, 55, 144$, and 3 occur repeatedly and almost exclusively.

13 year-old **Aidan** (American student; 1998 -) built a tree whose leaf patterns were modeled on these numbers out of PVC pipe and solar panels which demonstrated a 50% improvement over flat-panel solar collection. His research on this topic, at age 13, won him the 2011 Young Naturalist Award from the American Museum of Natural History.[4] His research essay concludes with the line, "But the best part of what I learned was that even in the darkest days of winter, nature is still trying to tell us its secrets."

Arranged as they are above there might not seem to be anything striking about these numbers. But, in numerical order the numbers

$$3, 5, 8, 13, 21, 34, 55, 89, 144$$

form a clear pattern. Each number is the sum of the two that come before it. Using this we can extend the pattern forward and backward:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

These numbers are called the **Fibonacci numbers**.

The Fibonacci numbers are denoted by $f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3$ and so on. By definition, each new Fibonacci number is obtained by adding the previous two Fibonacci numbers. Hence the **defining relation of the Fibonacci numbers** is expressed algebraically as $f_n = f_{n-1} + f_{n-2}$ subject to the *initial conditions* $f_1 = 1$ and $f_2 = 1$. This is a *recurrence relation*: to calculate a Fibonacci number you need to know the previous Fibonacci numbers.

In the Investigations below you will see a few of the varied situations in which the Fibonacci numbers arise. Despite its regular occurence in botany, this was the the genesis of the sequence. Instead, the sequence first appeared as a solution of a typically hokey word problem, one about rabbits, that appeared in an important mathematical text published in 1202 by a mathematician nicknamed Fibonacci.

2.2 Fibonacci

Like all other areas of learning, mathematics was dormant during the long Dark Ages (circa 450 - 1000 A.D.) in Europe. While mathematics awoke gradually over the two hundred years following the Dark Ages, its rejuvenation is marked most precisely by the works of Fibonacci. Properly named **Leonardo of Pisa** (Italian mathematician; 1175 - 1250), this son of a well-known Italian merchant was better known as **Fibonacci** (a contraction of filus Bonaccio, "son of Bonaccio"). Fibonacci traveled widely as a student, learning methods of Arabic mathematics when studying in Northern Africa and learning the system of Hindu-Arabic numerals. Fibonacci assembled what he had learned into Liber Abaci (literally "book of the abacus", meaning book of arithmetic), the most comprehensive book of arithmetic of its time. It laid out the benefits of the Hindu-Arabic numeral system and is partially responsible for its wide acceptance subsequently. Fibonacci went on to publish several other books that focused mainly on arithmetic and algebra. These textbooks and his success in mathematical competitions in the court of Emperor Frederick II established him as the premier mathematician of the age.

[4] See `http://www.amnh.org/learn-teach/young-naturalist-awards/winning-essays2/2011-winning-essays/the-secret-of-the-fibonacci-sequence-in-trees` for details.

Figure 2.1: Aidan's solar panel Fibonacci tree.

2.3 Fibonacci's Problem

Despite his impact on the revival of mathematics and the acceptance of the Hindu-Arabic numeral system, Fibonacci's most widespread notoriety comes from a single problem from among the hundreds that he used in Liber Abaci to illustrate the importance of the ideas laid out in this textbook. Fibonacci's famous problem was:

> How many pairs of rabbits will be produced in a year, beginning with a single pair, if in every month each pair bears a new pair which becomes productive from the second month on?

If we represent each pair of juvenile rabbits by xy and each pair of mature rabbits by XY, we can trace the number of rabbit pairs over the months as follows:

It was from this somewhat artificial word problem, not their appearance in nature, that the Fibonacci numbers were first discovered. Since their discovery they have, like breeding rabbits, flourished.

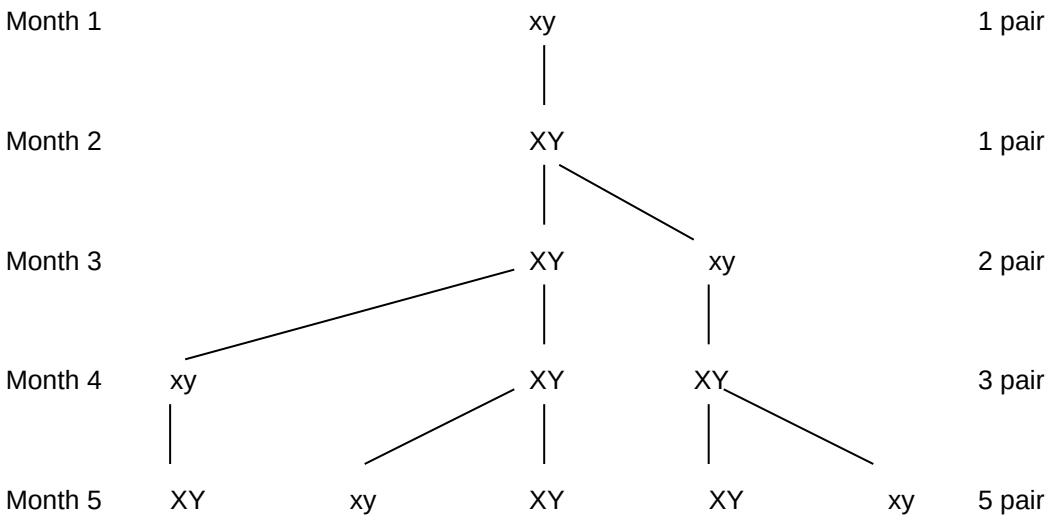


Figure 2.2: Fibonacci's rabbits

2.4 Fibonacci's Rabbits

1. Continue the breeding tree in Figure 2.2 for three more months, checking that it yields the next three Fibonacci numbers. (You might find it useful to use different colors rather than symbols to distinguish mature from juvenile rabbit pairs.)

2. Answer Fibonacci's question: how many pairs will be produced in a year?

We would like to know why the pattern of Fibonacci numbers appears in this hypothetical population.

3. Determine the number of adult rabbit pairs in each of the months $2-8$. What do you notice?

4. How can the number of adult rabbit pairs in a given month be determined by the number of rabbit pairs in earlier months?

5. Determine the number of juvenile rabbit pairs in each of the months $2-8$. What do you notice?

6. How can the number of juvenile rabbit pairs in a given month be determined by the number of rabbit pairs in earlier months? Explain why this happens.

7. Use Investigation **3** - Investigation **6** to prove that the number of pairs of rabbits must also follow the defining relation $f_n = f_{n-1} + f_{n-2}$ of the Fibonacci numbers.

8. Determine the twentieth Fibonacci number

9. How hard would it be to determine the fiftieth Fibonacci number? (Note: In Topic 2 we will revisit this problem.)

Figure 2.3: Spirals in a pinecone and a sunflower

2.5 Fibonacci Spirals in Nature

In Figure 2.3 are images of a pinecone and a sunflower. Their seeds emerge from the center, where the cone and flower are attached to the plant. As they develop at this *meristem*, the seeds (which are actually *cone scales* or *fruits* in this case and are known collectively as *primordia* in their developmental phase) grow and move outward away from the meristem. As they do so they form a regular pattern. Your eyes should see spiral arcs made from sequences of adjacent seeds, some that move away from the meristem in clockwise manner and others that move away from the meristem in a counter-clockwise manner.

In the appendix there are several copies of these images.

10. Using a marker, color one of the spiral arcs in the pinecone that moves in a clockwise manner from the outer edge of the image to the center of the meristem. You will note that the spiral arc doesn't continue perfectly at the center of the meristem. Skip over the spiral that is adjacent to the one you just colored and color the next one that appears to have the same orientation after that. Continue this way around the pinecone until you have colored as many non-adjacent spiral arcs in the clockwise family as you can. How many clockwise spiral arcs are there?

11. Using a different color marker and another copy of the image of the pinecone, color the counter-clockwise family of spiral arcs in the same way that you colored the clockwise family. How many counter-clockwise spiral arcs are there?

12. Repeat Investigation **10** for the sunflower.

13. Repeat Investigation **11** for the sunflower.

14. What is surprising about your answers to Investigation **10** - Investigation **13**?

15. Pinecones and sunflowers come in many varieties, some tightly packed and some more openly packed. Would you be surprised to learn that the number of spiral arcs in virtually all pinecones and sunflowers are Fibonacci numbers? Indeed, Fibonacci numbers appear often in flowers and seed-pods. Find several other specific examples.

2.6 Honeybee Family Trees

A typical honeybee hive consists of a single queen, upwards of 200 drones, and 20,000 or more worker bees. The queen and worker bees are female, while the drones are male. All offspring are produced by the queen, the worker bees do not reproduce. The drones' role is to help in reproduction. Fertilized eggs result in either a new queen or worker bees while unfertilized eggs result in drones. That is, all females - whether a new queen or the worker bees - have a mother, the queen, and a father, a drone. Drones only a mother, the queen, but no father.

16. Using the standard symbols for male and female, ♂and ♀, respectively, make a family tree of a male bee that goes back five generations.

17. Use the family tree in Investigation **16** to determine the number of i) parents, ii) grandparents, iii) great-grandparents, iv) great-great-grandparents, and v) great-great-great-grandparents a male bee has. What do you notice about these numbers?

18. Using the standard symbols for male and female, ♂and ♀, respectively, make a family tree of a female that goes back five generations.

19. Use the family tree in Investigation **18** to determine the number of i) parents, ii) grandparents, iii) great-grandparents, iv) great-great-grandparents, and v) great-great-great-grandparents a female bee has. What do you notice about these numbers?

Honeybees bring to mind two other mathematical marvels. First, bees build their honeycomb in hexagonal cells because this *regular tessellation* provides the optimal storage for a given use of wax. Bees are mathematicians of some merit!

More impressively, honeybees communicate the location of pollen sources with an intricate *waggle dance*. This dance was successfully translated only during the middle of the twentieth century. The ability of honeybees to communicate using such a sophisticated grammar remained a mystery until recently. In the mid 1990s the mathematician **Barbara Shipman** (; -) discovered that the grammar for the waggle dance language can be described by the same *higher dimensional flag manifolds* that are critical tools in the description of certain quantum mechanical fields and quantum mechanical interactions. [5]

As Galileo said,

[5]The article "Quantum honeybees" by Adam Frank, *Discover*, November, 1997, pp. 80-87 has an accessible description of Shipman's discoveries.

> The universe stands continually open to our gaze, but it cannot be understood unless one first learns to comprehend the language and interpret the characters in which it is written. It is written in the language of mathematics.

Our ability to see this in any facet of the natural, physical, and human world is limited only by our mathematical imagination. Shipman just happened to be a topologist studying higher dimensional flag manifolds and the daughter of a beekeeper who learned about the waggle dance from her father as a small child.

For more on both of these interesting topics, see the chapter "What's Worth Knowing?" in Discovering the Art of Mathematics - Student Toolbox.

2.7 Plant Growth

Fibonacci's rabbit problem is certainly not realistic. Rabbits do not produce in such a regular way and they die. Nonetheless, it is not difficult to envision situations where such growth is more realistic.

Consider the growth of a plant. As a plant grows a new shoot this shoot is not immediately ready to produce a new shoot of its own right away. Suppose the shoot has to grow two weeks before it can give rise to exactly one new shoot and then it is able to grow one new shoot each week thereafter. If each shoot behaves in this way a like this will, four weeks after germination, look like:

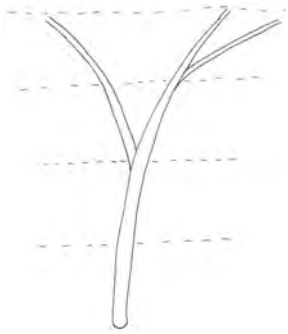


Figure 2.4: A four week old Fibonacci Plant

20. Draw the plant in Figure 2.4 after six weeks.

21. Draw the plant in Figure 2.4 after nine weeks. (Note: You might use the same coloring techniques as you applied with the rabbits to help you.)

22. What do you notice about the number of shoots on this plant at the end of each week?

23. Prove why, in this situation, the number of shoots is always a Fibonacci number.

One plant that exhibits this type of growth is the *sneezewort*.

2.8 Two Fibonacci Identities

One of the reasons for mathematicians' fascination with Fibonacci numbers is the many patterns and settings in which they arise. In fact, there is an entire journal, the *Fibonacci Quarterly*, devoted to the Fibonacci numbers and other similar numbers.

You will investigate two well-known identities here.

24. Write down and then evaluate the sum of the first three Fibonacci numbers; i.e., $1+1+2=$?

25. Write down and then evaluate the sum of the first four Fibonacci numbers.

26. Write down and then evaluate the sum of the first five Fibonacci numbers.

27. Write down and then evaluate the sum of the first six Fibonacci numbers.

28. Write down and then evaluate the sum of the first seven Fibonacci numbers.

29. How are the sums in Investigation **24** - Investigation **28** related to the Fibonacci numbers? State a conjecture regarding the value of the sum of the first n Fibonacci numbers.

30. Add the eighth Fibonacci number, 21, to each side of your equation in Investigation **28**. Can you see how this generates the correct result for the sum of the first eight Fibonacci numbers?

31. Generalize Investigation **30**. That is, show that if you add the $(n+1)^{st}$ Fibonacci number to each side of your equation in Investigation **29** this will generate the correct next stage.

32. Does this prove that your result in Investigation **29** is correct for all values of n? Explain.

Pascal's triangle is the triangular array of numbers in Figure 2.5. Each entry is obtained by adding the two numbers in the previous row that are closest to the entry being obtained.

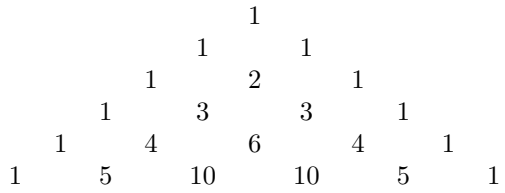


Figure 2.5: Pascal's Triangle

33. Determine the next three rows in Pascal's triangle.

The importance of Pascal's triangle lies in the fact that it catalogues the *binomial coefficients*. For example, when expanding $(x+y)^2$ we get $1x^2+2xy+1y^2$ and these coefficients are exactly those in the second row of Pascal's triangle. (Note: The row which contains the single entry 1 is called the zeroth row.)

Pascal's triangle is named after **Blaise Pascal** (French mathematician, philosopher and inventor; 1623 - 1662). By the age of nineteen Pascal had invented the first working mechanical calculator and precursor to the modern computer. He "discovered" Pascal's triangle in his mid twenties while investigating the mathematical nature of gambling problems, work which would lead to the development of what we now called the field of mathematical probability. By the age of 30 he withdrew from his mathematical and scientific efforts to focus on philosophy and religion.[6]

Like many other mathematical objects, Pascal's triangle is named for the first person whose research utilizing the object had far-reaching effects. Often these are not the first discoverers. Pascal's triangle was known in many other non-European cultures hundreds of years earlier.

34. Expand $(x+y)^3$ and show that the coefficients are correctly given by the third row of Pascal's triangle.

35. Make a conjecture about the expansion of $(x+y)^6$.

36. Add the entries in the individual rows of Pascal's triangle. What pattern do you see?

We cannot add the columns or diagonals of Pascal's triangle because they go on forever. But one can add the *shallow diagonals*. The first shallow diagonal contains the left-most 1 in the fourth row and the 2 in the third row. The second shallow diagonal contains the left-most 1 in the fifth row, the left-most 3 in the fourth row, and the right-most 1 in the third row.

37. What are the sums of the first and second shallow diagonals?

38. What numbers make up the third shallow diagonal and what is their sum?

39. What numbers make up the fourth shallow diagonal and what is their sum?

40. What numbers make up the fifth shallow diagonal and what is their sum?

41. What do you notice about the sums of the shallow diagonals?

There are many other fabulous patterns hidden in Pascal's triangle. The interested reader is invited to look up the term *Polya block walking* in any book on *combinatorics* for interesting ways to generate them.

2.9 The Mandelbrot Set

Pictured in Figure 2.6, the **Mandelbrot set** is one of the most famous sets in mathematics. It is an important example of a fractal - a mathematical object that is approximately self-similar across an infinity of scales. This set was named after **Benoît Mandelbrot** (French mathematician; 1924 - 2010) who, as an IBM researcher in the 1970s, was the first to use computers to explore visually the complex mathematical objects that had been first investigated by **Pierre Fatou** (French mathematician; 1878 - 1929) and **Gaston Julia** (French mathematician; 1893 - 1978). Fractals play a critical role in many natural and physical processes. A wealth of sophisticated, beautiful,

[6] Elementary Number Theory, 4th edition, by D.M. Burton, p. 10.

interactive Internet sites on fractals exist and there are accessible texts that could be used in parallel with this text.[7]

You will need to work through this section with the help of the Internet. In particular, you will need interactive scripts that enable you to view microscopic features of the Mandelbrot set by zooming in repeatedly. There are many sites where this can be done, but we recommend the Julia and Mandelbrot Explorer located at `http://aleph0.clarku.edu/~djoyce/julia/explorer.html` .

You must be aware that as you zoom in you will lose resolution when you employ the default settings. To regain resolution after repeatedly zooming in you will have to increase the number of *iterations* that the script uses to produce the images.

The Mandelbrot set looks a bit like a beetle that has smaller beetles that appear regularly around its boundary. No matter how far you zoom in you will continue to see these structures, which are called *bulbs*. In Figure 2.6, the rear cusp of the Mandelbrot set, the dimple on the right edge at 3:00, is called bulb 1. The front bud, the largest, circular bud on the left at 9:00, is called bulb 2. Label these bulbs. If we locate the largest bulb along the top half of the Mandelbrot set between the cusp labeled 1 and the bulb labeled 2 we see it is located right at the top of the Mandelbrot set, at 12:00. At the tip of this bulb there is a thin filament that splits into two branches. The filaments play a critical role in this bud's mathematical significance so we will label this bulb 3.

42. Locate the largest bulb along the top half of the Mandelbrot set between the bulb labeled 2 and the bulb labeled 3. Zoom in on this bulb so you can determine the number of filaments that make up the starburst at the tip of this bulb. This number will be the label for this bulb.

43. Now locate the largest bulb between the bulb labeled 3 and the one you found in Investigation **42**. Zoom in on it so you can determine the number of filaments that make up the starburst at its tip. This number will be the label for the bulb.

44. Repeat Investigation **43**, locating and labeling the largest bulb that appears between the bulbs you found in Investigation **42** andInvestigation **43**.

45. Repeat Investigation **43** again, locating and labeling the largest bulb that appears between the bulbs you found in Investigation **43** and Investigation **44**.

46. Repeat Investigation **43** again, locating and labeling the largest bulb that appears between the bulbs you found in Investigation **44** and Investigation **45**.

47. Are you surprised by the pattern you are finding?

[7]The classic book in this field in Mandelbrot's The Fractal Geometry of Nature, W.H. Freeman, 1983. Chaos and Fractals: New Frontiers in Science by Heinz-Otto Peitgen, Martmust Jurgens, and Dietmar Saupe, Springer-Verlag, 1992 is a beautiful book as well. The text Chaos Under Control: The Art and Science of Complexity by David Peak and Michael Frame, W.H. Freeman, 1994 was designed specifically for mathematics for liberal arts courses and is most highly recommended for this audience. Internet sites abound. In addition to the two above, the Dynamical Systems and Technology Project at Boston University – http://math.bu.edu/DYSYS/ and Mary Ann Connors Exploring Fractals site – http://www.math.umass.edu/ mconnors/fractal/fractal.html are excellent places to start.

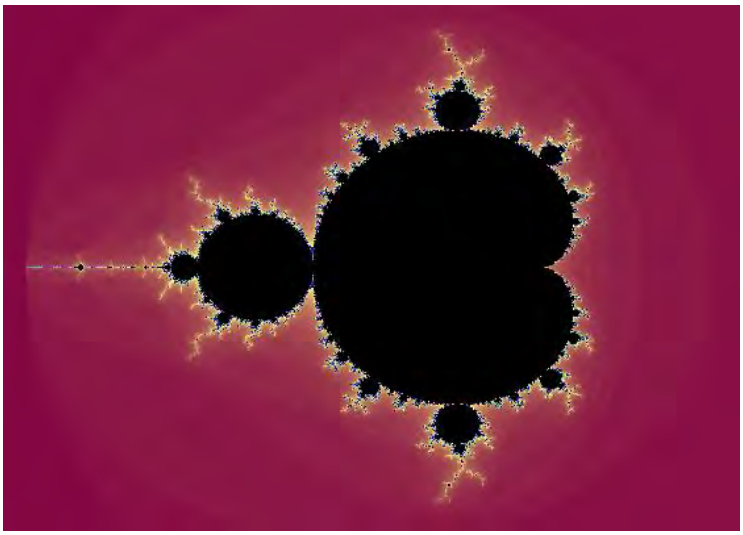


Figure 2.6: The Mandelbrot Set

48. Spend a few minutes zooming in on the filaments off the end of any single bud you have considered. Are the filaments just wisps of fractal dust or are there surprises hidden in them? Explain.

2.10 Fibonacci Numbers Everywhere?

Fibonacci numbers certainly capture the imagination. They have achieved an almost cult-like following, especially on the Internet where all sorts of mathematical aficionados pay homage to them. Some dubious occurrences of Fibonacci numbers are mixed below with some meritorious occurrences. Which is which?

49. You have 2 hands. 2 is a Fibonacci number. What else about your hands has Fibonacci numbers?

50. Slice open an apple, banana, or tomato. There are structures to count. Are there numbers in each of these structures that are Fibonacci numbers? What about other fruits and vegetables?

51. Consider the keys on a piano that make up an octave, as pictured in Figure 2.7. Where do you see Fibonacci numbers?

52. In basketball there are five players on each team. Five is a Fibonacci number. There are many other Fibonacci numbers related to the players, positions, and scoring. Describe them.

53. Find or make up an example of your own where Fibonacci numbers occur. Make sure your example is not related to those that we are studying in the Sections above and below.

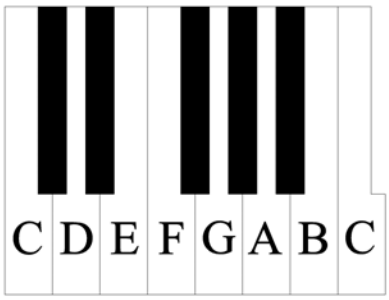


Figure 2.7: An octave on a piano keyboard

The appearance of the Fibonacci numbers in the examples above seem spurious. In some cases they are, but in some they are not. In fact, Fibonacci numbers occur routinely in music. They have played important roles in the music of Mozart, Beethoven, Bartok, and Schillinger. The patterns of music are harmoniously connected to the patterns of mathematics.[8]

> There aren't enough small numbers to meet the many demands made of them.
>
> **Richard Guy** (British mathematician; 1916 -)

54. How does Guy's reminder help us understand the apparently spurious appearance of Fibonacci numbers in our hands, in basketball, and in other surprising situations?

2.11 Phyllotaxis

Phyllotaxis is from the Greek *phyllo*, meaning leaf, and *taxis*, meaning arrangement. It means the study of the arrangement of leaves in relation to a stem or one another. In the Appendix, there is a template for a specific arrangement of leaves on a stem. Either copy or cut out this template.

The numbered rectangular sections serve as the leaves and they are attached to the main stem by a smaller stems represented by large dots at the base of each rectangle. Complete the following tasks to complete your model stem that will help you discover the mathematical aspects of phyllotaxis:

- Copy the template or remove it from you book.
- Draw a series of parallel lines through the stems (dots) at the bases of the leaves (rectangles) which connect: leaf 6 to leaf 5; leaf 4 to leaf 3; and leaf 2 to leaf 1.
- With a different color pen or marker, draw a series of parallel lines through the stems (dots) at the bases of the leaves (rectangles) which connect: leaf 1 to leaf 2 to leaf 3 and leaf 4 to leaf 5 to leaf 6.

[8]See e.g. Tibor Bachmann and Peter J. Bachmann, "An analysis of Bela Bartok's music through Fibonaccian numbers and the golden mean", *The Musical Quarterly*, ??; Jonathan Kramer, "The Fibonacci series in twentieth century music", *Journal of Music Theory*, vol. 17, no. 1, Spring 1973, pp. 110 - 149; Truid Hammel Garland and Charity Vaughan Kahn, Chapter 8: The Curiosities, in Math and Music: Harmonious Connections, Dale Seymour Publications, 1995.

Figure 2.8: Early stages of growth of the Bird of Paradise flower.

- Cut the template along all of the solid lines.
- Roll it lengthwise into a cylinder, joining edge B to edge A, with the excess along edge B rolled inside, and join the edges with tape.
- Bend the leaves (rectangles) down along the dotted lines at their bases.

This resulting model is that of a stem in which there are five leaves per tier. Leaves 1 - 5 make up this first tier and leaf 6 begins the next tier. Position your stem to stand vertically with the smallest leaf, leaf 6, at the top and the largest leaf, leaf 1, at the bottom.

55. Draw a top view of the stem, placing the leaves carefully in their correct position, possibly shrinking the diameter of the stem slightly to give it a more appropriate scale, and numbering the leaves so the order of their appearance can be seen.

56. Determine the angle, measured counterclockwise, between successive leaves (e.g. leaf 1 and leaf 2) in this arrangement.

57. Traverse the leaves in order, from 1 - 5, counterclockwise when viewed from above. Describe the path. For example, how many complete revolutions must you make before you arrive back at your starting place where the sixth leaf will start the next tier of leaves? And how is your path illustrated on your model stem?

58. Use Investigation **57** to determine the fraction of a complete revolution between successive leaves. Compare with Investigation **56**.

59. In what ways might this leaf arrangement be beneficial to this plant?

60. Determine the angle, measured clockwise, between successive leaves.

61. Traverse the leaves in order, from 1 - 5, clockwise when viewed from above. Describe this path as in Investigation **57**.

62. Use Investigation **61** to determine the fraction of a complete revolution between successive leaves. Compare with Investigation **60**.

The leaf arrangement in our model is called a 2/5 **phyllotactic ratio**.

63. You should see the defining relation of Fibonacci numbers at work in our model. Explain.

Suppose we were to arrange leaves so there were eight leaves per tier and there were three complete counterclockwise revolutions, when viewed from above, before arriving back at your starting place where the ninth leaf would start the next tier of leaves. Such an arrangement would be referred to as an arrangement with a 3/8 ***phyllotactic ratio***.

64. Draw a top view of this arrangement, much as you did in Investigation **55**.

65. What would be the angle between successive leaves?

66. If you traverse the leaves in order, from 1 - 8, clockwise when viewed from above, how many complete revolutions must you make before you arrive back at your starting place where the ninth leaf will start the next tier of leaves? What do you notice about this number?

67. Will the 3/8 phyllotactic ratio result in a similar connection to the Fibonacci numbers that you described in Investigation **63**? Explain.

68. Would the arrangement provide the same type of benefits to the plant as the 2/5 ratio? If so, what attributes of the plant might determine whether a 2/5 or 3/8 ratio was more beneficial?

69. Describe an arrangement with a 5/13 phyllotactic ratio in detail. Does it continue the pattern we have observed in Investigation **63** and Investigation **67**?

70. What would the next phyllotactic ratio be? Describe an arrangement with this ratio in detail. Do you think it continues the pattern we have observed in Investigation **63** and Investigation **67**? Explain.

71. For Bird of Paradise flower pictured on the left of Figure 2.9 determine which flowers are directly above others. Is this arrangement a Fibonacci phylotactic arragement? Explain.

72. Repeat Investigation **71** for the flower pictured in the center of Figure 2.9.

73. Repeat Investigation **71** for the flower pictured on the right of Figure 2.9.

For trees that have leaves that are arranged in spirals, this type of Fibonacci phyllotaxis is the rule. Some phyllotactic ratios for common trees are

Figure 2.9: Bird of Paradise flowers in full bloom.

1/2	Elm and Linden
1/3	Beech and Hazel
2/5	Oak, Cherry, and Apple
3/8	Poplar and Rose
5/13	Willow and Almond

We should be cautious however. As the important geometer **H.S.M. Coxeter** (British Mathematician; 1907 - 2003) said:

> It should be frankly admitted that in some plants the numbers do not belong to the sequence of f's [Fibonacci numbers] but to the sequence of g's [Lucas numbers] or even to the still more anomalous sequences $3, 1, 4, 5, 9, \ldots$ or $5, 2, 7, 9, 16, \ldots$ Thus we must face the fact that phyllotaxis is really not a universal law but only a fascinatingly prevalent tendency.

74. Let us break away from the Fibonacci numbers and make an arrangement with a 4/10 phyllotactic ratio. Describe it and explain whether it would be as beneficial as those above.

75. Describe a phyllotactic ratio that does not involve Fibonacci numbers but avoids the difficulty in Investigation **74**. Show that when you include the number of complete revolutions needed to traverse the tier of leaves in the clockwise direction, when viewed from above, this number together with the two numbers in the ratio satisfy the defining relation for Fibonacci numbers.

2.12 Fibonacci Spirals from Optimal Packing

As noted in Section 2.5, objects like pinecones are made up of primordia that originate at a meristem and then move outward from its center as new promordia develop. Mathematicians have long

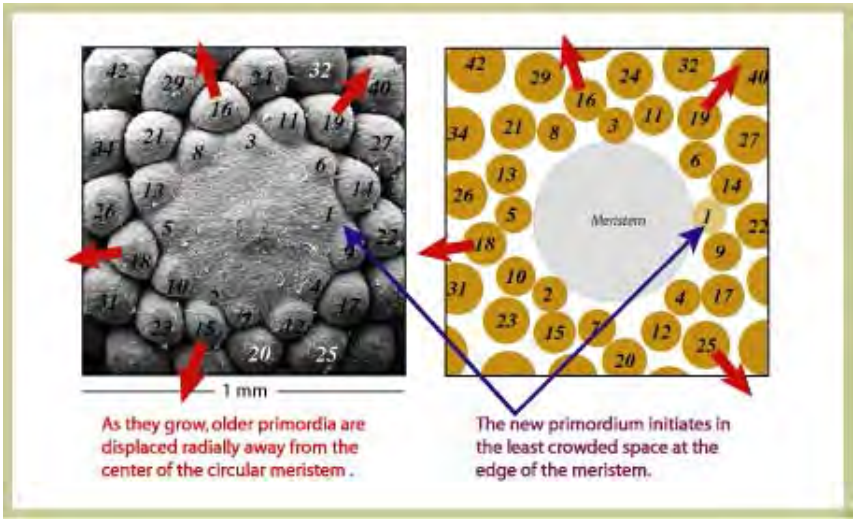


Figure 2.10: Norway Spruce primordia development

sought to understand the mechanics of this process and there has been much recent progress. An excellent description of some of the research, related on-line tutorials, and impressive interactive applets for exploration is available from Phyllotaxis - An Interactive Site for the Mathematical Study of Plant Pattern Forma which was developed at Smith College and is available at `www.math.smith.edu/~phyllo/index.html` .

In this section we briefly investigate one of the mechanisms for the development of spiral patterns. The photograph on the left of Figure 2.10 is scanning electron micrograph of a Norway spruce shoot. On the right is a schematic of the micrograph. The primordia are labeled according to age, those with higher numbers being older. The location of the genesis of each new primordia is, in this model, determined by the least crowded space at the edge of the meristem.

In the appendix there are several copies of the schematic. Use them as needed to complete the investigations below.

76. By finding the least crowded spaces, determine where the next five primordia are likely to appear. Call them $0, -1, -2, -3$, and -4 and draw them in on one of the copies of the schematic.

77. Why would it be beneficial for plants to develop in this way, with the primordia appearing in the least crowded space along the edge of the meristem at each stage in their development?

78. In looking at the schematic, you should see a pattern of counterclockwise spiral arcs . On a copy of the schematic, color their arms just as you did in Section II. How many counterclockwise spiral arcs are there?

79. What do you notice about the identifying numbers of successive primordia along the arms of the spiral arcs?

80. In looking at the schematic, you should also see a pattern of clockwise spiral arcs. On a copy of the schematic, color their arms just as you did in Section II. How many clockwise spirals are there?

81. What do you notice about the identifying numbers of successive primordia along the arms of the spiral arcs?

82. Similarly, you should see an almost radial pattern of arcs forming from the edge of the meristem where successive primordia differ by a constant Fibonacci number. Color in the arcs of this pattern much as you did above. How many radial arcs are there?

Of course, the rate of growth plays an important role in determining which Fibonacci number is evident in a given spiral or configuration of petals. For an interesting illustration of how growth rate changes the number of spirals, see Figs. 4.32 - 4.35 on pp. 119-21 of [CoGu].

83. On a copy of the schematic, put a point in the center of the meristem. Then draw lines from: the center point to the center of primordia 1; the center point to the center of primordia 2; the center point to the center of primordia 3; and the center point to the center of primordia 4. Use them to measure the angle between primordia 1 and primordia 2; primordia 2 and primordia 3; primordia 3 and primordia 4. How are the angles related to others that appear in this chapter?

The angle you found in Investigation **83** is called the **Golden Angle**. It is a sibling of the Golden Ratio - our next topic.

Chapter 3

The Golden Ratio

> Geometry has two great treasures; one is the theorem of Pythagoras; the other, the division of a line into extreme and mean ratio. The first we may compare to a measure of gold; the second we may name a precious jewel.
>
> **Johannes Kepler** (German mathematician; 1571 - 1630)

> Mighty is geometry; joined with art, resistless.
>
> **Euripedes** (Greek dramatist; 480 - 406 BC)

We are all familiar with the **counting numbers** $1, 2, 3, \ldots$ We are also familiar with the **integers** $\ldots, -2, -1, 0, 1, 2, \ldots$ In working with circles and trigonometry we have all used the remarkable number **pi**, denoted by the Greek letter that it is named after: $\pi = 3.14159265\ldots$ Many of us are familiar with the **base of the natural logarithm**[1], the number $e = 2.71828182\ldots$, which is used in the analysis of probabilities, interest rates, population growth and many other important processes. Some of us might even have experience with the number $i = \sqrt{-1}$ that is the base of the *imaginary* or *complex number system*. Much less well-known is the **Golden Ratio** which is the number denoted by the Greek letter *phi*:

$$\phi = \frac{1 + \sqrt{5}}{2} = 1.61803398\ldots$$

Yet the Golden Ratio was widely used before the discovery of both e and i. Moreover, it was widely used before there was *any notion* of zero or negative numbers!

3.1 The Golden Ratio

It is claimed by many that the Golden Ratio played a prominent role in the construction of the great pyramids and the Greek Parthenon, the design of the United Nations buildings, in the paintings of **Leonardo da Vinci** (sculptor, painter, inventor, scientist, engineer; 1452 - 1519) and **Albrecht Dürer** (German artist; 1471 - 1528), in the music of **Béla Viktor János Bartok**

[1] We denote this constant by the letter e in honor of **Leonhard Euler** (Swiss mathematician; 1707 - 1783) who was the first to investigate its remarkable properties. He also discovered the remarkable formula uniting many of these key constants: $e^{i\pi} + 1 = 0$. For more on this formula, see the chapter on $\sqrt{-1}$ in Discovering the Art of Mathematics - Truth, Reasoning, Certainty and Proof.

Figure 3.1: The Great Pyramid of Khufu (Cheops). Notice the size of the visitors.

(Hungarian composer and pianist; 1881 - 1945) and **Johann Sebastian Bach** (German musician and composer; 1685 - 1750), and psychological studies have even suggested that it is the most pleasing ratio there is – perhaps explaining its use in architecture, art and music[2]. In fact, the Greek letter ϕ is used to denote this constant in honor of the Greek artist **Phidias** (Greek sculptor, painter and architect; 480 - 430 BCE) who used the Golden Ratio in his famous sculptures[3].

It is strange that a number that is widely known by artists, architects, biologists, and musicians is rarely considered in mathematics courses. As this is a mathematics for liberal arts course, this seems like a perfect opportunity.

3.2 Division into Extreme and Mean Ratio

The Golden Ratio is the number $\phi = \frac{1+\sqrt{5}}{2}$. The notion of the Golden Ratio, although not so-called at that time, was first introduced by the ancient Greeks. As Greek mathematics was based solely on geometric methods, the Golden Ratio was introduced geometrically. It arose from the division of a line segment into two special segments. This process is called the division of a line into *extreme and mean ratio*; it appeared as Definition 3 in Book VI of Euclid's Elements[4] :

> A straight line is said to have been **cut in extreme and mean ratio** when, as the whole line is to the greater segment, so is the greater to the less.

[2]See, for example, the section "Experimental Aesthetics" in Chapter V of The Divine Proportion by H.E. Huntley. There is considerable debate over the validity of these claims. See the Perspectives section of this topic for more details.

[3]Ibid, p. 25.

[4]One of the most famous and widely read books of all time.

Figure 3.2: The Greek Parthenon

Thus the Golden Ratio is the precious jewel of geometry that Kepler spoke of at the outset of this lesson.

How can we understand this definition? For a line to be cut in extreme and mean ratio we must check that two ratios are equal. In his Elements (Book VI, Proposition 30), Euclid showed that any line segment can be so divided using straightedge and compass - the allowable tools of Greek geometry. In a slightly different spirit, although still geometric in nature, we can perform the division using straightedge and compass resulting in the construction[5] in Figure 3.3.

To see that we have succeeded, we check the equality of the specified ratios. If we apply the Pythagorean theorem to the right triangle we see that

$$\left(\overline{AB}\right)^2 + \left(\frac{\overline{AB}}{2}\right)^2 = \left(\overline{AG} + \frac{\overline{AB}}{2}\right)^2 \rightarrow \frac{5\left(\overline{AB}\right)^2}{4} = \left(\overline{AG} + \frac{\overline{AB}}{2}\right)^2.$$

Taking square roots and solving, we see that $\overline{AG} = \left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}$. It follws that[6]:

$$\frac{\overline{AB}}{\overline{AG}} = \frac{\overline{AB}}{\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}} = \frac{2}{\sqrt{5}-1} \cdot \frac{\overline{AB}}{\overline{AB}} = \frac{2}{\sqrt{5}-1} \cdot \frac{1+\sqrt{5}}{1+\sqrt{5}} = \frac{2\left(1+\sqrt{5}\right)}{4} = \frac{1+\sqrt{5}}{2}$$

and

[5]The perpendicular of length $\frac{1}{2}\overline{AB}$ is created first. Then the semicircle through B constructs point C. The semicircle centered at A and through C constructs point G.

[6]This is one of the few places that your skills in *rationalizing the denominator* might serve you well.

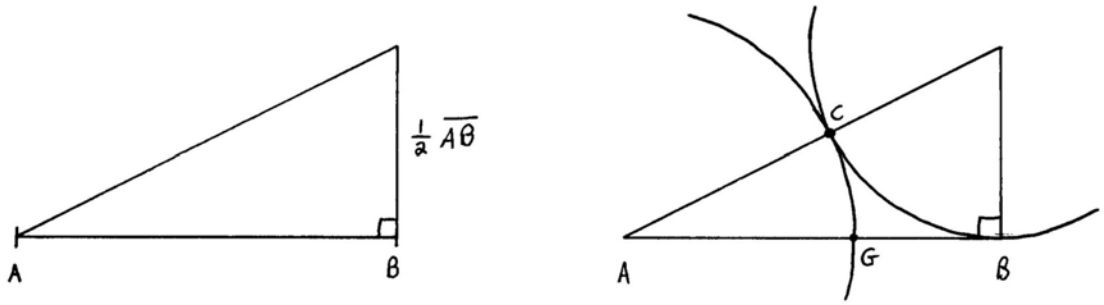


Figure 3.3: Geometric derivation of the Golden Ratio.

$$\begin{aligned}\frac{\overline{AG}}{\overline{GB}} = \frac{\overline{AG}}{\overline{AB}-\overline{AG}} &= \frac{\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}}{\overline{Ab}-\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}} = \frac{\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}}{\left(\frac{3-\sqrt{5}}{2}\right)\overline{AB}} \\ &= \left(\frac{\sqrt{5}-1}{2}\right)\cdot\left(\frac{2}{3-\sqrt{5}}\right)\cdot\frac{\overline{AB}}{\overline{AB}} \\ &= \frac{\sqrt{5}-1}{3-\sqrt{5}} = \frac{\sqrt{5}-1}{3-\sqrt{5}}\cdot\frac{3+\sqrt{5}}{3+\sqrt{5}} \\ &= \frac{2+2\sqrt{5}}{4} = \frac{1+\sqrt{5}}{2}\end{aligned}$$

as well.

Hence the ratios are equal, i.e. the line has been divided into mean and extreme ratio, *and* both ratios are equal to the Golden Ratio!

This may seem like an obtuse definition. But remember, π is defined as a ratio as well - the ratio of a circle's circumference to its diameter. So just give ϕ a little bit of time.

3.3 The Golden Ratio Algebraically

Algebra as we know it is a fairly recent mathematical invention, beginning its modern development in the latter part of the sixteenth century, and it was not available to the ancient Greeks who used geometry as their language for mathematical analysis. However, we can find the Golden Ratio easily using high school algebra.

Consider the line segment in Figure 3.4. We would like to find a value of $x > 1$ so that it is divided into extreme and mean ratio.

1. In terms of 1 and x, find expressions for the two ratios that we need to compare to see if the line is divided into extreme and mean ratio. Equate these ratios.

Figure 3.4: Algebraic derivation of the Golden Ratio.

2. Use algebra to simplify the equation in Investigation **1** into an equation that does not involve ratios. Then collect all nonzero terms to the left-hand side of the equation.

The function on the left-hand side of the equation in 2 is called a *defining function*, and you can probably guess that it will define the Golden Ratio.

3. Carefully graph the defining function from Investigation **2** by hand, using a graphing calculator, spreadsheet, or computer algebra system.

4. Use your graph in Investigation **3** to determine how many solutions the equation in Investigation **2** has.

5. Using repeated estimation, the *ZOOM IN* feature on your graphing calculator, numerical estimation on a spreadsheet, or numerical solution via a computer algebra system, find the solution x with $x > 1$ to the equation in Investigation **2**. Surprised?

6. Using algebraic techniques from high school algebra, solve the equation in Investigation **2** exactly. Surprised?

3.4 Nested Radicals

7. Use your calculator or a spreasheet to determine the values of $\sqrt{1}$, $\sqrt{1+\sqrt{1}}$, and $\sqrt{1+\sqrt{1+\sqrt{1}}}$ correct to several decimal places.

8. Could you continue taking repeated radicals as you did in Investigation **7**? If not, explain what the limitation is. If so, make a table of the values of the first ten repeated radicals correct to several decimal places.

At first glance it might seem that the infinitely repeated radical

$$\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}}}$$

is too bizarre to be evaluated or even to make sense. However, people are quick to accept the infinitely-repeated decimal $0.333\ldots$ as an exact value for the fraction $\frac{1}{3}$. So suspend judgment on whether an infinitely-repeated radical, like the one above, makes any sense just long enough to...

Figure 3.5: The United Nations Secretariat Building.

9. . . . hazard a guess of its numerical identity.

Let's see if we can determine its numerical identity precisely.

10. Denote the unknown, infinitely-repeated radical by $x = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}}}$. In simplified form, what is x^2?

11. Using 1 and x, express x^2 as an algebraic expression without using any radicals.

12. Use your answer to Investigation **11** and earlier investigations to determine the value of x exactly. Does your answer agree with your guess in Investigation **9**? Explain.

3.5 Continued Fractions

The ancient Greeks thought that all numbers could be expressed as fractions. In fact, their mathematical system was founded on this belief. When it was discovered that $\sqrt{2}$, the length of the diagonal of a 1 by 1 square, could not be written as a fraction it was a tremendous setback

to their sophisticated mathematical program. So great was the impact that the discoverer was, according to legend, drowned.

Many attempts were made to repair this difficulty. One was to allow a more general form of fractions called *continued fractions*. Some examples of continued fractions are

$$\frac{1}{1+\frac{1}{3}} = \frac{1}{\frac{4}{3}} = \frac{3}{4}, \frac{3}{2-\frac{1}{2}} = \frac{3}{\frac{3}{2}} = 2$$

and even Bombelli's [7] remarkable

$$\sqrt{13} = 3 + \frac{4}{6 + \frac{4}{6+\frac{4}{6+\ldots}}}$$

Those of you who find arithmetic with fractions frustrating can certainly be grateful to the Babylonians for the decimal numbers that saved you from arithmetic with continued fractions.

13. Convert the fraction $1+\frac{1}{1}$ into **simple fraction**, that is, a fraction of the form $\frac{a}{b}$ where a, b are integers.

14. Convert the continued fraction $1+\frac{1}{1+\frac{1}{1}}$ into a simple fraction.

15. Convert the continued fraction $1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}$ into a simple fraction.

16. Convert the continued fraction $1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}$ into a simple fraction.

17. Write the continued fraction that would come next in the pattern illustrated by Investigation **13** - Investigation **16**. Then convert it into a simple fraction.

18. Write the continued fraction that would come next in the pattern illustrated by Investigation **13** - Investigation **16**. Then convert it into a simple fraction.

19. Write the continued fraction that would come next in the pattern illustrated by Investigation **13** - Investigation **16**. Then convert it into a simple fraction.

20. The numerators and denominators in the simple fractions that answer Investigation **13** - Investigation **19** form an important pattern. What pattern is this and how is it related to other material we have considered?

21. Extend the pattern in Investigation **20** several more stages. Then make a table that gives the decimal values of each of the fractions in Investigation **13** - Investigation **19** and your extended data correct to several decimal places.

Of all infinite continued fractions, $1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\ldots}}}}$ seems the simplest.

22. Does the data in Investigation **21** suggest a value for $1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\ldots}}}}$? Explain.

[7] Discovered in 1572. See e.g. [Bur, p. 279].

Let's see if we can determine the value of this infinite object precisely, as we did with the infinite radical.

23. Denote the unknown continued fraction by $x = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}}$. Using only 1 and x, express x as an algebraic expression containing only standard fractions.

24. Simplify your equation in Investigation **23** to find an equation involving x that is fraction-free.

25. Use your answer in Investigation **24** and earlier problems to determine the value of x exactly. Does your answer agree with Investigation **22**? Explain.

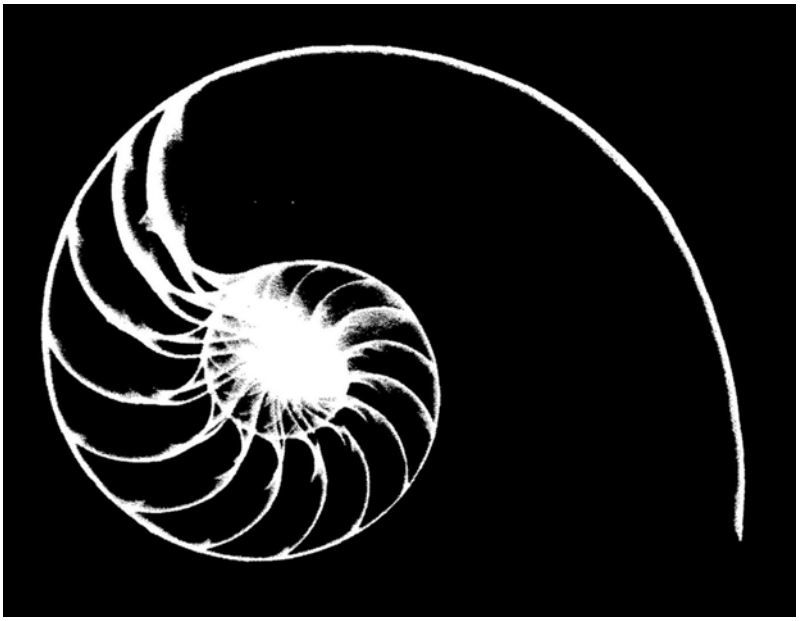


Figure 3.6: Nautilus shell cross section.

3.6 Powers of ϕ.

26. Your investigations here have an added benefit. Namely, they show that the ratio of successive Fibonacci numbers, $\frac{F_{n+1}}{F_n}$ approaches an important *limit* as $n \to \infty$. What is this limit?

27. What does this limit tell you about the *rate of growth* of the Fibonacci numbers? Explain.

28. Make a table of values of the function $b_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$ for $n = 1, 2, 3, 4, \ldots, 8$.

29. How close are these values to whole numbers? Is this surprising? Explain.

30. What is even more surprising about these numbers?

The function $B_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$ is called **Binet's formula**. Its values are always whole numbers – in fact, exactly those special whole numbers that you should have noticed in Investigation **30**.[8]

31. In the previous chapter you were asked how hard it would be to determine the fiftieth Fibonacci number. Can you determine it now?

3.7 Golden Rectangles

A rectangle is called a **Golden Rectangle** if the ratio of longer side to the shorter side is the Golden Ratio. The studies noted above suggest that it is the most pleasing of all possible rectangular shapes, that the superstructure of the Parthenon forms a Golden Rectangle, and that the face of Mona Lisa in the famous painting by Leonardo da Vinci is also in the ratio that forms a Golden Rectangle.

In Figure 3.7 is a rectangle whose width is ϕ and whose height is 1. Two circular arcs, AF and FG, and two perpendiculars, EF and GH, have been drawn.

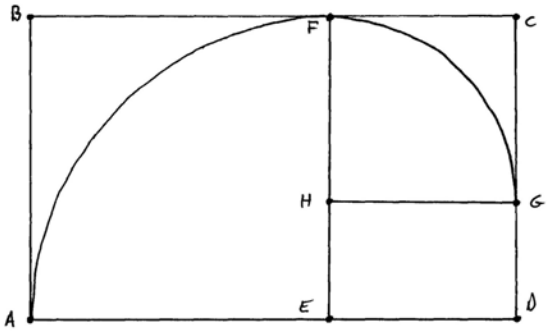


Figure 3.7: First Stages of the Golden Spiral.

32. Is the rectangle $ABCD$ a Golden Rectangle? Explain.

33. Is the smaller rectangle $CDEF$ a Golden Rectangle? Prove your result.

34. Is the even smaller rectangle $DEHG$ a Golden Rectangle? Prove your result.

35. Following the evident pattern, draw in another circular arc and another perpendicular. Is the even smaller rectangle that results a Golden Rectangle as well? Prove your result.

[8]This seems like a miraculous formula and one might be tempted to think that it may be remarkably hard to prove. Actually, it is straightforward to define the Fibonacci sequence using 2×2 matrix algebra. In this setting, the *eigenvalues* of the *transition matrix* are $\frac{1}{\sqrt{5}}\left(\frac{1\pm\sqrt{5}}{2}\right)$ and the formula is an immediate result.

36. Do you think you could repeat the process in Investigation **35** again and again? Is there any limit? Explain.

37. Draw the sequence of circular arcs that would be created when one continues this process. Is the resulting figure aesthetically pleasing?

The shape that you drew in Investigation **37** is the shape of nautilus shells (see figure Figure **??**), one of many natural organisms whose growth is controlled by the Golden Ratio[9]. The process that you carried out in Investigation **36** shows that, in some sense, Golden Rectangles are *fractals*.[10].

Figure 3.8: "Spirale" by Lino Tagliapietra, from the Corning Musuem of Glass. The artist says he was "inspired by a nautilus shell". Notice how reminiscent the opposing spirals are to the Fibonacci spirals found in the previous chapter.

3.8 Star Pentagrams

The object in Figure 3.9 is called a **star pentagram.** It was the sacred symbol of the *Pythagoreans*, a cult-like group of important historical import in mathematics.

38. Measure each of the line segments of different length in the star pentagram and make a chart giving their lengths.

[9]See the Perspectives section at the end of this chapter for details and references. Also, compare with Investigation **27**.

[10]Loosely speaking, a fractal is a geometric shape that reveals interesting fine structure, often self-similar in nature, that recurs indefinitely as it is magnified. Fractals have become quite popular and both non-technical print introductions and beautiful, dynamic Internet Java-scripts are widely available. (E.g. [Ste, Ch. 13], [FrPe], [Con], [Cool].)

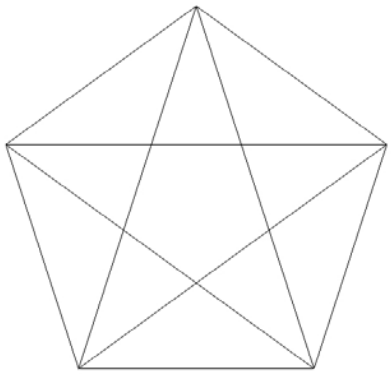


Figure 3.9: Star Pentagram.

39. Are there any pairs of line segments in the star pentagram that form a golden ratio? If so, list them.

40. Could you draw another star pentagram somewhere within the given star pentagram? If so, provide an illustration. If not, explain why not.

41. Are there any limits to the number of star pentagrams that can be drawn within the original? Explain.

3.9 Magical Rectangles

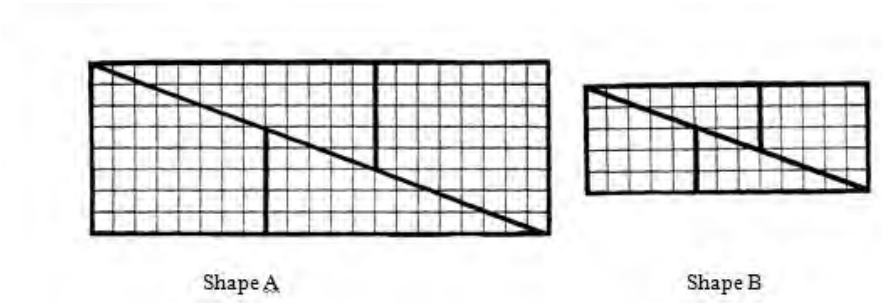


Figure 3.10: Magical rectangles.

The puzzle in this section is attributed to **William Hooper** (; -) in 1794[11] by perhaps the greatest mathematical puzzler of all time, **Martin Gardner** (Mathematics and science writer; 1914 - 2010). The puzzle is based on the related figures in Figure 3.10.

[11] See Mathematics, Magic and Mystery, Dover, 1956, p. 131.

42. How are the dimensions of the pieces that comprise Shape A in Figure 3.10 related to material we have recently been studying?

43. What do you notice about the dimensions of the pieces that comprise Shape B?

44. What are the areas of Shapes A and B?

45. Make a copy of Shapes A and B and cut out the pieces along the darkened lines. Show how you can rearrange the pieces to form squares.

46. What are the areas of the squares?

47. Are your answers to problems Investigation **44** and Investigation **46** compatible? Is this situation reasonable or even acceptable? Explain.

48. Can you construct other rectangles where the same behavior might take place? Explain.

Shape C in Figure 3.11 is related to Shapes A and B above.

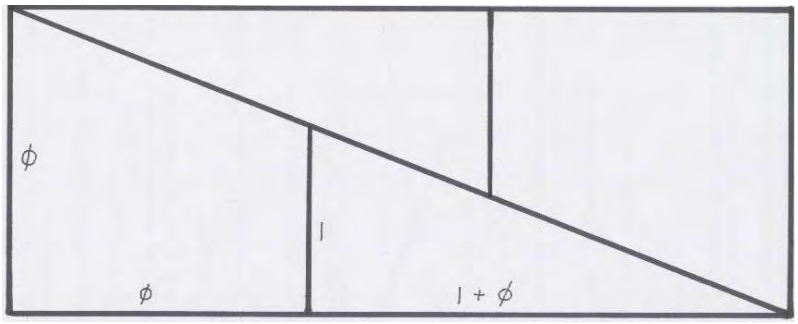


Figure 3.11: Shape C: A golden, magical rectangle.

49. What is the area of Shape C (in terms of ϕ)?

50. Make a copy of Shape C and cut out the pieces. Show how you can rearrange them to form a square.

51. What is the area of this square?

52. Are your answers to Investigation **49** and Investigation **51** compatible? Explain. (Hint: Use your result from question Investigation **2** above to help you simplify if necessary.)

53. Is the behavior of the shapes constructed from the pieces from Shape C analogous to the behavior of the corresponding shapes constructed from the pieces from Shapes A and B? Explain whether this is surprising or not.

Magical rectangles such as these have long been used as amusements. They are effective because they strike a powerful blow at our basic trust of strong conservation laws - conservation of area in this case. While this is an important and generally valid law - it comes with exceptions. In 1924 **Stefan Banach** (Polish mathematician; 1892 - 1945) and **Alfred Tarski** (Polish mathematician; 1902 - 1983) showed that it is theoretically possible to cut an orange into five pieces that can be reassembled, with no stretching or distorting, into two oranges of the same size and same volume as the original! This result strikingly demonstrates that area as we know it does not, theoretically, satisfy a strict conservation law. The apparent paradox, known as the **Banach-Tarski Theorem** as it is a deductively established result, is one of many unbelievable realities we must face when dealing with the infinite. Several of these are explored in the Additional Investigations section.

3.10 Perspectives on the Golden Ratio

54. Claims of the ubiquity of the Golden Ratio in art, architecture, and music abound in print sources as well as on the Internet. The validity of some of these instances of mathematical folklore is established in documented sources. For example, Le Corbousier's use of the Golden Ratio in the design of the United Nations Secretariat Building (pictured in Figure 3.5) is described in Connections: The Geometric Bridge Between Art and Science by Jay Kappraff, World Scientific Publ. Co., 2001. However, the majority of these claims falter under detailed analysis. George Markowsky challenges several of the better known claims in "Misconceptions about the Golden Ratio", *The College Mathematics Journal*, vol. 23, no. 1, January, 1992, pp. 2 - 19. Find one specific example of a claim that the Golden Ratio occurs in a well-known work of art, architecture, music, or other human creation. In a brief essay, describe this occurrence and then turn a more skeptical eye to the issue in an effort to determine whether there is real legitimacy to the claim that the Golden Ratio plays a real role in the object under study.

55. In contrast to the debate about the occurrence of the Golden Ratio in the human world, the Golden Ratio occurs with surprising frequency in the natural world. For example, the Golden Ratio plays a critical role in the arrangement of leaves on the stems of many plants. (See e.g. the section "Phyllotaxis" in Ch. XII of The Divine Proportion by H.E. Huntley, Dover, 1970 or The Power of Limits: Proportional Harmonies in Nature, Art and Architecture by Gyorgi Doczi, Shambhala Publ., 1994.) The Internet abounds with claims of the occurrence of the Golden Ratio in nature; there is even a Golden Mean Gauge! (`www.goldenmeangauge.co.uk/nature.html`.) Find an instance where the Golden Ratio occurs in nature. Write a brief essay (appropriate to share with fellow students) that illustrates the occurrence. You should include appropriate diagrams, some explanation of what natural function gives rise to the Golden Ratio, and reliable references.

Chapter 4

Primes and Congruences

> The positive integers stand there, a continual and inevitable challenge to the curiosity of every healthy mind.
>
> **G.H. Hardy** (English mathematician; 1877 - 1947)

> It will be another million years, at least, before we understand the primes.
>
> **Paul Erdös** (Hungarian mathematician; 1913 - 1996)

> Were it not for your [Duke of Brunswick] unceasing benefits in support of my studies, I would not have been able to devote myself totally to my passionate love, the study of mathematics.
>
> **C.F. Gauss** (German mathematician; 1777 - 1855)

4.1 Primes

In this book's Introduction we were reminded of the prime numbers, those positive integers whose only divisors are 1 and the number itself. Any positive integer that is not prime is called **composite**. Any number that evenly divides another positive integer is called a **factor** of the latter.

For example, the number 462 is composite since it is even. We can *completely factor* 462 into its prime factorization $462 = 2 \times 3 \times 7 \times 11$. $2, 3, 7$, and 11 are all factors of 462, as are combinations of them like $6, 14$, and 77. The ***prime factorization*** of 462 is called complete because none of the factors can be broken down any further - all factors are prime. If we start with a composite number, we are able to factor it, then factor the factors, and then factor these smaller factors, and continue until all of the factors are primes.

Not only can every positive integer be completely factored into primes, but the representation is unique up to the order in which the factors appear. This result is called the **fundamental theorem of arithmetic**. It is truly of fundamental importance for it says is that the prime numbers are, via multiplication, the building blocks of the positive integers. As elements serve as the building blocks for all chemical compounds, the primes serve as the building blocks for the positive integers. We should study the behavior of these building blocks, just as we study the periodic table and how the elements behave in combination.

In discussing Goldbach's conjecture it was noted that contemporary mathematicians do not consider the number 1 to be prime. It is precisely here this matter can be given appropriate context. An essential component of the fundamental theorem of arithmetic is the uniqueness of the factors.

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397		

Table 4.1: The primes under 400.

462 has precisely four prime factors - $2, 3, 7, 11$. If 1 were considered a prime number then it would be a factor as well. And in fact, it could be a repeated factor: $462 = 1 \times 1 \times 1 \times 2 \times 3 \times 7 \times 11$. This opens a flood-gate of complications. It is this then that lead to the decision that we should not consider 1 to be a prime number.

Mathematicians have long tried to find patterns among the primes, and despite some success and fascinating stories like that of "The Twins" (see Section 4.5 below), they have had little success. Because large primes are the combinations that unlock encryption schemes, they are an invaluable commodity. Thus, the search for patterns among the primes occupies a great deal of mathematics' contemporary work - as we shall see in the Chapter 5.

4.2 Twin Primes and Other Arithmetic Progressions of Primes

The numbers 5 and 7 are called **twin primes** because they come in pairs, as close as two odd primes can be. 11 and 13, 17 and 19, and 29 and 31 are other twin prime pairs. As we shall see in Chapter 5, mathematicians have long known there are infinitely many primes, they have been unable to determine whether there are infinitely many twin prime pairs or not. Most believe there infinitely many - this belief is called the **twin prime conjecture** - but this remains a major open question in number theory. Solve this mystery and you will be a mathematical celebrity.

1. Find all of the twin primes under 100.

2. Find all of the twin primes between 100 and 200.

3. Find all of the twin primes between 200 and 300.

4. Find all of the twin primes between 300 and 400.

5. What do you notice about the number of twin primes in each of these ranges?

6. Why do you think this might be happening?

7. Find a ***progression*** of three twin primes; that is, a sequence of three primes each that is a twin prime to the one that follows it.

8. Prove that no other progression of three twin primes can exist.

9. Can you find a progression of twin primes longer than three terms? If not, why? If so, how large of a progression can you find?

Cousin primes are a pair of prime numbers that are four away from each other. **Sexy primes** are a pair of primes that are six away from each other.

10. Find several pairs of cousin primes.

11. Can you find a progression of three cousin primes? If one progression exists, are there others? (Prove your answer.)

12. Can you find a progression of cousin primes that is longer than three terms? If not, why? If so, how long of a progression can you find?

13. Find several pairs of sexy primes.

14. Can you find a progression of three sexy primes? If one progression exists, are there others? (Prove your answer.)

15. Can you find a progression of sexy primes that is longer than three terms? If not, why? If so, how long of a progression can you find?

16. Make up your own name for a pair primes that are eight apart. Explain your name.

17. Find several pairs of eight-apart primes.

18. Can you find a progression of three eight-apart primes? If one progression exists, are their others? (Prove your result.)

19. Can you find a progression of eight-apart primes that is longer than three terms? If not, why? If so, how long of a progression can you find?

20. How long of a progression of 30-apart primes can you find?

In 1910, **Edward B. Escott** (; -) discovered that all of the terms in the progression

$$199, 409, 619, \ldots, 1669$$

were prime.

21. How far apart are the numbers on Escott's list?

22. How many numbers are on Escott's list?

23. Looking back at your examples, which "apart numbers" generate fairly long progressions of primes?

24. What properties do these useful "apart numbers" share? How are these useful "apart numbers" related to each other?

From 1910 - 1963, mathematicians were not able to find a longer run of consecutive ***primes in arithmetic progression*** than Escott. At the time of this writing (2014) the longest run of consecutive primes in arithmetic progression that is known is 26.[1] On the basis of this evidence, it is stunning that one can *prove* that for *any* finite length there *must* exist a run of consecutive primes in arithmetic progression of at least this length. In other words, despite being stuck at 26, we know that there is an arithmetic progression of one billion primes in a row! This startling result was proven in 2004 by **Ben Green** (British mathematician; 1977 -) and **Terence Tao** (Australian mathematician; 1975 -).[2] At age 31, Tao won mathematics' highest honor - the Fields medal - in part for his work on this problem.

The Green/Tao theorem, as it is called, is an ***existence theorem*** which proves existence but does not tell you how to actually construct the desired objects. It gives us no clue how to find these elusive arithmetic progressions of primes that can exceed any finite length. The Green/Tao theorem had many additional consequences, many outlined in a paper by a premier number theorist named **Andrew Granville** (British mathematician; 1962 -).[3] Here you will investigate one such prime pattern.

The array of numbers

$$\begin{array}{cc} 3 & 7 \\ 19 & 23 \end{array}$$

is called a 2×2 ***generalized arithmetic progression of primes*** (GAP) because all of the numbers are prime and along each row the numbers are 4 apart and along each column the numbers are 16 apart.

25. Find another 2×2 generalized arithmetic progression of primes.

26. There is 3×3 generalized arithmetic progression of primes whose smallest member is 29 and whose largest member is 113. Find the other members of this GAP.

The Green/Tao theorem insures that larger and larger such GAPs exist, including a Rubik's cube like $3 \times 3 \times 3$ GAP. When Westfield State College undergraduate students **Michael Guenette** (American student; -) and **Jeffrey P. Vanasse** (American student; -) began reading Granville's paper in 2008 with the author of this book they were stunned to learn that nobody alive had ever found an example of the lowly $3 \times 3 \times 3$ GAP despite the fact that we knew that GAPs of any finite size must exist. They repeatedly collected ideas to search for it. Each time they described their ideas to me I dissuaded them, explaining how the number of cases to check by searching exhaustively would overwhelm the potential of the computer. Each week they came in with improved ideas. Eventually I acquiesced. With the coding help of another of their teachers, **Marcus Jaiclin** (American mathematician; -), in two weeks the students had found it, the first known example of the $3 \times 3 \times 3$ GAP! The minimal example is shown in Figure 4.1. Their discovery was widely reported.[4]

So there is great progress in finding long runs of arithmetic progressions of primes. But what about the more "basic" question of the total number of twin primes or cousin primes or sexy

[1] Search "Primes in arithmetic progression records" to learn if this record has been extended since this writing.

[2] Green, Ben and Tao, Terence (2008), "The primes contain arbitrarily long arithmetic progressions", *Annals of Mathematics* 167 (2): 481?547.

[3] "Prime Number Patterns", *The American Mathematical Monthly*, vol. 115, No. 4, April 2008, pgs. 279-296.

[4] See e.g. `http://www.sciencedaily.com/releases/2008/11/081117220257.htm` and see `http://www.westfield.ma.edu/math/GAP.page.html` for more information.

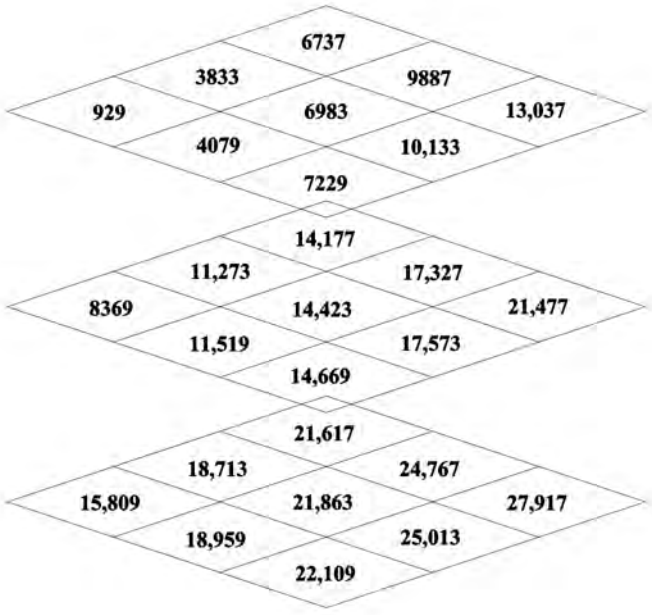


Figure 4.1: $3 \times 3 \times 3$ GAP by Guenette, Vanasse, Fleron and Jaiclin.

primes? We just have no idea how many of any of these primes there are. And, until recently, most would admit that there was little hope for imminent progress.

So it was with great excitement when **Yitang Zhang** (Chinese mathematician; 1955 -) announced that he had proven a ***bounded gaps theorem*** for primes. His result is that if you put all of the twin primes together with all of the cousin primes together with all of the sexy primes together with all of the eight apart primes you just named and keep collecting all of the prime pairs that are separated by larger and larger gaps, when you reach gaps of size 7,000,000 the resulting collection of primes will be infinite. What this means is that *at least* one of the families of primes (i.e. twins, cousins, sexies,...) *must* be infinite.

A group of mathematicians, lead by Tao, are hard at work to lower Zhang's bound of $7,000,000$. At the time of this writing (2014) the *Polymath8 project* had reduced the bounded gaps' size needed to insure infinitude from $7,000,000$ to 246.

After many decades with little progress to speak of, the twin prime conjecture may be teetering.

Zhang's result is a powerful, surprising result. Zhang was not widely known before his work was announced. As a teen he was exiled and performed hard labor instead of the mathematics he wished to study. He eventually completed degrees in mathematics and immigrated to the United States. Struggling to find an academic position, the Ph.D. mathematician worked for a time at

a Subway restaurant.[5] At the time of his discovery his official position was as a Lecturer at the University of New Hampshire - a low rank position at the institution not known for high-profile research breakthroughs. He was subsequently promoted to Full Professor and won many awards, including a MacArthur Genius Award with a prize of $625,000.

Earlier we promised that number theory was accessible, here you see another example of the breadth of the people who have contributed to number theory's wonderful contemporary growth.

4.3 Fermat Primes

The French monk Father **Marin Mersenne** (French theologian, philosopher and mathematician; 1588 - 1648) was an important facilitator of mathematical communication. He helped mathematics successfully escape from the Dark Ages that had stagnated intellectual life. **Pierre de Fermat** (French lawyer and mathematician ; 1601 - 1665), whose monumental contributions to number theory are explored throughout most of the forthcoming chapters, frequently communicated with Mersenne. In one letter to Mersenne Fermat announced he had "found that numbers of the form $2^{2^n}+1$ are always prime numbers and have long since signified to the analysts the truth of this theorem."

In honor of Fermat, we call these numbers **Fermat numbers** and denote the general Fermat number by $F_n = 2^{2^n}+1$.

As Fermat observed,

$$F_0 = 2^{2^0}+1 = 3,$$

$$F_1 = 2^{2^1}+1 = 5, \text{ and,}$$

$$F_2 = 2^{2^2}+1 = 17$$

are all prime.

27. Determine F_3 by hand.

28. From Table 4.1 we can ascertain that F_3 is prime. Check this using only a basic calculator. Explain precisely how you have proven that this number is prime.

29. Using only a basic calculator, determine F_4.

30. Using a basic calculator, how long do you think it would take you to determine whether F_4 was prime? Explain.

31. To determine whether the fifth Fermat number, $F_5 = 2^{2^5}+1 = 4,294,967,297$, is prime, theoretically what must one do?

32. In light of Fermat's virtually unblemished record, would it seem wise to challenge the primality of the fifth Fermat number in an era when computers and electronic calculators were not available?

[5] See `http://news.cnet.com/8301-17938_105-57618696-1/yitang-zhang-a-prime-number-proof-and-a-world-of-persistence/`.

As discussed in Chapter 6, Euler was the first to fruitfully extend any of Fermat's significant work in number theory. That is the case here as well.

Instead of using brute force to try to find factors of F_5, Euler ingeniously eliminated the majority of potential factors by analyzing properties potentially successful divisors would be required to have. In particular, he showed that if F_5 was not prime it must have a prime factor of the form $64k + 1$ where k is a positive integer.

33. Compute the numbers $64k + 1$ for $k = 1, 2, \ldots, 10$.

34. Which of the ten numbers in your answer to Investigation **33** are prime?

35. Check to see if any of the primes from your answer to Investigation **34** divide F_5. What does this tell you about F_5?

When a Fermat number is prime we refer to it as a **Fermat prime**.

36. Would you be surprised to learn that mathematicians have shown that the next twenty six Fermat numbers, $F_6 = 2^{2^6} + 1, \ldots, F_{32} = 2^{2^{32}} + 1$, are all composite? They are. How badly mistaken was Fermat in his conjecture about Fermat primes?

4.4 Mersenne Primes

In addition to his correspondence with Fermat, Mersenne made his own important contributions in the search for primes. He suggested that we consider numbers of the form

$$M_n = 2^n - 1,$$

numbers which have since been called **Mersenne numbers** in his honor. The first four Mersenne numbers are

$$M_1 = 2^1 - 1 = 1,$$

$$M_2 = 2^2 - 1 = 3,$$

$$M_3 = 2^3 - 1 = 7, \text{and},$$

$$M_4 = 2^4 - 1 = 15.$$

When Mersenne numbers are prime, like $M_2 = 3$ and $M_3 = 7$, they are called **Mersenne primes**.

37. Find the next six Mersenne numbers, $M_5 - M_{10}$.

38. Which of these Mersenne numbers are prime?

39. Based on the evidence you have thus far, can you make a conjecture - based on specific conditions on n - about when a Mersenne number M_n i) is a prime, and, ii) is not a prime? Explain.

40. What does your conjecture in Investigation **39** tell you about Mersenne numbers M_n when n is even and greater than 2? Explain.

41. Compute each of the products $(2^2+1)\cdot(2^2-1)$, $(2^3+1)\cdot(2^3-1)$, and $(2^4+1)\cdot(2^4-1)$. How do these products relate to Mersenne numbers?

42. Extend your observations in Investigation **41** to prove your conjecture in Investigation **40**.

43. The thirteenth, seventeenth, and nineteenth Mersenne numbers ($M_{13} = 2^{13}-1 = 8191$, $M_{17} = 2^{17}-1 = 131,071$, and $M_{19} = 2^{19}-1 = 524,287$, respectively) are all prime numbers. Do these facts and your proof in Investigation **42** bolster your faith in the validity of your conjecture in Investigation **39** about the Mersenne numbers that are prime?

44. Is the eleventh Mersenne number, $M_{11} = 2^{11}-1 = 2047$ prime? What does this tell you about your conjecture in Investigation **39**?

4.4.1 Modern Analysis of Mersenne Primes before Computers

Mersenne made a detailed study of Mersenne numbers. He claimed to know exactly which of the first 257 Mersenne numbers were prime and which were not. His work did not include proofs of these results. So mathematicians continued to investigate Mersenne's claims. In 1876 **Édourd Lucas** (French mathematician; 1842 - 1891) proved that

$$M_{127} = 170,141,183,460,469,231,731,687,303,715,884,105,727$$

was prime, as Mersenne claimed. This was the largest prime known to humankind for over 75 years!

But Mersenne made a few mistakes. One of these was with M_{67} which Mersenne claimed was prime. The story surrounding this number is rich:

> Édouard Lucas worked a test whereby he was able to prove that the Mersenne number M_{67} was composite; but he could not produce the actual factors. At the October 1903 meeting of the American Mathematical Society, the American mathematician Frank Nelson Cole had a paper on the program with the somewhat unassuming title "On the Factorization of Large Numbers." When called upon to speak, Cole walked to a [chalk] board and, saying nothing, proceeded to raise the integer 2 to the 67th power; then he carefully subtracted 1 from the resulting number and let the figure stand. Without a word he moved to a clean part of the board and multiplied, longhand, the product
>
> $$193,707,721 \times 761,838,257,287.$$
>
> The two calculations agreed. The story goes that, for the first and only time on record, this venerable body rose to give the presenter of a paper a standing ovation. Cole took his seat without having uttered a word, and no one bothered to ask him a question. (Later, he confided to a friend that it took him 20 years of Sunday afternoons to find the factors of M_{67}.) [Bur; p. 206]

45. About how many digits does M_{67} have?

46. How long do you think it might take you to calculate M_{67}, from its definition, by hand?

47. Describe the mathematics Cole was likely doing in these 20 years of Sunday afternoons to uncover this secret.

48. Do you think that Cole's time in determining a factorization of M_{67} was well spent? Explain.

4.4.2 Modern Analysis of Mersenne Primes with Computers

With the advent of desk calculators and early computers, by 1947 the primality of all 257 numbers on Mersenne's list were determined. Mersenne made only five mistakes out of 257 numbers - a remarkable accomplishment since these numbers grow so fast, as we have already seen.

The growth in the size of the largest know prime has been remarkable over the last 70 years. The term "exponential growth" is often used in everyday speech as a generic way to describe large rates of growth. This is inappropriate as the term has a precise and important meaning. Its use in this context is appropriate. The number of digits in the largest known primes has increased by a factor of 10 about every twelve years since 1945.[6] Lucas' prime, the enormous number above, has *only* 39 digits. In 1961, the record was a $1,332$ digit number. In 1979, the record $13,395$ digits. In 1992, the record $227,832$ digits. In 1999, the record $2,098,960$ digits.

In fact, since 1996 *all* of the largest known prime numbers have been Mersenne primes and they have been discovered by volunteers of the Great Internet Mersenne Prime Search (GIMPS). As part of GIMPS, volunteers run sophisticated computer analysis on pieces of data while their computers are idle. Called ***distributed computing***, volunteers essentially loan their idle, unused computer time to a scientific effort. If you would like to be part of the GIMPS search, and maybe become famous, you can download software at `www.mersenne.org`. This software runs in background in the lowest priority on your computer, using your computer's capabilities when you are not actively using them.

Discovered on December 5, 2001, by 20 year-old **Michael Cameron** (; -) running GIMPS software on his PC, was the primality of the Mersenne number $2^{13466917} - 1$, an almost five-fold increase in the number of digits of the largest known prime from just three years earlier. There have been seven new prime number records since then, three by **Curtis Cooper** (; -) a professor of mathematics and computer science at the University of Central Missouri who keeps GIMPS running on all of his campus' computers. His discoveries include the current record:

$$M_{57,885,161} = 2^{57,885,161} - 1$$

which is a $17,425,170$ digit number. The initial digits of this number are:

$$581,887,266,232,246,442,175,100,212,113,232,368,636,370,852,325,421,589,325\ldots$$

and the final digits are:

$$937,745,410,942,833,323,095,203,705,645,658,725,746,141,988,071,724,285,951.$$

In between these 104 digits are $17,425,66$ digits that have been *removed*.

49. If this page were filled with digits in this way, 35 lines to a page, how many digits could fit on the page?

50. How many pages would it take to write out the digits to Cooper's Mersenne prime in the way just described? Explain.

51. Does this help you appreciate how large this prime is and how remarkable it is that we know deductively that this number is prime? Explain.

[6] See `http://primes.utm.edu/notes/by_year.html` for the largest known primes by year and an interesting discussion about the use of *linear regression* to quantify the growth.

4.5 The Twins

A moving story of arithmetical insight is told by **Oliver Sacks** (British-American neurologist and author; 1933 -) in the chapter "The Twins" from The Man Who Mistook His Wife for a Hat [7] This story involves two autistic twins who had extraordinary abilities to recognize numbers and number relationships in many everyday things around them. For example:

> A box of matches on their table fell, and discharged its contents on the floor: "111," they both cried simultaneously; and then, in a murmur, John said "37". Michael repeated this, John said it a third time and stopped. I counted the matches – it took some time – and there were 111.

52. What does 37 have to do with 111?

53. Why did the twins repeat 37 as they did?

54. What is the mathematical importance of 37 to 111?

This storyline was adapted as one of the pivotal scenes in the movie "Rain Man" when the character Charlie Babbitt (played by **Tom Cruise** (American actor; 1962 -)) begins to realize the remarkable power of brother Raymond, an autistic savant (played by **Dustin Hoffman** (1937; -)). In this adapted scene[8] Raymond wants toothpicks to eat his pancakes. When the waitress accidentally spills the box of toothpicks on the floor, Raymond says "82, 82, 82." Charlie tells him he's "not even close." Raymond replies "246 total." The waitress says that there are 250 in the box and then realizes there are exactly 4 left in the box.

In real life, Sacks spent a long time sitting in the company of the twins to gain their trust. After a great many visits the twins became comfortable and one day began speaking in numbers. Sacks secretly recorded these numbers and later determined they were all eight digit prime numbers. Subsequently he snuck a book of primes into their "meetings". One day he participated in the conversation. After a period of shock, the twins welcomed him into the prime conversation. When Sacks later contributed a nine digit prime, the twins were shocked. But they responded with nine digit primes of their own. And then ten digit primes. And then numbers with more and more digits. Sacks assumed they must be primes, but was uncertain as his book did not include numbers this large and this was well before handheld technology put this information at our immediate disposal.

What is remarkable is that there is no know algorithm for generating primes and no efficient way to determine whether a given number is prime. These problems are holy grails to number theorists. As the great Euler said:

> 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.

Yet, these two twins, whose arithmetic abilities were essentially nonexistent, somehow knew how to communicate with the prime numbers. Is it possible that the secret of the primes was known to these twins? Perhaps. But if it was it has been lost. The twins were separated to help prevent their "unhealthy communication together... in an appropriate, socially acceptable way." They subsequently seemed to lose their special abilities with primes.

[7] HarperPerrenial edition, 1990, pp. 195 - 213.

[8] Which can be found on YouTube by searching "Autism Tootpick Count".

4.6 Congruences: aka Clock Arithmetic

Fermat, then Euler, **Joseph-Louis Lagrange** (Italian mathematician and astronomer; 1736 - 1813), and **Adrien-Marie Legendre** (French mathematician; 1752 - 1833), found clever indirect methods to work with gigantic numbers of the sort considered above. This enabled them to make the most significant advances in number theory during the sixteen and seventeenth centuries. But it was the brilliant Gauss who unified their methods and results. His masterpiece, Disquisitiones Arithmeticae, was written at the age of twenty and yet it "not only began the modern theory of numbers but determined the directions of work in the subject up to the present time."[9]

In this work Gauss introduces the *theory of congruences* which you might already know as ***clock*** or ***modular arithmetic***. Simply enough, 7 hours after 11 o'clock will be 6 o'clock. We write this as

$$7 + 11 \equiv 6 \pmod{12}$$

which we read as "7 plus 11 is congruent to 6 mod 12." The military uses 24-hour clocks so we would have

$$7 + 11 \equiv 18 \pmod{24}.$$

However, 7 hours after 23 hundred hours (i.e., 11 o'clock p.m.) is 6 hundred hours:

$$7 + 23 \equiv 6 \pmod{24}.$$

Gauss noticed that we can define congruences like this for any "clock." We say that $7 + 23 \equiv 6 \pmod{24}$ because $7 + 23 = 30$ and the remainder when 30 is divided by 24 is 6. So we will say a is **congruent** to r mod m and write $a \equiv r \pmod{m}$ whenever a leaves remainder r when divided by m. The remainder r is called the **residue** and the base m of the "clock" is called the **modulus**. In his Disquisitiones, Gauss showed that congruences form arithmetical systems where we can not only add numbers, but subtract, multiply and exponentiate numbers, as well.

There is a slight inconsistency with the mathematical definition and the description using clocks. Namely, using a clock we would say $5 + 7 \equiv 12 \pmod{12}$ since 5 hours after 7 o'clock is 12 o'clock. Indeed, the numbers on a standard clock are $1 - 12$. But, when we consider this congruence with remainders we have $5 + 7 \equiv 0 \pmod{12}$ since the remainder when $5 + 7$ is divided by 12 is 0. For mathematicians mod 12 arithmetic uses the numbers $0 - 11$ instead of $1 - 12$ with 0 taking the place of 12. While the mathematicians approach is best for a deep study of modular arithmetic, for our purposes here either convention will be appropriate.

4.7 Application of Congruences

In one of his remarkable insights, Euler "noticed" that the Mersenne number $M_{83} = 2^{8^3} - 1 = 9,671,406,556,917,033,397,649,408$ was not prime but rather had 167 as a factor. "Noticing" this is remarkable, it seems to be an unpleasant task to check that 167 divides this gigantic number. Let's see how we can use congruences to do this. [10]

[9] Morris Kline, from Mathematical Thought from Ancient to Modern Times, Oxford University Press, 1972, p. 813.

[10] Adapted from The History of Mathematics by David M. Burton.

If 167 is a factor of $2^{83}-1$, then this means 167 divides $2^{83}-1$ evenly. Another way to say this is there is no remainder, which means $2^{83}-1 \equiv 0 \pmod{167}$ So how can we compute powers of 2 mod 167? Well,

$$2^8 = 256 \text{ so } 2^8 \equiv 256 \pmod{167} \equiv 89 \pmod{167}.$$

Since $(2^8)^2 = 2^{16}$, we have

$$2^{16} \equiv (89 \pmod{167})^2 \equiv 89^2 (\text{mod} 167) \equiv 7921 (\text{mod} 167) \equiv 72 (\text{mod} 167).$$

Similarly,

$$2^{32} \equiv 72^2 \pmod{167} \equiv 5184 \pmod{167} \equiv 7 \pmod{167}, \text{ and}$$
$$2^{64} \equiv 7^2 \pmod{167} \equiv 49 \pmod{167}.$$

So then

$$2^{83} \equiv \left(2^{64} \pmod{167}\right) \times \left(2^{16} \pmod{167}\right) \times \left(2^3 \pmod{167}\right)$$
$$\equiv (49 \times 72 \times 8) \pmod{167} \equiv 28224 \pmod{167} \equiv 1 \pmod{167}.$$

Hence, $2^{83}-1 \equiv (1-1) \pmod{167} \equiv 0 \pmod{167}$.

This is a very powerful method indeed. In fact, without methods like these, the computations that are necessary to encrypt messages, with algorithms like the RSA algorithm (considered in Section 4.10, would not be feasible.

4.8 Powers and Congruences

55. Reduce each of the congruences below to a number smaller than the modulus, 3:

$$1^2 \equiv \_\_\_ \pmod{3}$$
$$2^2 \equiv \_\_\_ \pmod{3}$$
$$3^2 \equiv \_\_\_ \pmod{3}$$
$$4^2 \equiv \_\_\_ \pmod{3}$$
$$5^2 \equiv \_\_\_ \pmod{3}$$
$$6^2 \equiv \_\_\_ \pmod{3}$$
$$7^2 \equiv \_\_\_ \pmod{3}$$

56. Do you see a pattern in your answers to Investigation **55**? If so, do you think it will continue indefinitely? Explain why.

57. Reduce each of the congruences below to a number smaller than the modulus, 4:

$$1^3 \equiv \_\_\_ \pmod{4}$$
$$2^3 \equiv \_\_\_ \pmod{4}$$
$$3^3 \equiv \_\_\_ \pmod{4}$$

$$4^3 \equiv \_\_\_ \pmod 4$$
$$5^3 \equiv \_\_\_ \pmod 4$$
$$6^3 \equiv \_\_\_ \pmod 4$$
$$7^3 \equiv \_\_\_ \pmod 4$$
$$8^3 \equiv \_\_\_ \pmod 4$$
$$9^3 \equiv \_\_\_ \pmod 4$$

58. Do you see a pattern in your answers to Investigation **57**? If so, do you think it will continue indefinitely? Explain why.

59. Reduce each of the congruences below to a number smaller than the modulus, 5:

$$1^4 \equiv \_\_\_ \pmod 5$$
$$2^4 \equiv \_\_\_ \pmod 5$$
$$3^4 \equiv \_\_\_ \pmod 5$$
$$4^4 \equiv \_\_\_ \pmod 5$$
$$5^4 \equiv \_\_\_ \pmod 5$$
$$6^4 \equiv \_\_\_ \pmod 5$$
$$7^4 \equiv \_\_\_ \pmod 5$$
$$8^4 \equiv \_\_\_ \pmod 5$$
$$9^4 \equiv \_\_\_ \pmod 5$$

60. Do you see a pattern in your answers to Investigation **59**? If so, do you think it will continue indefinitely? Explain why.

61. Reduce each of the congruences below to a number smaller than the modulus, 6:

$$1^5 \equiv \_\_\_ \pmod 6$$
$$2^5 \equiv \_\_\_ \pmod 6$$
$$3^5 \equiv \_\_\_ \pmod 6$$
$$4^5 \equiv \_\_\_ \pmod 6$$
$$5^5 \equiv \_\_\_ \pmod 6$$
$$6^5 \equiv \_\_\_ \pmod 6$$
$$7^5 \equiv \_\_\_ \pmod 6$$
$$8^5 \equiv \_\_\_ \pmod 6$$
$$9^5 \equiv \_\_\_ \pmod 6$$

62. Do you see a pattern in your answers to Investigation **61**? If so, do you think it will continue indefinitely? Explain why.

63. Reduce each of the congruences below to a number smaller than the modulus, 7:

$$1^6 \equiv \_\_\_ \pmod 7$$

$$2^6 \equiv \_\_\_ \pmod 7$$

$$3^6 \equiv \_\_\_ \pmod 7$$

$$4^6 \equiv \_\_\_ \pmod 7$$

$$5^6 \equiv \_\_\_ \pmod 7$$

$$6^6 \equiv \_\_\_ \pmod 7$$

$$7^6 \equiv \_\_\_ \pmod 7$$

$$8^6 \equiv \_\_\_ \pmod 7$$

$$9^6 \equiv \_\_\_ \pmod 7$$

64. Do you see a pattern in your answers to Investigation **63**? If so, do you think it will continue indefinitely? Explain why.

65. You should see some patterns emerging that tie together some of the of the groups of congruence computations. Make one or more conjectures describing congruences of the form

$$a^{n-1} \bmod n,$$

based on properties of the numbers a and n.

4.9 The Chinese Remainder Theorem - Mathematical Magic

A popular online trick is "Calculating Your Age by Chocolate." The trick proceeds via the following steps:

- Choose how many times a week you would like to eat chocolate - any positive whole number.
- Multiply this number by 2.
- Add 5 to the product.
- Multiply the sum by 50.
- Add the current year to the product.
- From this sum subtract 250 if you have already had a birthday this year, otherwise subtract 251.
- From this difference subtract the year of your birth.

66. Pick a number of times a week you want to eat chocolate and perform the steps in the trick. What do you notice about the answer?

67. Repeat the trick with the different starting number.

68. Determine how the trick works algebraically by denoting the starting number by the variable x and performing all of the steps in the trick. Describe how the trick works and any potential limitations on it.

Number tricks based on simple algebraic identities like this have been performed for hundreds of years.

A much more substantial trick based on congruences was described by Fibonacci in his Liber Abbaci in 1202. Instead of calling it a "trick" he referred to it as "a pleasant game." But the intent was clear, a method through which "you can know the number said to him in private."[11]

The basis for this trick is the *Chinese remainder theorem* whose earliest know statement appears in the work of **Sun Tzu** (Chinese mathematician; circa 300 - circa 500).

69. Think of any number between 1 and 105. Call your mystery number x.

70. What is x congruent to mod 3? Label your answer as c_1, so we have $x \equiv c_1 \pmod 3$.

71. What is x congruent to mod 5? Label your answer as c_2, so we have $x \equiv c_2 \pmod 5$.

72. What is x congruent to mod 7? Label your answer as c_3, so we have $x \equiv c_3 \pmod 7$.

73. What do the numbers 3, 5, and 7 have to do with 105?

74. Evaluate the expression $m = c_1 \times 35 \times 2 + c_2 \times 21 \times 1 + c_3 \times 15 \times 1$.

75. Reduce m mod 105. Surprised?

76. Do you think that this trick will work for any number between 1 and 105? Explain.

77. Now think of any number between 1 and 231. Call your mystery number x.

78. What is x congruent to mod 3? Label your answer as c_1, so we have $x \equiv c1 \pmod 3$.

79. What is x congruent to mod 7? Label your answer as c_2, so we have$x \equiv c_2 \pmod 7$.

80. What is x congruent to mod 11? Label your answer as $c3$, so we have $x \equiv c_3 \pmod{11}$.

81. Evaluate the expression $m = c_1 \times 77 \times 2 + c_2 \times 33 \times 3 + c_3 \times 21 \times 10$.

82. In the expression for m what do you think gave rise to the numbers $77, 33$, and 21? Explain.[12]

83. Reduce m mod 231. Surprised?

[11] Quoted on p. 189-90 of The Mathematical Experience by Philip J. Davis and Reuben Hersh.

[12] The numbers 2, 3, and 10 in this expression are a bit more mysterious. They were chosen so that $77 \times 2 \equiv 1 \pmod 3, 33 \times 3 \equiv 1 \pmod 7$, etc. With this in mind, one can now generalize this trick to include any number of moduli. In other words, you could have the dupe choose any number between 1 and $255, 255 = 3 \times 5 \times 7 \times 11 \times 13 \times 17$ and then ask for the six necessary *moduli*.

4.10 Secret Codes, Ciphers and Cryptography

> Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing that shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.[13]
>
> **Edgar Allan Poe** (American author and poet; 1809 - 1849)

The long history of secret codes was mentioned in the introduction. We have now mathematically arrived at a locale where we can begin to view the mathematics that underlies modern encryption schemes.

In the previous section you saw how the Chinese remainder theorem can be used to recover an unknown number from knowledge of specific residues. This gives rise to a **cipher**, an algorithm for encrypting secret information. If you wanted to share secret numbers with a friend, all you would need to do is secretly agree beforehand on the the ***key*** - a large number which is the product of unique primes. To share a secret number you could send your friend a list of the residues and they could reconstruct the secret number. Even if your list of residues were intercepted by a foe, it would be hard for your secret number to be reconstructed without the identity of the key.

This is a good first example see how a mathematical cipher works. There are practical limitations to this particular method. And there is the enormous limitation that has plagued all ciphers throughout history - the sender and receiver must both have prior knowledge of the key. In any arena where the goal is to keep information secret, how can keys be effectively shared in secret? It was an enormous breakthrough in the 1970's when a host of computer scientists and mathematicians developed methods of **public key cryptography** where there are two distinct keys, a **private key** which is known by the receiver and a **public key** which is revealed to the world and allows anyone to encrypt messages which can only be decrypted by the holder of the private key.

One of the most important such public key crypotsystems is the ***RSA algorithm*** named after **Ron Rivest** (American computer scientist; 1947 -), **Adi Shamir** (Israeli computer scientist; 1952 -), and **Leonard Adleman** (American computer scientist and biologist; 1945 -). As you shall see, the underlying mechanism that drives this method is ***Fermat's little theorem*** - the result you found in Investigation **65**.

To employ the RSA algorithm the Receiver must build the keys. This is done as follows:

- Two very large primes p and q are chosen.
- The product $n = p \cdot q$ is computed. The number n is one part of the public key.
- An exponent e is chosen so that $1 < e < (p-1)(q-1)$ and e shares no common factors with $(p-1)(q-1)$. The number e is the other part of the public key.
- The equation $k \cdot e \equiv 1 \pmod{(p-1)(q-1)}$ is solved for k. The number k is the private key.
- The public key (n, e) is made public for all to see.

With the keys identified, but before we describe the workings of the cipher, it is important to understand the essential security matter - factoring large numbers into primes. The primes p and

[13] Quoted in "Cryptology: From Caesar Ciphers to Public-key Cryptosystems," by D. Luciano and G. Prichett, in *The College Mathematics Journal*, Vol. 18, No. 1, Jan. 1987, pp. 2-17.

q are generally chosen to have about 200 digits and so n has about 400 digits. This number is part of the public key, made public for all of the world to see!

84. Suppose a foe with knowledge of the public key was able to factor n into its prime factors. Describe why this would enable the foe to determine the private key and break any message within this particular RSA scheme.

This is a prime example of why our understanding of primes is so important. And why the incredible abilities of The Twins might have helped uncover one of the great mysteries in all of mathematics.

85. A Sender needs to translate their message text into a number so it can be encrypted before it is sent. After decryption the Receiver will need to translate the number which is output by this algorithm back into the message text. Determine a way that you could represent any alphabetic, text based message as a single number in such a way that the message can be easily reconstructed from the number.

To send a secret message a Sender simply converts the text message into a single number, as in Investigation **85**. Denote this number by m for "message." The Sender then computes:

$$c \equiv m^e \pmod{n}.$$

The encrypted ciphertext, denoted by c, can then be sent as a *public message*, as it can only be decrypted by the Receiver who is the only person in possession of the private key.

The Receiver decrypts the message by computing:

$$c^k \bmod n.$$

But why does this work? Why does this recover the secret message m?

86. Since k is defined to satisfy $k \cdot e \equiv 1 \pmod{(p-1)(q-1)}$, explain why we can write $k \cdot e - 1 = j(p-1)(q-1)$ for some integer j.

87. Explain why the number computed by the Receiver, $c^k \bmod n$, is equal to

$$m^{e \cdot k} \bmod n.$$

88. Explain why $m^{e \cdot k} = m^{e \cdot k - 1} \cdot m$.

We are now ready to invoke Fermat's little theorem, which will be done both $\bmod p$ and $\bmod q$ and then combined.

89. Explain why

$$m^{e \cdot k} = \left(m^{p-1}\right)^{j(q-1)} \cdot m.$$

90. Modulo p this means

$$m^{e \cdot k} \equiv \left(m^{p-1}\right)^{j(q-1)} \cdot m \pmod{p}.$$

Use Fermat's little theorem to explain why this expression on the right is congruent to m.

91. Explain why $m^{e \cdot k} - m$ is a multiple of p.

92. Explain why $m^{e \cdot k} - m$ must also be a multiple of q.

93. Since $m^{e \cdot k} - m$ is a multiple of both of the different primes p and q, explain why it must be a multiple of the product $p \cdot q$.

94. Determine the number $m^{e \cdot k} \bmod n$ and explain why this means that the Receiver has recovered the secret message.

So this is some slightly technical algebra. But consider the enormity of what you have just shown. You have just rediscovered the inner workings a special application of a 300 year-old, theoretical result about whole numbers - one that has revolutionized secrecy and that is fundamental to the information age. Unlike the cute application of algebra in "chocolate math," in RSA we have an algorithm that, together with related advances in public key encryption methods, is fundamental to *all* of e-commerce, computer security, weaponry codes, and secure communication. The linchpin to all of this? As yet we have found no efficient methods for factoring large numbers or finding the pattern to the primes - the key builders in encryption can stay far ahead of the numerical lock pickers.

For most of the history of cryptography, Poe's declaration that opened this section seemed valid. But human ingenuity combined with powerful mathematics has managed to create ciphers which cannot be resolved.

4.11 Connections

4.11.1 History: Alan Turing and World War II Codebreaking

Alan Turing (British mathematician; 1912 - 1954) was one the twentieth century's most important mathematicians. He did critical work in logic and in the development of modern computer science. Additionally, he played a critical role in the intelligence efforts during the Second World War. In fact, his efforts prompted the mathematician Peter Hilton to remark:

> I.J. Good, a wartime colleague and friend, has aptly remarked that it is fortunate that the authorities did not know during the war that [Alan] Turing was a homosexual; otherwise, the Allies might have lost the war.[14]

Figure 4.2: Alan Turing.

Indeed, when his homosexuality was discovered after the war he was subjected to house arrest and a variety of medical "treatments." Soon afterward this highly decorated war hero committed suicide.

Find out more about the life and mathematical accomplishments of Alan Turing. Write a brief, two- to three-page biographical essay, addressed to fellow students, that describes your findings.

4.11.2 History: Polish Mathematicians and World War II Codebreaking

Alan Turing's contributions to mathematics visionary and greatly ahead of his time. His work for the Allies' code breaking efforts were part of a larger effort in which many mathematicians played important roles.

The focus of most of the code breaking work was to discover the secret workings of the German ***Enigma machine*** a mechanical encryption/decryption machine which worked with a number of rotors and gears. The working of these machines can be described as *permutations*.

[14] Quoted in "Cryptanalysis in World War II – and Mathematics Education," by Peter Hilton, *Mathematics Teacher*, Vol. 77, Oct. 1984, pp. 548-52.

Figure 4.3: Four rotor Enigma machine (right) and Enigma plugboard (left).

Some of the simplest Enigma machines were decrypted as early as 1932 by **Marian Adam Rejewski** (Polish mathematician; 1905 - 1980).

The work of the Allied mathematicians is celebrated in the Bletchley Park Museum not far from London, England and at the National Cryptologic Museum in Annapolis Junction, Maryland. Additionally, enormous amounts of information about these topics is available online, in print, and in documentaries. There are also numerous novels and movies that present historically-based fiction related to the actual events and accomplishments.

4.11.3 History: Navajo Code Talkers and World War II Encryption

While the code breaking focus in the war in the Atlantic was on the German Enigma machine, the war in the Pacific had its own important links to encryption. Allied intelligence agents were somewhat successful at breaking Japanese secret codes. The outcome at the Battle of Midway, one of the changing points in the war, was dramatically impacted by U.S. intelligence success in codebreaking.

In sharp contrast, the Axis forces had much less success at deciphering Allied codes. One reason was that U.S. forces encrypted some of their most important messages first by having native Americans, most notably Navajos, translate the messages into their native language first before they were then encrypted using mathematical algorithms. These ***Navajo Code Talkers***, as the most well-known group were called, had been secretly enlisted in the Marine's intelligence efforts. Congressional Gold Medals were awarded to the 29 Navajo Code Talkers in December, 2000.

The story of the Navajo Code Talkers serves as the basis for the major motion picture Windtalkers (MGM, 2002). Find out more about the Navajo Code Talkers and their role in U.S. intelligence efforts in the Second World War.[15] Write a brief, two- to three-page biographical essay, addressed

[15]See, e.g., Navajo Weapon: The Navajo Code Talkers by Sally McClain, Rio Nuevo Publishers, 2002; Warriors: Navajo Code Talkers by Kenji Kawano, Kanji Kawano, and Carl Gorman, Northland Publishers, 1990; The Navajo

to fellow students, that describes your findings.

4.11.4 Secret Codes and Statistics

The oldest and historically most frequently employed type of secret codes are based on a scheme where each letter of the alphabet is replaced by a different letter. While one can try to complicate this basic scheme in many ways, codes like this are relatively easy to break using statistical methods. For a nice introduction to the statistical analysis of codes, in a guided discovery approach that is quite similar to the approach in this text, see Section 9.2 "The Breaking of Ciphers and Codes: An Application of Statistics" (pp. 537 - 545) in Mathematics: A Human Endeavor by Harold R. Jacobs.[16]

Code Talkers by Doris A. Paul, Dorrance Publishing, 1998.

[16] Third edition, 1994 by W.H. Freeman.

4.12 Further Investigations

4.12.1 Dirichlet and Primes in Arithmetic Progressions

The discussion of twin primes and arithmetic progressions of primes focussed on primes that arise consecutively in arithmetic progressions. In the mid-Eighteenth century mathematicians were not concerned with these primes arising consecutively, but rather how frequently primes occurred in a given arithmetic sequence. For example, the ***arithmetic progression*** starting at 3 with gap size 4 generates the primes that are circled:

$$\textcircled{3}, \textcircled{7}, \textcircled{11}, 15, \textcircled{19}, \textcircled{23}, 27, \textcircled{31}, 35, 39, \textcircled{43}, \textcircled{47}, 51,$$
$$55, \textcircled{59}, 63, \textcircled{67}, \textcircled{71}, 75, \textcircled{79}, \textcircled{83}, 87, 91, 95, 99, \ldots$$

For the numbers up to 100, this arithmetic progression has missed the primes

$$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97.$$

It has generated 13 primes and missed 12. In other words, it has generated roughly half of the primes under 100. As you count primes generated further and further out, this arithmetic progression generates the primes with a frequency of about $\frac{1}{2}$. Indeed, it is the case that *asymptotically* the frequency is exactly $\frac{1}{2}$.

A general result which establishes the frequency of primes in any arithmetic progression was proved in 1837 by **Johann Peter Gustav Lejeune Dirichlet** (German mathematician; 1805 - 1859). It is a beautiful and powerful result, established with the invention of mathematical tools in number theory which remain in critical use today - including in investigations of the $1 Million *Riemann hypothesis* which we will meet shortly.

F1. Investigate the proportion of primes that appear to be generated in the general arithmetic progression $a, a+d, a+2d, a+3d, \ldots$ by investigating a number of specific cases. It may be useful to compile data with a group. Using this empirical data, see if you can rediscover Dirichlet's result.

4.12.2 The Euler-Fermat Theorem

In Investigation **65** you should have been able to characterize the results for some of the groups of congruence computations, namely those with prime moduli. You may have found individual patterns for some of the non-prime moduli, but likely nothing to tie them together.

Fermat never found such a connection, but Euler would later after he proved Fermat's little theorem.

For any number n define the **Euler phi function**, denoted by $\phi(n)$, to be the number of positive integers between 1 and n whose greatest common factor with n is 1. So, for example, $\phi(8) = 4$ since $1, 3, 5$ and 7 are numbers less than 8 who share only 1 as a common factor with 8.

F2. Explain why $\phi(3) = 2$.

F3. Explain why $\phi(4) = 2$.

F4. Explain why $\phi(5) = 4$.

F5. Explain why $\phi(6) = 2$.

F6. Prove that $\phi(p) = p - 1$ for any prime p.

F7. In Investigation **57** you investigated mod 4 congruences of cubes. Instead, consider squares. That is, reduce each of the congruences below to a number smaller than the modulus, 4:

$$1^2 \equiv \_\_\_ \pmod 4$$
$$2^2 \equiv \_\_\_ \pmod 4$$
$$3^2 \equiv \_\_\_ \pmod 4$$
$$4^2 \equiv \_\_\_ \pmod 4$$
$$5^2 \equiv \_\_\_ \pmod 4$$
$$6^2 \equiv \_\_\_ \pmod 4$$
$$7^2 \equiv \_\_\_ \pmod 4$$
$$8^2 \equiv \_\_\_ \pmod 4$$
$$9^2 \equiv \_\_\_ \pmod 4$$

F8. Similarly, for mod6 congruences investigate squares instead of quintics:

$$1^2 \equiv \_\_\_ \pmod 6$$
$$2^2 \equiv \_\_\_ \pmod 6$$
$$3^2 \equiv \_\_\_ \pmod 6$$
$$4^2 \equiv \_\_\_ \pmod 6$$
$$5^2 \equiv \_\_\_ \pmod 6$$
$$6^2 \equiv \_\_\_ \pmod 6$$
$$7^2 \equiv \_\_\_ \pmod 6$$
$$8^2 \equiv \_\_\_ \pmod 6$$
$$9^2 \equiv \_\_\_ \pmod 6$$

F9. Choose some other moduli $n > 6$ which is non-prime and reduce each of the congruences below:

$$1^{\phi(n)} \equiv \_\_\_ \pmod n$$
$$2^{\phi(n)} \equiv \_\_\_ \pmod n$$
$$3^{\phi(n)} \equiv \_\_\_ \pmod n$$
$$4^{\phi(n)} \equiv \_\_\_ \pmod n$$
$$5^{\phi(n)} \equiv \_\_\_ \pmod n$$
$$6^{\phi(n)} \equiv \_\_\_ \pmod n$$

$$7^{\phi(n)} \equiv \_\_\_ \pmod{n}$$
$$8^{\phi(n)} \equiv \_\_\_ \pmod{n}$$
$$9^{\phi(n)} \equiv \_\_\_ \pmod{n}$$
$$10^{\phi(n)} \equiv \_\_\_ \pmod{n}$$
$$11^{\phi(n)} \equiv \_\_\_ \pmod{n}$$

F10. Can you now generalize Fermat's little theorem to describe congruences of the form $a^{\phi(n)} \bmod n$?

4.12.3 Example of RSA Implementation

Those interested in trying a concrete example of implementing RSA to develop a small-scale set of keys to encrypt and decrypt a simple message will find the article "Using Clock Arithmetic to Send Secret Messages" by Catherine A. Forini, *The Mathematics Teachers*, Vol. 89, No. 2, February 1996, pp. 100 - 104 to be helpful.

One can also find many worked out examples on the Internet.

F11. Set up your own small-scale RSA scheme and use it to encode and decode a simple message.

Chapter 5

Class Numbers: A Bridge Between Two $1 Million Dollar Problems

> If I were to awaken after having slept for a thousand years, my first question would be: Has the Riemann hypothesis been proven?
>
> **David Hilbert** (German mathematician; 1862 - 1943)

> It will be another million years, at least, before we understand the primes.
>
> **Paul Erdos** (Hungarian mathematician; 1913 - 1996)

> It would be very discouraging if somewhere down the line you could ask a computer if the Riemann hypothesis is correct and it said, 'Yes, it is true, but you won't be able to understand the proof.'
>
> **Ronald Graham** (American mathematician; 1935 -)

5.1 Guiding Problems

At the 1900 International Congress of Mathematicians, the most prestigious mathematical conference and which is held every four years, **David Hilbert** (German mathematician; 1862 - 1943), perhaps the preeminent mathematician of the time, proposed a list of problems to challenge mathematicians for the next century. The complete list included 23 problems. These problems have become known as ***Hilbert's problems***. The prestige these problems have had are a tribute to the great insights of Hilbert to focus on these specific problems.

Over the past century, the majority of Hilbert's problems have been resolved.

On May 24, 2000, "to celebrate mathematics in the new millennium" the Clay Mathematics Institute announced seven *Millennium Prize Problems* each which carried a $ 1 Million prize for its solution. The topics in this chapter are integrally related to two of these problems, both of which remain unresolved, the *Riemann hypothesis* and the *Birch and Swinerton-Dyer conjecture*.

The quotes that open the chapter give some sense of the importance these problems hold for mathematicians. The influential **George Polya** (Hungarian mathematician and educator; 1887 - 1985) tells a wonderful story about the grip the Riemann hypothesis had on **Godfrey Harold Hardy** (English mathematician; 1877 - 1947):

You must know that Hardy had a running feud with God. In Hardy's view God had nothing more important to do than frustrate Hardy. This led to a sort of insurance policy for Hardy one time when he was trying to get back to Cambridge after a visit to [Herald] Bohr in Denmark. The weather was bad and there was only a small boat available. Hardy thought there was a real possibility the boat would sink. So he sent a postcard to Bohr saying, "I proved the Riemann Hypothesis. G.H. Hardy." That way if the boat sank, everyone would think that Hardy had proved the Riemann Hypothesis. God could not allow so much glory for Hardy so he could not allow the boat to sink.

5.2 Distribution of the Primes

To me, that the distribution of prime numbers can be so accurately represented in a harmonic analysis is absolutely amazing and incredibly beautiful. It tells of an arcane music and a secret harmony composed by the prime numbers.[1]

Enrico Bombieri (Italian mathematician; 1940 -)

In Chapter 4 there were investigations of different types of primes. A fundamental question is: How many primes are there? If Fermat had been correct and all numbers of the form $F_n = 2^{2^n} + 1$ were prime then there would clearly be infinitely many primes - this expression would generate them one after another indefinitely. Similarly if we could find out which among the Mersenne numbers were prime. We noted that by Zhang's new bounded gaps theorem there are infinitely many primes that are separated by at most 246. But is there an easier way to see that there are infinitely many primes?

It turns out there are many different proofs that there are infinitely many primes. One of the author's favorites was thought of by **Filip Saidak** (; -) as he was waiting for a bus![2] The mind works in such mysterious ways. If you're interested in this beautiful proof, it's included in the chapter "Proof" in Discovering the Art of Mathematics: Reasoning, Proof, Certainty & Truth. Here you'll rediscover one of the most famous of the proofs of the infinitude of the primes, Euclid's proof his Elements.

1. Complete each of the following computations and determine if the resulting number is prime or not:

$$2 + 1 =$$

$$2 \cdot 3 + 1 =$$

$$2 \cdot 3 \cdot 5 + 1 =$$

$$2 \cdot 3 \cdot 5 \cdot 7 + 1 =$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 =$$

2. Do you think that the pattern in Investigation **1** will continue indefinitely? Why or why not?

3. If the pattern in Investigation **1** did go on for ever, what could you conclude about the number of primes?

[1] From "Prime Territory: Exploring the Infinite Landscape at the Base of the Number System", *The Sciences*, Sept/Oct 1992.

[2] Personal communication.

4. Complete the calculation

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1,$$

and then determine if the resulting number is prime. If it is not prime, completely factor the number into *prime factors*.

5. Repeat Investigation **4** for the number $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1$.

6. Repeat Investigation **4** for the number $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 + 1$. (Hint: 347.)

7. In the preceding Investigations, if the number formed was not prime then how are its prime factors related to the primes used to create the number?

8. If the pattern in Investigation **7** did continue forever, what would this tell you about the number of prime numbers? Explain.

Consider the general number formed in this sequence we're using to find more primes. It has the form

$$2 \cdot 3 \cdot 5 \cdots p_n + 1$$

where $2, 3, 5, \ldots p_n$ are consecutive primes.

9. Is the number $2 \cdot 3 \cdot 5 \cdots p_n + 1$ divisible by 2? Explain.

10. Is the number $2 \cdot 3 \cdot 5 \cdots p_n + 1$ divisible by 3? Explain.

11. Is the number $2 \cdot 3 \cdot 5 \cdots p_n + 1$ divisible by 5? Explain.

12. Is the number $2 \cdot 3 \cdot 5 \cdots p_n + 1$ divisible by p_n? Explain.

13. Is the number $2 \cdot 3 \cdot 5 \cdots p_n + 1$ divisible by any of the primes between 2 and p_n? Explain.

14. Explain why this guarantees that there is another prime larger than p_n.

15. Thereby, explain why this process proves that there are infinitely many primes.

Now that we know the primes go on forever a natural question to ask is: How are the primes distributed among the other numbers? With enormous patience, mathematicians of the eighteenth and nineteenth century compiled lists of primes and sought to determine their distribution. Some of the most basic data is that between $1 - 1,000$ there are 168 primes. Between $1,001 - 2,000$ there are 135 primes. Between $2,001 - 3,000$ there are 127 primes. Between $3,001 - 4,000$ there are 120 primes. It seems the primes arise less frequently the larger the numbers we look at.

16. Put yourself in the role of an eighteenth century mathematician seeking to determine whether a given number was prime or not. What must you do to guarantee that the number is prime?

17. Suppose two numbers are chosen at random, one significantly larger than the other. Why is the larger number less likely to be prime?

Let's return to numbers like those you used in the Euclidean proof of the infinitude of the primes, numbers like:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$$

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$ is prime. What about other, nearby numbers?

18. Without using a calculator determine whether $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 2$ is prime or not.

19. Similarly, without a calculator, determine whether $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 3$ is prime or not.

20. Repeat Investigation **19** for each of the numbers $2{\cdot}3{\cdot}5{\cdot}7{\cdot}11{\cdot}13{+}4$ through $2{\cdot}3{\cdot}5{\cdot}7{\cdot}11{\cdot}13{+}13$.

21. How many consecutive numbers have you found that are composite?

22. Determine how you could find over 50 composite numbers in a row.

23. Determine how you could find over 100 composite numbers in a row.

24. Is there any limit to the number of consecutive composite numbers you could find? Explain.

25. Contrast your answer in Investigation **24** with the conclusion of the twin prime conjecture. What does this contrast tell you about the distribution of the prime numbers?

Thus, we see great volatility in the distribution of the primes. As early as 1800 mathematicians began to suspect the distribution of primes could be understood if instead you considered it *on average* as one moves farther and farther out along the number line. And some began to think the behavior may be related to the *natural logarithm* via the expression $\frac{n}{\ln n}$.

26. Compute $\frac{n}{\log_e n}$ for $n = 1000$ and compare the result with the data about primes given above.

27. Repeat for $n = 2000, 3000$ and 4000.

In 1859 **Bernhard Riemann** (Berman mathematician; 1826 - 1866) wrote a 6-page paper named "On the Number of Prime Numbers Less Than a Given Quantity." This became one of the most important papers written in the history of mathematics, giving rise to the Riemann hypothesis which was both a Hilbert Problem and one of the Millennium Prize Problems. The handwritten manuscript, along with an English translation, are available at `http://www.claymath.org/publications/riemanns-1859-manuscript`. While the Riemann hypothesis remains an open question, the paper's approach was so powerful - in particular because it brought the power of *imaginary numbers* and *complex numbers* to the study of number theory - that it enabled mathematicians to make progress on the average behavior of the distribution of the prime numbers. In 1896 **Jacque Salamon Hadamard** (French mathematician; 1865 - 1963) and **Charles Jean Gustave Nicolas Baron de la Vallee Poussin** (Belgian mathematician; 1866 - 1962) independently proved the celebrated *Prime Number Theorem* which says that as you go farther and farther out in the number line the number of primes in the first n numbers is more and more closely approximated by the quantity $\frac{n}{\log_e n}$.

This still leaves the specific behavior of the distribution of primes quite mysterious. **Don Zagier** (American mathematician; 1951 -), one of the Directors of the Max Planck Institute for Mathematics, summarized our understanding of the distribution of the prime numbers as follows:

> There are two facts about the distribution of prime numbers which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that despite their simple definition and role as the building blocks of the natural numbers, the prime numbers... grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behaviour, and that they obey these laws with almost military precision.

5.3 Class Numbers

The results of investigations in the previous suggestion should give a fairly clear indication of our fairly meager understanding of the distribution of the primes. Much deeper understanding of the primes would follow from a positive validation of the Riemann Hypothesis. Indeed, even its name speaks to this fact. Mathematicians generally use the word "conjecture" rather than "hypothesis". However, many mathematicians have worked as if the Riemann hypothesis will be validated and can be used in their work, so the word "hypothesis" is appropriate. **Peter Sarnak** (South African mathematician; 1953 -) notes:

> The Riemann Hypothesis is the central problem and it implies many, many things. One thing that makes it rather unusual in mathematics today is that there must be over five hundred papers - somebody should go and count - which start "Assume the Riemann Hypothesis", and the conclusion is fantastic. And those [conclusions] would then become theorems...With this one solution you would have proven five hundred theorems or more at once.[3]

In this section we consider an accessible topic that involves the distribution of primes using the fantastical, and surprising, lens of imaginary and complex numbers to see. The *class numbers* that arise in these investigations are related to two 1$ Million problems.

28. Consider the number sequence which begins $0, 2, 6, 12, 20$. There is a simple way that this pattern can be extended.[4] What would the next six terms be if extended in this simple way?

We would like to find a function f whose outputs are precisely this sequence. In table form this means we want a function with the following table of values:

n	f
0	0
1	2
2	6
3	12
4	20

29. Copy the table above into your notes, adding several more of the values you found.

30. Find a pattern in this table of values.

31. Can you use this pattern to determine a formula for the function f?

Patterns can be viewed in many different ways. One way to view the pattern in the table above is to factor each f value into two terms.

32. Factor each term on the right of the table into two terms. Can you do this so there is a clear pattern in the individual factors?

[3] From Dr. Riemann's Zeros by K. Sabbagh, Atlantic, 2002, p.188

[4] One must be careful. Although problems like this appear on standardized exams of all sorts, they are inappropriately misleading. There are infinitely many ways in which this sequence can continue. 0, 2, 6, 12, 20, 0, 6, 12, 20, 0, 6, 12, 20,... is one perfectly acceptable way. So is 0, 2, 6, 12, 20, 0, 4,12, 24, 40, 0, 6, 18, 36, 60,... In fact, there is nothing wrong with 0, 2, 6, 12, 20, 3, 4, 3, 4, 3, 4,..., it's just not what we might expect.

33. Use this factoring to determine a formula for the function f.

34. Check your result for several known values of n to insure your formula is correct.

The function $s(n) = n^2 + n + 17$ is closely related to the function you just found.

35. Make a table of values of the function s as the variable n ranges from 0 to 8.

36. The difference between the f values from one row of the table to the next are called **first differences**. Compute the first differences of the functions f and s and show they are the same. Explain why this should be so.

37. You should notice an interesting attribute that all of the s values in your table in Investigation **35** share. Explain.

38. Do you believe that all entries in the table, no matter how far it is continued, will share the attribute you have described in Investigation **37**? Explain.

39. Check your result in Investigation **37** by continuing your table to include the values $n = 8, \ldots, 15$. Does this increase your confidence in your previous answer?

40. What is the value of the next output, $s(16)$? Does it share this pattern of all outputs sharing the same attribute?

41. What about the value of the next output, $s(17)$? Show algebraically why this output must violate your pattern.

5.4 A Class Number Sieve

The function s was very interesting because it generated a long list of primes. Is there a different function that generates even more primes?

With $s(n) = n^2 + n + 17$ as our impetus, we are going to look via *quadratic functions* of the form $q(n) = n^2 + n + c$ where we will let the value of c vary.

42. Show that the first differences of the quadratic q will be the same as those of f and s above regardless of the value of c.

The observation in Investigation **42** will allow us to analyze the family of quadratics q in our search for primes. We will do so by constructing a *Class Number Sieve* - a physical tool for looking for prime generating quadratic functions that we now describe.

The appendix contains several sheets you will need. Take a 1 - 250 number table and highlight all of the prime numbers using a highlighter. Cut off one of the margins and then roll the table into a 1 - 250 cylinder which is slightly offset so as you follow the numbers $1 - 2 - 3 - \cdots$ around the cylinder $11 - 12 - 13 - \cdots$ immediately follow 10 on the cylinder. I.e. so you have wrapped the number line around the cylinder in a spiral. Tape it securely. To complete the prime cylinder, record a 0 just before the 1 in the number spiral. The exterior of the sieve is constructed using the indicated sheet from the appendix. Carefully use a razor knife to cut out each of the highlighted cells on sieve. Highlight the border of top, left window with a highlighter - it will be our **sieve**

setting. Cut both the right and left margins off the sieve along the indicated lines. Put clear, transparent tape over the front and back of each of the "windows" in the sieve for strength. Then wrap the sieve around the cylinder. Carefully align the marks on the right with the appropriate windows so it orientation will be the same as the number table cylinder.

Figure 5.1: Completed Class Number Sieve.

43. Rotate the sieve so the sieve setting is 17. Your sieve should look like that in Figure 5.1 What do you notice about the entries in the windows? I.e. precisely how do these entries relate to results of earlier investigations?

44. Rotate the sieve again so the sieve setting is 0. What do you notice about the entries in the windows? I.e. precisely how do these entries relate to results of earlier investigations?

45. You should see a critical relationship between entries in the windows for a given sieve setting and the functions q parameterized by the value of c. Describe this relationship precisely

Our observations in Investigation **43** - Investigation **45** show us that this **Class Number Sieve** is tool we need to investigate the family of quadratics q and their ability to generate primes.

We could continue providing a list of prompts, but this is a perfect opportunity for you to explore. After all, mathematics is really characterized by open ended investigations of exactly this sort. I.e. we've taken you on a guided tour so far, now it is time to set out on your own for a bit.

Goal: Understand the ways in which functions q generate primes as outputs depending on the value of the parameter c.

This investigation should take some time. You should write down notes, observations, perhaps tables of data, etc. You should come up with a number of results, both positive and negative (i.e. generating lots of primes versus not many at all), which you should state as precise conjectures. These conjectures should relate to our study of the distribution of primes above.

5.5 Gauss' Class Number Problem

In the previous section you found that several sieve settings were special - giving rise to long strings of consecutive primes. Are there other sieve settings that exist simply beyond the physical limits of the class number sieve we built? The answer to this question about whole numbers takes us - miraculously - into the realm of *complex number fields* such as the *Gaussian integers*.

The **quadratic formula** for solving the quadratic equation $ax^2 + bx + c = 0$ is one of the most well-known of all mathematical formulae:

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

46. Factor to solve the quadratic equation $x^2 + 4x - 12 = 0$.

47. Solve this same quadratic equation by using the quadratic formula.

48. Factor to solve the quadratic equation $3x^2 + 6x - 24 = 0$.

49. Solve this same quadratic equation by using the quadratic formula.

50. Does the quadratic equation $x^2 + 1 = 0$ have any solutions? Explain.

51. Apply the quadratic formula to this same quadratic equation, simplifying the result. Have you found a solution?

The quadratic formula typically comes with a dire warning against negative **discriminants**, $b^2 - 4ac < 0$, as square roots of negative numbers do not exist. While square roots of negative numbers do not exist as *real numbers*, to say they do not exist is badly misleading. As early as the sixteenth century mathematicians realized that solution of important, concrete mathematical questions could be obtained most easily by taking detours involving square roots of negative numbers. Mathematicians *adjoined* the **imaginary unit** $i = \sqrt{-1}$ into our number system and extended the arithmetic operations in a 'natural' way to form what is known as the **complex number field**, the set of numbers of the form $a + \sqrt{-1}b = a + ib$, where a, b are real numbers. The chapter "Existence of $\sqrt{-1}$: A Case Study" in Discovering the Art of Mathematics: Truth, Reasoning, Certainty & Proof gives a nice tour of some of the foundational aspects of the complex number field, including an illustration of how the geometry of complex multiplication gives a vivid, simple explanation of why the product of two negative numbers should be positive.

By the time of **Carl Friedrich Gauss** (German mathematician; 1777 - 1855) imaginary and complex numbers were widely accepted tools. Gauss realized that in the realm of number theory they could also serve as important tools.

52. Use the quadratic equation to solve the quadratic equation $n^2 + n + 17 = 0$ studied above and there by establish a connection between the sieve number $c = 17$ and the *class number*[5] $d = 67$.

Gauss found several other class numbers as well.

53. Mimic Investigation **52** to find a connection between an important sieve number above and the class number $d = 43$.

54. Repeat Investigation **53** for the class number $d = 19$.

55. Repeat Investigation **53** for the class number $d = 163$.

56. Repeat Investigation **53** for the class number $d = 7$.

Taking note of numbers like $\frac{1}{2} + \frac{\sqrt{7}i}{2}$ Gauss became curious about systems of numbers of the form $\mathbb{Z}/2\mathbb{Z}[\sqrt{d}i] = \left\{\frac{a}{2} + \frac{b\sqrt{d}i}{2}\right\}$. That they would be noteworthy seems almost absurd - *half-integers* combined with the *irrational* $\sqrt{d}$ and the imaginary $i = \sqrt{-1}$. What a mess. Except that he found that for *some* of these systems the equivalent of the fundamental theorem of arithmetic held - there were clearly defined prime numbers and each number had a unique factorization into primes!

57. Explain why both 2 and 4 belong to the system $\mathbb{Z}/2\mathbb{Z}[\sqrt{15}i]$.

58. Compute the product $\left(\frac{1}{2} + \frac{\sqrt{15}i}{2}\right)\left(\frac{1}{2} - \frac{\sqrt{15}i}{2}\right)$.

59. The numbers $2, \frac{1}{2} + \frac{\sqrt{15}i}{2}$ and $\frac{1}{2} - \frac{\sqrt{15}i}{2}$ are all ***irreducible*** in $\mathbb{Z}/2\mathbb{Z}[\sqrt{15}i]$, the numbers we would like to call the primes. Explain why the fundamental theorem of arithmetic does not hold in $\mathbb{Z}/2\mathbb{Z}[\sqrt{15}i]$.

60. Compute $\left(\frac{1}{2} + \frac{\sqrt{7}i}{2}\right)\left(\frac{1}{2} - \frac{\sqrt{7}i}{2}\right)$.

61. Find another way to factor the product from Investigation **60**. Try to factor it as completely as you think you can.

62. So it would appear that $\mathbb{Z}/2\mathbb{Z}[\sqrt{7}i]$ does not have unique factorization either. Deceptively, 2 is *not* prime in $\mathbb{Z}/2\mathbb{Z}[\sqrt{7}i]$. $\frac{1}{2} + \frac{\sqrt{7}i}{2}$ is one factor of 2, find the other.

In fact, $\mathbb{Z}/2\mathbb{Z}[\sqrt{7}i]$ has an equivalent of the fundamental theorem of arithmetic! This is why 7 has the special designation as a class number. Gauss and his contemporaries knew of 9 class numbers: 1, 2, 3, 7, 11, 19, 43, 67, and 163. Other than the first two, each gives rise to an important sieve number you considered above. *And* each gives rise to a number system with unique factorization into primes.

The big question is: Are there any other class numbers?

For over 100 years, nobody knew. In 1934 **Hans Arnold Heilbronn** (German mathematician; 1908 - 1975) and **Edward H. Linfoot** (British mathematician; 1905 - 1982) proved that there

[5]Strictly speaking this is not the precise way in which mathematicians use this term. But it is appropriate here given the context of our study.

was at most one more such class number, and it would be astronomically large if it existed. In 1952, after he retired, **Kurt Heegner** (German educator; 1893 - 1965), who did mathematics as a hobby, published a paper claiming to prove that Guass' original list was complete; there were no other class numbers. Apparently nobody noticed the importance of the paper!

In 1967 **Harold Stark** (American mathematician; 1939 -) and **Alan Baker** (English mathematician; 1939 -) proved this result in a mainstream journal. After this, people became aware of Heegner's proof. When they did they discovered his proof was indeed correct.[6] Later, as mathematicians studied more general class number problems, Heegner was rewarded. In 1983 **Don Zagier** (American mathematician; 1951 -) and **Benedict Gross** (American mathematician; 1950 -) announced in they had extended the breakthrough of **Dorian Goldfelds** (American mathematician; 1947 -) in 1975 to solve the more general Gauss class number problem (in a 300 page paper which included a 100 page calculation!). In this paper they named a key new type of mathematical object *Heegner points* in honor of Heegner's forgotten work.

Remarkably, these results show that the special sieve numbers you found above are the end of the road!! There are no sieve numbers c which perform in the way those found above do. There is no run of prime outputs any longer than those you already found for quadratic functions of the form we were considering!

Might different types of functions find more primes? *Single variable polynomials* like the quadratics above will not work to generate primes indefinitely - **Christian Goldbach** (German mathematician; 1690 - 1764) proved this long ago. In contrast, in proving *Hilbert's 10th problem* **Martin Davis** (American mathematician; 1928 -), **Yuri Matiyasevich** (Russian mathematician; 1947 -), **Hilary Putnam** (American philosopher and mathematician; 1926 -) and **Julia Robinson** (American mathematician; 1919 - 1985) guaranteed there was a multivariable polynomial that would generate all of the primes. They proved this even though they did could not explicitly find such a polynomial! In 1976 **James P. Jones** (Canadian mathematician; -), **Daihachiro Sato** (Japanese mathematician; 1932 - 2008), **Hideo Wada** (Japanese mathematician; -), and **Douglas Wiens** (Canadian statistician; -)[7] actually found such a polynomial explicitly:

$$\begin{aligned}(k+2)(1-&[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-[2n+p+q+z-e]^2\\&-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-0^2]^2\\&-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2\\&-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2+[n+l+v-y]^2\\&-[(a^2-1)t^2+1-m^2]^2-[ai+k+1+l+i]^2\\&-[p+l(a-n-1)+b(2an+2an+2a-n^2-2n-2)-m]^2\\&-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2\\&-[z+pl(a-p-p^2-1)-pm]^2)\end{aligned}$$

When the variables $a, b, c, \ldots, x, y, z$ - yes, one for each letter of the English alphabet - take on positive values then the set of positive outputs is precisely the set of prime numbers. Unfortunately, this function is really only of theoretical interest. For the output to be positive each term in large brackets must simultaneously be zero as they are nonnegative and subtracted from 1. Hence, as

[6] See Mathematics: The New Golden Age by Keith Devlin, pp. 79-80.

[7] "Diophantine representation of the set of prime numbers," *American Mathematical Monthly*, Vol. 83, No. 6, June-July, 1976, pp. 449-64.

Underwood Dudley (American mathematician; 1937 -) reminds us, "the first positive value might not appear until considerably after the end of the universe, and even then it might be something trivial, like 17."[8]

5.6 The Riemann Hypothesis

> Prime numbers are a lot like musical chords... A chord is a combination of notes played simultaneously. Each note is a particular frequency of sound created by a process of resonance in a physical system. Put together, notes can make a wide variety of music. In number theory, zeroes of the zeta function are the notes, primes numbers are the chords, and theorems [like the Riemann hypothesis] are the symphonies.[9]
>
> **Barry Cipra** (American mathematical journalist; -)

> "Loosely speaking, the Riemann hypothesis states that the primes have music in them", [Michael] Berry says. But Berry is looking for more than a musical analogy - he hopes to find the actual instrument behind the *zeta function* - a mathematical drum whose natural frequencies line up with the zeroes of the zeta function. The answer, he thinks, lies in quantum mechanics. "There are vibrations in classical physics too" he notes, "but QM is a richer, more varied source of vibrating systems than any classical oscillators that we know of."[10]
>
> **Barry Cipra** (American mathematical journalist; -)

For two millennia humanity has tried to unlock the secrets of the prime numbers. The Riemann hypothesis is one of the keys to unlocking these secrets. It suggests deep relationships with music and with physics. Yet over 150 years since it was stated by Riemann, it stands as one of the major challenges to mathematicians. Above we studied Gauss' Class Number Problem above because you could actually explore mathematics related to this great problem. Here we give a general description of Riemann's hypothesis.

At the heart of the Riemann Hypothesis is a function called the *zeta-function*. **Leonard Euler** (Swiss mathematician; 1707 - 1783) discovered the following remarkable, and very infinite, identity:

$$\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\ldots=\left(\frac{1}{1-(\frac{1}{2})^s}\right)\times\left(\frac{1}{1-(\frac{1}{3})^s}\right)\times\left(\frac{1}{1-(\frac{1}{5})^s}\right)\times\left(\frac{1}{1-(\frac{1}{7})^s}\right)\times\cdots,$$

which holds for all real numbers $s>1$.

63. Write out several more terms in the *infinite series* on the left.

64. What is the pattern in the numerators of the terms on the left?

65. Write out several more terms in the *infinite product* on the right.

66. What is the pattern of the fractions in the numerators of the terms on the right?

[8] "Formulas for Primes," *Mathematics Magazine*, Vol. 56, No. 1, Jan. 1983, pp. 17-22

[9] From "A Prime Case of Chaos", in What's Happening in the Mathematical Sciences:1998-99, vol. 4, American Mathematical Society, p. 7.

[10] From "A Prime Case of Chaos" in What's Happening in the Mathematical Sciences: 1998-99, Vol. 4, American Mathematical Society, p. 7.

In his landmark 1859 paper Riemann *continued* this function to an analytic function on the entire complex plane except for a single *pole* at $s = 1$. I.e. this function, now known as the **Riemann zeta function**, isn't just a function for real numbers $s > 1$, but it is a well-behaved function for all complex numbers $s \neq 1$. Amazingly, through this function, our search for an understanding of the behavior of the primes manifests itself as a search for the location of the zeroes of a complex valued function of a complex variable.

The **Riemann Hypothesis** posits that all *nontrivial* zeroes of this function lie along the line $\frac{1}{2}+t\sqrt{-1}$. Through December, 2005 when it went offline, ZetaGrid was a ***distributed computing*** site where computer users could donate their idle CPU time to search for zeroes of the zeta function. The first 900 billion zeroes they found are located on the proposed line. We don't know about the rest. As mathematicians have struggled over the decades with this problem they have studied related objects and problems. This has lead them to so-called ***L-functions*** which are kin to the Riemann zeta-function. It is hoped that the study of such functions will shed light on the Riemann Hypothesis as well as many other problems.

So where does the Class Number Problem fit into all of this? In his prize-winning article on the Riemann Hypothesis[11], **J. Brian Conrey** (Director of the American Institute of Mathematics; -), tells us:

> There is a growing body of evidence that there is a conspiracy among L-functions - a conspiracy which is preventing us from solving RH! ... The history of Gauss' [Class Number Problem] is extremely interesting; it has many twists and turns and is not yet finished - we seem to be players in the middle of a mystery novel... Much effort has gone toward find[ing] an effective solution to Gauss' problem. However, the L-function conspiracy blocks every attempt exactly at the point where success appears to be in sight. We begin to suspect that the battle for RH will not be won without getting to the bottom of this conspiracy.

5.7 Another $ 1Million Problem

Remarkably, our journey through the lower slopes of Gauss' Class Number problem not only connects to the steepest trails through the uncharted mathematical territory whose peak represents the conquest of the Riemann hypothesis, it has also taken us to trailheads to another of $1 Million Millennium Prize Problem, the ***Birch and Swinnerton-Dyer Conjecture***.

While we tried to give some sense of the exact nature of the Riemann hypothesis - the location of zeroes of an analytically continued complex function of a complex variable - the challenge to describe the Birch and Swinnerton-Dyer conjecture is even greater. For the purposes of explorers using this book as a guide of discovery this is not essential. We can tell some of the story to help elucidate the nature of contemporary mathematics.

As noted, the trailheads to the Riemann hypothesis [RH] and Birch and Swinnerton-Dyer conjecture [BSDC] are close together, both connected to the Gauss' Class Number Problem. We don't know where they will go. But from how far we can see, RH proceeds ahead analytically. In contrast, BSDC moves much more algebraically along the slopes we can seen. RH is an old,

[11] "The Riemann Hypothesis," *Notices of the American Mathematical Society*, March 2003, pp. 341 - 353; winner of the 2008 Conant Prize.

classical problem, while BSDC resulted from joint work by Bryan Birch and Peter Swinnerton-Dyer in the 1960's. RH involves the distribution of the primes and needed data for its genesis. Yet its premise is global in nature. In contrast, BSDC relied heavily on extensive bodies of research carried out with the help of powerful computers into the nature of very specific mathematical objects. I.e. it arose from much more local considerations.

Despite these differences, perhaps these trails converge much higher up the slopes as both are fundamental to the study of L-functions.[12]

For more on these two topics, see The Millennium Problems: The Seven Greatest Unsolved Mathematical Puzzles by Keith Devlin.

[12] "L-series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss," Notices of the American Mathematical Society, Vol. 31, No. 7, November 1984, pp. 739-43.

Chapter 6

Partitions

> "What's one and one and one and one and one and one and one and one and one and one?" "I don't know," said Alice. "I lost count." "She can't do addition," said the Red Queen.
>
> **Lewis Carroll** (British Author and Mathematician; 1832 - 1898)

> Read Euler, he is our master in all.
>
> **P.S. Laplace** (French Mathematician; 1749 - 1827)

> The trouble with the integers is that we have examined only the very small ones. Maybe all the exciting stuff happens at really big numbers, ones we can't even begin to think about in any very definite way. Our brains have evolved to get us out of the rain, find where the berries are, and keep us from getting killed. Our brains did not evolve to help us grasp really large numbers or to look at things in a hundred thousand dimensions.
>
> **Ronald L. Graham** (American Mathematician; 1935 -)

6.1 The Births of Modern Number Theory

Throughout this text the work of many mathematicians in number theory is mentioned. In every field of mathematics each new generation adds a new story to the edifice of mathematics, and each new generation has many builders. Yet in number theory the large cast of players is overshadowed by just three mathematicians - Pierre de Fermat, Leonhard Euler, and Carl Friedrich Gauss - whose work is chiefly responsible for the formative history of number theory. As **André Weil** (French Mathematicain; 1906 - 1998), one of the twentieth century's foremost number theorists, notes in his definitive work on the history of number theory:

> One might... try to record the date of birth of the modern theory of numbers; like the god Bacchus, however, it seems to have been twice-born. Its first birth must have occurred at some point between 1621 and 1636, probably closer to the later date... when Fermat acquired a copy of this book [a translation of the Greek Diophantus' Arithmetica]... As to its rebirth, we can pinpoint it quite accurately. On the first of December 1729, Goldbach asked Euler for his views about Fermat's statement that all integers $2^{2^n}+1$ are primes... After that day, Euler never lost sight of this topic and of number theory in general... Number theory reached full maturity [with Gauss].[1]

[1] Number Theory: An Approach through History from Hammurapi to Legendre, Birkhauser Boston, 1984.

We have either already seen, or will soon see, the mathematics that initiated these key moments in the history of number theory.

6.2 The Development of Mathematics Illustrated by Number Theory

The births of number theory at the hands of Fermat, then Euler, and its later passage into adulthood through the work of Gauss provide an illustration that typifies mathematical growth and development.

Mathematics is generally presented in schools in its final, polished form. A typical topic is hundreds of years old, and generations of mathematicians and teachers have organized and reorganized it into a highly logical, streamlined form. It seems certain and lifeless. Long ago its validity was proven and its connections to other areas were found. It is rare that students are provided the opportunity to explore the examples, problems, and issues from which an area of mathematics germinated.

Yet mathematics almost always begins with examples, problems, compelling issues, and uncertainty. A great deal of work is done before the patterns, insights, and conjectures of one generation are replaced by the proven theories of another. It is generally a generation after that who assembles the work into a coherent whole.

In number theory, it was Fermat that found the patterns, had the insights, and made the conjectures that would fuel number theory for many generations. He provided few if any proofs, writing his ideas in the margins of Diophantus' Arithmetica. It was Euler, a century later, who provided proofs and generalizations of many of Fermat's most important observations. A generation later, it was Gauss that made the work of Euler a coherent whole.

We spoke of Gauss in the previous topic and will return to him in the next, investigating some of the mathematics that made his Disquisitiones Arithmeticae such a landmark achievement. Here we will concentrate on a few of the many remarkable connections between Euler and Fermat.

6.3 Connections Between Fermat and Euler

6.3.1 Fermat Primes

We investigated Fermat primes, prime numbers of the form $2^{2^n}+1$ in Chapter 4. Given Fermat's renown, nobody questioned his claim that all of these numbers were prime. It was not until Euler that we find someone with enough mathematical prowess to disprove Fermat. Euler's proof that the "Fermat prime" $2^{2^5}+1$ is not prime, which you recreated in investigations Investigation **33** - Investigation **35** in Chapter 4, is one of the great mathematical discoveries.[2] At this time (late 2013) we know that of the first thirty-three Fermat numbers only the first five are primes.

[2]In Journey Through Genius: The Great Theorems of Mathematics, [Dun1], Euler scholar **William Dunham** (American mathematician; 1947 -) gives an accessible treatment of Euler's discovery - one that he includes as one of his descriptions of mathematics' thirteen great theorems.

6.3.2 The (Mathematical) Key to Modern Encryption

In Section **??** of Chapter 4, you studied congruences of the form $a^{n-1} \pmod{n}$. The desired result in Investigation **65** in that section is that

$$a^{n-1} \equiv 1 \pmod{n}$$

whenever n is prime and a is not a multiple of n. This result is known as **Fermat's Little Theorem**, to distinguish it from his famous "Last Theorem" which you will see in the final chapter of this book. While the result was known to ancient mathematicians (e.g. the 5th century B.C. Chinese; see [Flan, pp. 134-7]), it was rediscovered and reintroduced into mathematics by Fermat in a letter to **Bernard Frénicle de Bessy** (French Mathematician; 1605 - 1675) on 18 October, 1640. Fermat was characteristically glib in providing justification. He told Frénicle, "I would send you the demonstration, if I did not fear its being too long." ([Bur, pp. 88-9])

It was Euler who supplies the first proof of Fermat's Little Theorem, almost 100 years later, in 1736. And Euler did Fermat one better this time. Not only did he prove Fermat's Little Theorem, he showed that it could be generalized. (See the Further Investigations in Section 4.12.2 of Chapter 4 for investigations that motivate this result.) That is, Fermat's Little Theorem is a special case of a more general pattern which is known by the name of its discoverer. What we refer to as **Euler's Theorem** is the result that:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

whenever a and n have no common factors. Here ϕ is the *Euler phi-function* which will have the value $n-1$ whenever n is prime, yielding Fermat's Little Theorem in that case.[3]

As shown in Section 4.10 in Chapter 4, Fermat's Little Theorem, and its generalization to Euler's Theorem, are of no little significance. These results are the fundamental mathematical results upon which most modern encryption methods are based!

6.3.3 Primes and Sums of Two Squares

After the even prime number 2, all primes are odd. If you check, you will easily see that any odd number can be written in the form $2k+1$, where k is a whole number. We don't learn much about primes writing the odd primes in this way. However, any odd number can also be written either as $4k+1$ or $4k-1$, where k is a whole number. Fermat discovered that the $4k+1$ **primes** behave quite differently than the $4k-1$ **primes**.

Here you will rediscover that pattern which Fermat discovered (on Christmas day in 1640[4]) and Euler first proved.

1. Prove that every number which is of the form $4k-1$ or $4k+1$ is odd.

2. Prove that every odd number can be written in the form $4k-1$ or $4k+1$ where k is a non-negative integer.

3. Show that 29 is a prime of the form $4k+1$.

[3] In Chapter 3 we used the Greek letter phi to denote the Golden Ratio. This same letter is being used here but with a different meaning. It will always be clear from context which is being denoted. For one thing, the Golden Ratio is a constant while phi represents a function in the current context.

[4] [Bur, p. 242].

4. 29 can be written as the sum of two squares: $29 = 2^2 + 5^2$. Can 29 be written as the sum of two different squares? Prove your result.
5. Show that 37 is a prime of the form $4k + 1$ and determine exactly how many ways 37 can be expressed as the sum of two squares, proving your result.
6. Choose another prime of the form $4k + 1$ and determine exactly how many ways it can be expressed as the sum of two squares, proving your result.
7. Repeat Investigation **6** for another prime of the form $4k + 1$.
8. What pattern do you notice for the $4k + 1$ primes?
9. Show that 23 is a prime of the form $4k - 1$.
10. Can 23 be written as the sum of two squares? Prove your result.
11. Show that 31 is a prime of the form $4k - 1$ and determine exactly how many ways 31 can be expressed as the sum of two squares, proving your result.
12. Choose another prime of the form $4k - 1$ and determine exactly how many ways it can be expressed as the sum of two squares, proving your result.
13. Repeat Investigation **12** for another prime of the form $4k - 1$.
14. What pattern do you notice for the $4k - 1$ primes?

6.3.4 Sums of Squares

Fermat and Euler were interested in what they could learn about expressing numbers as sums of squares. As your investigation of the $4k - 1$ primes show, more than two squares will sometimes have to be used. For example, the $4k - 1$ prime 31 requires four squares: $5^2 + 2^2 + 1^2 + 1^2$. In Section 7.7 in Chapter 7, you will (re-)discover that any number can be expressed as the sum of not-many-more than two squares. Fermat claimed to have a proof of this result, but his proof was never found. (As we shall see, this is a recurring theme for Fermat.) Euler set to work on this problem as early as 1730. He worked on it for *40 years* with partial success, proving many partial results, before Lagrange used many of Euler's results to give a complete proof. Compelled to find his own proof, three years later, after working on the problem for *43 years*, Euler found a simpler, original proof. [Dud, pp. 149-50]

You might ask, "What is so special about squares? Why not use other powers?" This is a natural question, known as *Waring's Problem*, and it is the foci of Chapter 7 and Chapter **??**.

6.3.5 Fermat's Last Theorem

Fermat's Last Theorem is one of the two main foci of Chapter 8. As mentioned in this book's Introduction, the theorem is the most famous and long-standing problem in all of mathematics. It concerns positive integer solutions to the equation $a^n + b^n = c^n$ for each of the exponents $n = 2, 3, 4, 5, \ldots$ The first documented progress was due to Fermat, who proved that there were no solutions when $n = 4$. The next documented progress was due to Euler who proved that there were no solutions when $n = 3$. These two results provided hope to mathematicians' quests for this holy grail for more than three centuries.

6.4 Partitions

What we are doing in number theory is building theoretical telescopes.

Ken Ono (American mathematician; -)

Primality and factorization both arise in the context of multiplication. Since the integers also have addition as an operation[5], it is natural to wonder whether we can find patterns when integers are represented as sums of other integers. The section above on sums of squares is one example.

Even simpler than writing positive integers as sums of squares is to write them as sums of other positive integers. For example, we can write

$$2 = 2 \text{ and } 2 = 1 + 1.$$

In writing 2 this way, unlike writing it with multiplication and primes, where there is only one way to write it, there is no uniqueness. Can we find a pattern to this non-uniqueness?

Decompositions of a positive integer into sums of positive integers are known as **partitions**. In counting partitions, the two partitions $2 + 1$ and $1 + 2$ of 3 are considered to be identical; order does not matter. Clearly, the partitions of two given above are the only ones, and 1 only has one partition, $1 = 1$. How many partitions of 3 are there? 4? Is there a pattern? You will investigate this below.

The first detailed study of partitions was taken up by Euler in response to queries from the mathematician **Philippe Naudé** (; 1684 - 1745). Euler had great success. While many of Euler's results relied on *infinite series*, and would take us too far afield, the investigations in this and the next topic will use partitions as a vehicle to explore rich, accessible, and important contemporary mathematical questions.

6.4.1 Enumerating Partitions

15. Find all the partitions of 3.

16. Use your answer to Investigation **15** to complete the following table:

Interger; n	#Partitions; $p(n)$
1	1
2	2
3	

17. Based on the table in Investigation **16**, how many partitions of 4 do you expect?

18. What kind of reasoning are you using in your answer to Investigation **17**?

19. Find all the partitions of 4.

[5]Sets that have one operation which satisfies special properties are called *groups*, a critically important class of mathematical objects. More special are those sets, like the integers, which have two operations, such as addition and multiplication, which satisfy special properties and are called *rings*. One learns about such objects when one studies *modern abstract algebra* (not to be confused with high school or college algebra, although these fields are related) in which **Evariste Galois** (French Mathematician; 1811 - 1832), a famous mathematical prodigy who was killed in a duel at the age of 20, and **Niels Henrik Abel** (Norwegian Mathematician; 1802 - 1829), another prodigy who died from tuberculosis at age 27, were critical founding figures.

20. Does your result in Investigation **19** agree with your conjecture in Investigation **17**? What does this tell you about the reasoning that you used to make your conjecture?

21. Use your answer to Investigation **19** to complete the following table:

Interger; n	#Partitions; $p(n)$
1	1
2	2
3	
4	

22. Find a pattern in the table in Investigation **21**, and use it to predict how many partitions of 5 you expect. What kind of reasoning are you using to make this prediction?

23. Find all the partitions of 5.

24. Does your result in Investigation **23** agree with your conjecture in Investigation **22**? What does this tell you about the reasoning that you used to make your conjecture?

25. Use your answer to Investigation **23** to complete the following table:

Interger; n	#Partitions; $p(n)$
1	1
2	2
3	
4	
5	

26. Find a pattern in the table in Investigation **25**, and use it to predict how many partitions of 6 you expect. What kind of reasoning are you using to make this prediction?

6.4.2 Counting Strategies

As n becomes larger and larger, the number of partitions of n increases quickly. To find all the partitions successfully, it is important to have a strategy to insure that none are missed.

27. Find all of the partitions of 6, describing your *specific* strategy to insure that you have found all of the partitions.

28. Does your result in Investigation **27** agree with your conjecture in Investigation **26**? What does this tell you about the reasoning that you used to make your conjecture?

29. Use your answer in Investigation **27** to complete the following table:

Interger; n	#Partitions; $p(n)$
1	1
2	2
3	
4	
5	
6	

30. Find a pattern in the table in Investigation **29**, and use it to predict how many partitions of 7 you expect. What kind of reasoning are you using to make this prediction?

31. Find all of the partitions of 7, justifying how you know you have found all of the partitions.

32. Does your result in Investigation **31** agree with your conjecture in Investigation **30**? What does this tell you about the reasoning that you used to make your conjecture?

33. Use your answer to 17) to complete the following table:

Interger; n	#Partitions; $p(n)$
1	1
2	2
3	
4	
5	
6	
7	

34. Find a pattern in the table in Investigation **33**, and use it to predict how many partitions of 8 you expect. What kind of reasoning are you using to make this prediction?

35. Find all the partitions of 8, justifying how you know you have found all of the partitions.

36. Does your result in Investigation **35** agree with your conjecture in Investigation **34**? What does this tell you about the reasoning that you used to make your conjecture?

6.4.3 Patterns in the Partition Function

A list of the number of partitions of the first forty-five integers, excluding those you have found above, appears below. None of your "patterns" really continue. There is no "simple" pattern. It was not until 1934 that an explicit formula for $p(n)$ was found – two centuries after partitions were first significantly considered.[6]

Fill in the missing partitions, being sure to check your results with others in your class.

[6]This discovery was made by **Hans Rademacher** (German Mathematician; 1892 - 1969). This formula is complex, providing, as a consequence, the "simple *asymptotic*" result that as the integer n gets closer and closer to infinity the number of partitions of n gets closer and closer to $\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{4n\sqrt{3}}$, a result that had been established by Hardy and Ramanujan in 1918. Given the availability of efficient computer algebra systems, it is somewhat easier to generate the number of partitions using the *generating function* $\prod_{n=1}^{\infty}\frac{1}{1-x^n} = \left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^2}\right)\left(\frac{1}{1-x^3}\right)\cdots$, which is an infinite product (!!) discovered by Euler. See Additional Investigations for more details.

Interger; n	#Partitions; $p(n)$	n	$p(n)$	n	$p(n)$
1	1	16	231	31	6,842
2	2	17	297	32	8,349
3		18	385	33	10,143
4		19	490	34	12,310
5		20	627	35	14,883
6		21	792	36	17,977
7		22	1,002	37	21,637
8		23	1,255	38	26,015
9	30	24	1,575	39	31,185
10	42	25	1,958	40	37,338
11	56	26	2,436	41	44,583
12	77	27	3,010	42	53,174
13	101	28	3,718	43	63,261
14	135	29	4.565	44	75,175
15	176	30	5.604	45	89,134

37. In the table, find all integers whose number of partitions is a multiple of 5.

38. If you delete some of the numbers from your answer to Investigation **37** the remaining numbers fall in a regular pattern, called a ***partition congruence mod 5***. Describe it precisely.

39. Do you think that the pattern in Investigation **38** continues forever? Explain.

40. Following the example of Investigation **37** and Investigation **38**, find and precisely describe a partition congruence (mod 7).

41. Following the example of Investigation **37**, Investigation **38**, and Investigation **40**, find and precisely describe a partition congruence (mod 11).

Ramanujan believed that the only partition congruences were those found above or those formed by products of 5, 7, and 11; for example, $1925 = 5^2 \times 7 \times 11$ partition congruences. In the decades following his death, mathematicians found a few more partition congruences, but believed that they were isolated, explicable examples. Said mathematician **George E. Andrews** (American Mathematician; 1938 -), one of the foremost international experts on questions in this area of number theory, "It was really believed that there would probably never be any new major discoveries regarding partition congruences."[7]

6.4.4 Amazing New Discoveries

While working through awkward, non-traditional passages in Ramanujan's notebooks in 1999-2000, **Ken Ono** (American mathematician; -) made a remarkable breakthrough. Inspired by Ramanujan's work he discovered a way to prove that there are partition congruences for every prime number greater than 3! That is, in addition to $5, 7$, and 11 partition congruences, there are $13, 17, 19, 23, \ldots$ partition congruences as well! Moreover, he proved this result while explicitly finding only *one* new partition congruence.

[7] Quoted in [Pet1].

42. In his research Ken Ono found only one new partition congruence. Yet he was still able to prove deductively that there are infinitely many partition congruences. How do you think somebody can prove, deductively, that something exists, or even infinitely many of them exist, without discovering a procedure that explicitly identifies them?

Subsequently, a Penn State undergraduate student, **Rhiannon L. Weaver** (; -), found an algorithm, or procedure, for generating new, previously undiscovered partition congruences of the type guaranteed by Ono's work. She found more than 70,000 new congruences, and her methods can be programmed to generate additional partition congruences.

43. Is it amazing that an undergraduate made such progress on this problem? Explain.

Chapter 7

Power Partitions

> The principal agent is the object itself and not the instruction given by the teacher. It is the child who uses the objects; it is the child who is active, and not the teacher.
>
> **Maria Montessori** (Italian Physician and Educator; 1870 - 1952)

> No thought, no idea, can possibly be conveyed as an idea from one person to another. When it is told it is to the one to whom it is told another fact, not an idea... Only by wrestling with the conditions of the problem at first hand, seeking and finding his own way out, does [she]he think.
>
> **John Dewey** (American philosopher, psychologist and educator; 1859 - 1952)

7.1 Another Story about Gauss

Some of the remarkable accomplishments of the prodigy Gauss have already been told. We start here with a story of his mathematical precociousness.

It is sometimes reported that as a child of three Gauss corrected errors in his father's payroll calculations.[1] More often repeated, and more widely accepted, folklore about Gauss involves busywork punishment Gauss's elementary school teacher assigned to him. The problem was to determine the *sum* of the *series*

$$1 + 2 + 3 + \cdots + 98 + 99 + 100.$$

Without doing any calculations on his small slate, Gauss wrote the correct answer almost immediately: 5050. How'd he do it?

7.2 Mathematics Manipulatives

Gauss noticed a pattern that can be nicely illustrated by *mathematical manipulatives* - concrete, physical objects that are used for hands-on explorations of mathematics and are widely used in contemporary elementary mathematics classrooms.

[1] See, e.g., [Bur, p. 510].

The manipulatives pictured here are small cubes of a uniform size which can be snapped together; they are sold under the names **Multi-link Cubes®** and **Unifix Cubes®**. Try to find some of these manipulatives, or something akin to them, so you can explore using them as you read.

So that we can provide illustrations, we begin with a smaller version of Gauss' problem – finding the sum of the series

$$1 + 2 + \ldots + 7 + 8.$$

We can represent each of the *summands* concretely using the manipulative cubes, as shown on the left image in Figure 7.1.

Figure 7.1: The numbers 1 - 8 concretely as Multi-link Cubes®.

Snapping our cubes together, the sum of these numbers is simply the number of cubes in the "staircase" on the left in Figure 7.2. By itself this does not seem like much help but if you notice two of these staircases fit together perfectly into one rectangle, as shown on the right in Figure 7.2, you have essentially solved the problem solved.

1. Determine the number of cubes that make up the rectangle formed by the joined staircases in Figure 7.2.

2. Determine the sum $1 + 2 + \ldots 7 + 8$.

Finding the sum of the first eight numbers is not difficult. What is important is the idea or strategy on which it is based. This idea can be applied to many variations of this problem, including Gauss's problem.

3. Use this strategy to show that Gauss was correct: $1 + 2 + 3 + ... + 98 + 99 + 100 = 5050$.

4. What is the sum of the *series* $1 + 2 + \ldots + 999 + 1000$?

5. What is the sum of the series $1 + 2 + \ldots + 100,000 + 100,001$?

Figure 7.2: The $1+2+\ldots+7+8$ staircases and a pair of $1+2+\ldots+7+8$ staircases joined.

6. Can you *generalize* these results, explaining how you can determine the sum of any series of the form

$$1+2+3+\ldots+(n-2)+(n-1)+n?$$

Either do so or explain specifically what limitations the method has.

In fact, this method can be generalized to find the sum of any *arithmetic series*. This general method should be fairly clear after you determine how to adapt Gauss's method to the following examples:

7. Adapt Gauss's method to determine the sum of the series $1+4+7+...+34+37+40$.

8. Similarly, determine the sum of the series $1+5+9+...+93+97+101$.

9. Similarly, determine the sum of the series $5+8+11+...+21+24+27$.

10. What are the important aspects of each of the series that have been considered here that enable this method to be adapted to determine the sum of the series? Explain.

Because you have a pile of cubes in front of you, it is an opportune time for a first investigation of the problem that will occupy much of the rest of this book.

11. Build a large, solid cube from the manipulative cubes ("cubies"). Identify how big it is and how many cubies it is made up of. Now take it apart. Can you build two smaller, solid cubes using exactly the same number of cubies, in total, that were used to make up the original cube? If not, how close can you get?

12. Starting from the same larger cube, can you build *three* smaller, solid cubes using exactly the same number of cubies, in total, that were used to make up the original cube?

13. Can you build *four* smaller, solid cubes using exactly the same number of cubies, in total, that were used to make up the original cube?

14. Build a different sized starting cube and repeat Investigation **11** - Investigation **13**.

7.3 Proofs Without Words

Many people's experience with mathematical proof is primarily through their high-school geometry course, where the dominant proof language is the revered *two-column proof*. Seen in this light, one might agree with **Sir Arthur Eddington** (British Astrophysicis; 1882 - 1944) who said:

> Proof is an idol before which the mathematician tortures [her]himself.

One might go even further and agree with **Paul Lockhart** (American Mathematician and Teacher; -) whose chapter "High School Geometry: Instrument of the Devil" in A Mathematician's Lament describes as "treachery" the way proof is considered in high school geometry. He says:

> Posing as the arena in which students will finally get to engage in true mathematical reasoning, this virus [high school geometry] attacks mathematics at its hear, destroying the very essence of creative retinal argument, poisoning the students' enjoyment of this fascinating and beautiful subject, and permanently disabling them from thinking about math in a natural and intuitive way.[2]

This quite unfortunate as proof is actually an essential part of what it means to make sense of mathematics. A more appropriate view of proof is that of **Andrew Gleason** (American Mathematician; 1921 - 2008) who regularly said:

> Proofs really aren't there to convince you that something is true – they're there to show you why it is true,

Another nice view of proofs is from **Gian-Carlo Rota** (American Mathematician; 1932 - 1999) who said:

> Proof is beautiful when it gives away the secret of the theorem, when it leads us to perceive the actual and not the logical inevitability of the statement that is proved.

A particularly accessible style of mathematical proof is something mathematicians call *Proofs Without Words*. The "staircase proofs" from the previous section were proofs without words. Another famous example of a proof without words arises from the following problem:
Problem What do you get when you add up the first few odd numbers?

One way to begin to investigate this problem is to collect some data:

$$\begin{aligned} 1 &= 1 \\ 1+3 &= 4 \\ 1+3+5 &= 9 \\ 1+3+5+7 &= 16. \end{aligned}$$

[2] A Mathematician's Lament, p. 67.

15. Do you notice a pattern in this data?

16. Check the next few examples to see if your pattern correctly continues. Does it?

You may now feel comfortable *conjecturing* that this pattern you have discovered will always hold. But what is needed is a proof.

One can make staircases as in the previous section. But there is a much more direct, insightful strategy.

17. Using your manipulative cubies (or square manipulative tiles or even graph paper whose squares you can color) choose one cubie of one color and three cubies of another color. Can you arrange them into an appropriate shape so you clearly see 1, 3 and the sum 4?

18. Now choose one cubie of one color, three of another color and five of another color. Arrange them into an appropriate shape so you clearly see 1, 3, 5, and the sum 9.

19. Explain how this approach can be continued. Clearly explain why each additional added term will be the correct size and why the resulting shape will always be a square.

20. Can you really "see" this proof? Do you understand why we would call such a thing a proof without words?

Certainly, this proof lives up to the ideal of proof described by Gleason and Rota. And Lockhart calls this proof a "divine revelation." He says, "I feel that this structure was 'out there' all along; I just couldn't see it. And now I can! This is really what keeps me in the math game – the chance that I might glimpse some kind of secret underlying truth, some sort of message from the gods."[3]

Maria Montessori would appreciate this use of mathematical manipulatives. But they should not just be considered a learning tool for the young. "Proof without Words" is a semi-regular column in some widely read mathematics journals, and two full length books containing exemplary examples of these proofs have been published.[4]

And proofs without words arise in research level mathematics as well. We can illustrate this using partitions.

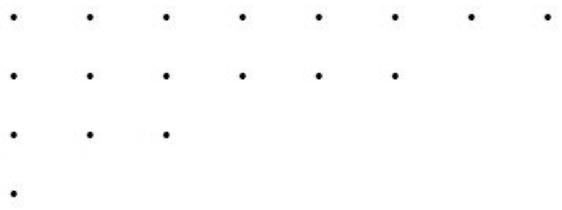


Figure 7.3: Two partitions of 18.

[3] A Mathematician's Lament, p. 114.

[4] The journals are *American Mathematical Monthly*, *Mathematics Magazine*, and *The College Mathematics Journal*. The books are Proofs without Words and Proofs without Words II both edited by Roger B. Nelsen. All are published by the Mathematical Association of America.

Figure 7.3 is made up of 18 dots. Count off the rows and you get one partition of $18 : 18 = 8 + 6+3+1$. Count off the columns and you get a different partition of $18 : 18 = 4+3+3+2+2+2+1+1$. These two partitions are called *conjugate partitions*. Figures such as this provide the critical insight in proving the *Rogers-Ramanujan Partition Identity*[5] which is the intimidating identity

$$\sum_{i=0}^{\infty} \frac{x^{i^2}}{(1-x)(1-x^2)\cdots(1-x^i)} = \prod_{j=0}^{\infty} \frac{1}{(1-x^{5j+1})(1-x^{5j+4})}$$

which involves an infinite series on the left and an infinite product on the right.

In Hardy and Wright's classic text [HaWr] diagrams such as that in Figure 7.4 are commonplace in *combinatorial proofs* about partitions. And one of the more important results in the theory of partitions is *Euler's pentagonal number theorem* which bears no small relationship to the pattern in Figure 7.5.

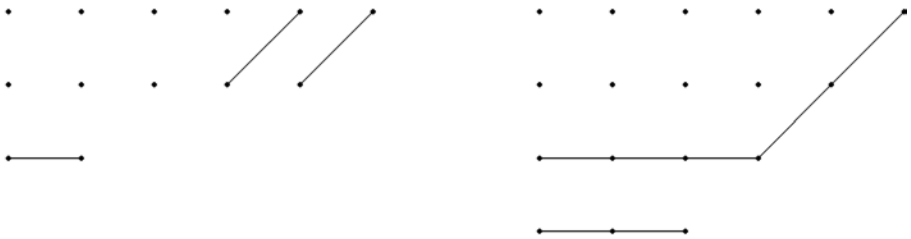


Figure 7.4: Partition diagrams.

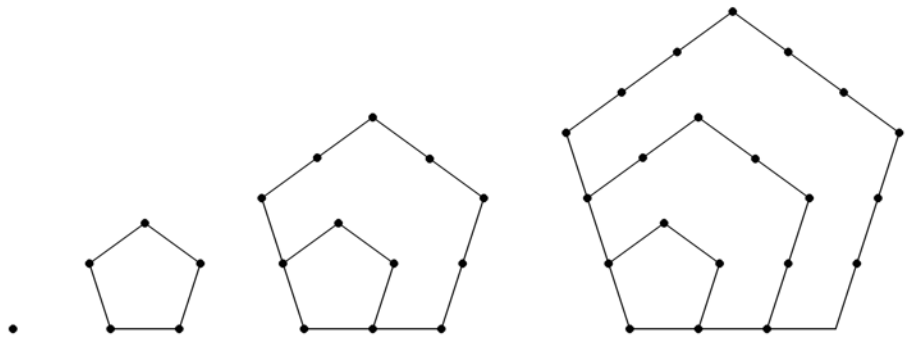


Figure 7.5: Pentagonal numbers: $1, 5, 12, 22, \ldots$

Mathematicians, it seems, would be at home in a progressive, elementary school mathematics classroom together with young children exploring all sorts of patterns via Multi-link Cubes®.

[5]See pp. 736-7 of "Partition Identities – from Euler to the Present", H.L. Alder, *American Mathematical Monthly*, vol. 76, no. 7, Aug.-Sept. 1969, pp. 733-46.

7.4 Interesting Numbers

Earlier we read about the great **G.H. Hardy** (English mathematician ; -) and the prodigy **Srinivasa Ramanujan** (Indian mathematician; 1887 - 1920). It was Hardy that brought Ramanujan to Oxford to share in his remarkable mathematical abilities. Hardy tells a touching and oft-retold story of his visit to see Ramanujan in the hospital before his untimely death:

> "The cab I rode to the hospital had a particularly dull number: 1729." "No Hardy," Ramanujan replied immediately, "it's a very interesting number. It is the smallest number that is expressible as the sum of two cubes in two different ways."

21. Make a table of the first dozen cubes.

22. Use it to write the number 1729 as the sum of two cubes.

23. Use it to write the number 1729 as the sum of two cubes different from those used in Investigation **22**.

24. Are your solutions to Investigation **22** and Investigation **23** partitions? If so, is there a word that would describe precisely what type of partitions they are?

25. How remarkable is it that Ramanujan knew this about the number 1729? What does it tell you about his fluency with numbers?

7.5 Square Partitions

In the story above about 1729 Ramanujan was concerned with both the *number* of cubes used to provide a sum of 1729 and the *number* of ways it could be done. Instead of considering both issues at once, let us begin by considering the number of ways a given number can be partitioned into powers.

26. The numbers $1 = 1^2, 4 = 2^2, 9 = 3^2, \ldots$ are called *perfect squares*. Define the term perfect square.

27. Make a table of the first 20 perfect squares.

We called $6 = 4 + 1 + 1$ a partition of the number 6. Since each of $4, 1$, and 1 are squares we can also write 6 as $6 = 2^2 + 1^2 + 1^2$. We will call partitions of this form **square partitions**.

28. Find and record all of the square partitions of each of the numbers $1 - 8$.

29. Use your answers to Investigation **7.5** to complete the following table:

Integer, n	# Square Partitions, $s(n)$
1	1
2	1
3	1
4	
5	
6	
7	
8	

30. Find a pattern in the number of square partitions and use it to predict the number of square partitions for the numbers 9 - 12.

31. Find all square partitions of 9.

32. Does your result in Investigation **31** agree with your conjecture in Investigation **30**? What does this tell you about the type of reasoning you used to make this prediction?

33. If you continued to look for patterns in the number of square partitions, how successful do you think your efforts might be in? How does this compare/contrast with your success in finding patterns in the number of partitions in the last chapter?

7.6 Cubical Partitions

34. Define *cubical partition*.

35. Find all cubical partitions of the numbers 1 - 18.

36. Use your answers to Investigation **35** to complete the following table:

Integer, n	# Cubical Partitions, $c(n)$
1	1
2	1
3	1
4	
$\vdots$	
18	

37. Do you think there is a pattern in the number of cubical partitions that we can discover and concisely describe? Explain.

Our success with finding patterns in the number of partitions, be it regular, square, or cubical, has been limited. These so-called *partition enumeration problems* are indeed quite hard. Many of them have not been solved after decades of intensive study. So, let us turn to a different problem suggested by the story of Ramanujan and 1729.

7.7 Minimal Square Partitions

In the story 1729 was special because it was the smallest integer that was the sum of two cubes in two different ways. In other words, it was the smallest integer that had two different cubical partitions, each with just two terms.

Every number certainly has a square partition – just add $1 = 1^2$ as many times as you need to reach the number. For example, $8 = 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2$. Because every number can be written this way, there is nothing to study. On the other extreme, the perfect squares $1, 4, 9, \ldots$ are special for they have square partitions where only one term needs to be "added": e.g. $1 = 1^2, 4 = 2^2$, and $9 = 3^2$. What happens between these extremes? The number 8 can be

written as the sum of two squares: $8 = 2^2 + 2^2$. Since 8 is not a perfect square, the ***minimum square partition*** of 8 is $2^2 + 2^2$ which is a partition with exactly two terms.

38. Can 3 be written as the sum of two squares? If not, what is the minimal square partition of 3?

39. Use your results from questions above to complete the following table:

Integer, n	Minimum Square Partition	# Terms in the Minimum Square Partition
1	1^2	1
2	$1^2 + 1^2$	2
3		
4	2^2	1
⋮	⋮	⋮
12		

40. Is there a pattern to the number of terms in the minimum square partitions? Explain.

41. What was the largest number of terms that were needed from the minimum square partitions in the table in Investigation **39**?

Let us call the number that answers Investigation **41 Waring's number for square partitions** and denote it by W_2. We would like to know if W_2 is universal. In other words, we want to know if every positive integer can be square partitioned using this many or fewer terms.

42. Does 19 have a square partition involving W_2 or fewer terms?

43. Does 32 have a square partition involving W_2 or fewer terms?

44. Does 57 have a square partition involving W_2 or fewer terms?

45. Does 79 have a square partition involving W_2 or fewer terms?

46. Does 187 have a square partition involving W_2 or fewer terms?

47. Are you becoming confident that every whole number can be square partitioned in W_2 or fewer terms? Explain why or why not.

As early as 1621, the French mathematician **Claude Bachet** (French Mathematician; 1581 - 1638) suggested that W_2 terms were sufficient to square partition every positive integer. He checked every number up to 325 as evidence in support of the truth of his conjecture.

48. How long do you think it would take to check whether the first 325 positive integers could be square partitioned by at most W_2 terms? Once you did this, would you have a proof that W_2 terms were sufficient to square partition every positive integer? Explain.

Both Bachet and Fermat believed that the Greek mathematician **Diophantus** (Greek Mathematician; - circa 250 A.D.), one of the prominent historical figures in the history of number theory, was aware that W_2 terms were sufficient. Yet no record of a proof by Diophantus remains, Bachet never had a full proof and Fermat, writing in the margins of a copy of Diophantus' book Arithmetica, wrote that he had a proof but never wrote it down! We'll see that Fermat had a history of doing this, much to the chagrin of later mathematicians.

In 1772 Lagrange published a proof that finally demonstrated that W_2 terms are enough to square partition every number. Lagrange acknowledged his indebtedness to the supporting work of Euler, who had worked on the problem for 40 years! Remarkably, just one year after Lagrange proved the result, Euler gave a much simpler proof – one that is essentially the proof that is taught in undergraduate number theory courses.[6]

49. Complete the statement of Lagrange's theorem on square partitions below:

> **Theorem** (Lagrange, 1772) Every positive integer can be written as the sum of _____ squares.

7.8 Waring's Problem

A natural question is to ask whether a similar result holds for cubical partitions, quartic (fourth power) partitions, quintic (fifth power) partitions, and so on. This *generalization* was first explicitly considered by **Edward Waring** (English Mathematician; 1741 - 1793) in 1770 in his book Meditationes Algebraicae. His conjecture, that a similar result holds for all power partitions, has become known as **Waring's problem**. We explore it for cubical partitions.

50. Use earlier results to complete the following table:

Integer, n	Minimum Cubical Partition	# Terms in the Minimum Cubical Partition
1	1^3	1
2	$1^3 + 1^3$	2
3		
⋮	⋮	⋮
8	2^3	1
⋮	⋮	⋮
12		

51. Is there a pattern to the number of terms in the minimum cubical partitions? Explain.

52. What was the largest number of terms that were needed from the minimum cubical partitions in the table in investigation 50?

Just as above, let us call the number we are looking for **Waring's number for cubical partitions** and denote it by W_3.

[6] E.g. Chapter 12 of [Bur].

53. Do you think that the number you found in investigation Investigation **52** is W_3? Explain.

54. Does the number 43 have a cubical partition involving the number of terms considered in Investigation **52** or fewer?

55. Does the number 81 have a cubical partition involving the number of terms considered in Investigation **52** or fewer?

56. Does the number 107 have a cubical partition involving the number of terms considered in Investigation **52** or fewer?

57. Do you think you know what W_3 is? Explain.

58. Does the number 23 have a cubical partition involving the number of terms considered in Investigation **52** or fewer? If not, what is the number of terms in the minimum cubic partition?

59. Does the number 239 have a cubical partition involving the number of terms considered in Investigation **52** or fewer? If not, what is the number of terms in the minimum cubic partition?

60. Do you think you know what W_3 is? Explain.

61. Would it surprise you if I told you that it had been proven deductively that out of all infinitely many positive integers, the numbers 23 and 239 were the only positive integers that required this many terms to be cubically partitioned? Explain.

It was first proved in 1939 by **Leonard Eugene Dickson** (American Mathematician; 1874 - 1954) that you will never need more cubes to cubically partition any positive integer than you needed in investigations Investigation **58** and Investigation **59**. So we know exactly what W_3 is.[7] If it wasn't for the anomalies 23 and 239, the number you found in Investigation **52** would be W_3.

7.9 Solving Waring's Problem

Waring's problem concerns higher and higher powers indefinitely and we have seen that the work of many prominent mathematicians only settled the problem for the powers $n = 2, 3$. So it might seem that a solution to Waring's problem might be difficult if not downright impossible.

In fact, Waring's problem was "solved" in 1909 by **David Hilbert** (German Mathematician; 1862 - 1943), one of the twentieth century's greatest mathematicians. Hilbert solved it not by finding the identity of all of the Warning numbers W_n, but by proving that there must always be a number H_n so that every positive integer can be partitioned by H_n or fewer n^{th} powers. Interestingly, Hilbert's proof was an existence proof - it proved that these number H_n existed for every n without telling you what the H_n actually were!

62. Just because one knows theoretically that H_n exists, how does this guarantee that W_n exists as well?

[7] See, e.g., "On expressing integers as the sum of cubes and other unsolved number-theory problems," by Martin Gardner, *Scientific American*, Dec. 1973, pp. 118-21.

63. Give several examples of problems where you can prove that the answers exist without explicitly finding the answers, or where the answers might be remarkably hard to actually find.

Encouraged by Hilbert's existence proof, mathematicians have spent the twentieth century trying to find the values of the Waring numbers.

64. Fill in the following chart for the first three Waring numbers:

Partitions	Waring Number, W_n
Integer	$W_1 =$
Square	$W_2 =$
Cubic	$W_3 =$

65. Use Investigation **64** to make a conjecture about the remaining Waring numbers.

66. It was determined in 1986 that the fourth Waring number is $W_4 = 19$. Does this result agree with your conjecture in Investigation **65**? Do you have any confidence that you might be able to find a pattern in the Waring numbers considering this new information? Explain.

67. While mathematicians believe they finally have found a pattern, albeit a fabulously complicated one, that gives the value of each W_n, they have been unable to prove it.[8] Is this surprising to you? Explain.

68. What does investigation Investigation **67** suggest to you about how much is known about expressing the positive integers as sums of other positive integers, what should be one of the "simplest" parts of mathematics?

7.10 Further Investigations

F1. Determine the 10^{th} and 50^{th} pentagonal numbers.

[8]The pattern is $W_n \approx 2^n + Int((\frac{3}{2})^n)2$. This pattern is explored more fully in the section "Euler's formula for Waring numbers" in the Additional Investigations.

Chapter 8

The World's Greatest Mathematical Problem

> I had this very rare privilege of being able to pursue in my adult life what had been my childhood dream. I know it's a rare privilege but, if one can do this it's more rewarding than anything I could imagine.
>
> **Andrew Wiles** (English Mathematics Professor; 1953 -)

8.1 The Pythagorean Theorem

Ask anybody with a high-school education what formula they remember best from their 10-plus years of mathematics courses, and they are most likely to reply "$a^2 + b^2 = c^2$." Often, although not always, people can tell you that this formula describes the relationship between the legs and the hypotenuse of any right triangle and is called the **Pythagorean theorem**.

This important theorem is illustrated in the figures in Figure 8.1 and Figure 8.2, which actually provide a deductive proof of this theorem.[1] Although this theorem is, by name, attributed to the most famous of all mathematicians – **Pythagoras** (Greek mathematician; c. 570 BC - c 495 BC) - it turns out to have been well-known by many other ancient cultures. The Babylonian clay tablet known as ***Plimpton 322***, which dates to about 1700 B.C., was thought to be a record of accounting transactions. In 1945 **Otto Neugebauer** (Austrian mathematician and historian of Science; 1899 - 1990) and **Abraham Sachs** (American archeologist and linguist; 1915 - 1983) wrote the ground-breaking Mathematical Cuneiform Texts which showed that ancient cultures were much more advanced in mathematics and navigation than we had previously thought. Among other things, their deciphering of Plimpton 322 showed that the Babylonians knew and used the Pythagorean theorem more than one-thousand years before the birth of Pythagoras.

1. Explain why the figures that make up Figure 8.2 provide a deductive proof of the Pythagorean theorem, supplying any missing details as necessary.

[1] From Discovering Geometry by Michael Serra, Key Curriculum Press, 1997.

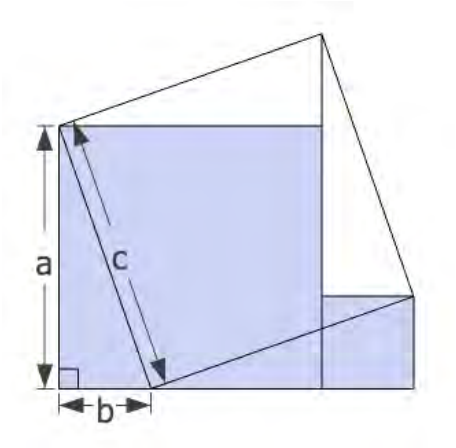


Figure 8.1: Initial set-up for proof without words of the Pythagorean theorem in Figure 8.2

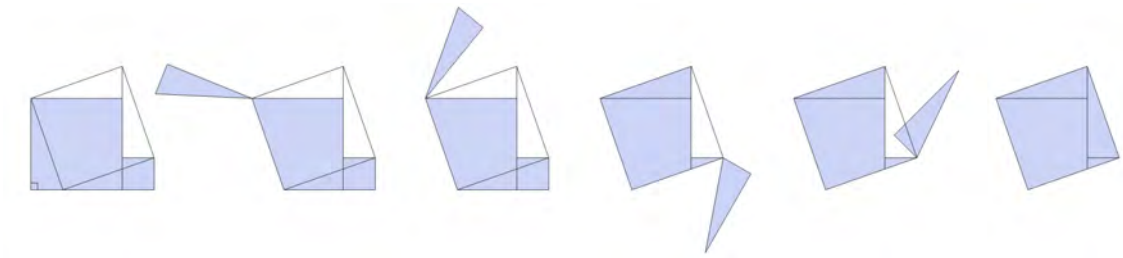


Figure 8.2: Proof without words: The Pythagorean theorem

8.2 Hundreds of Proofs

The Pythagorean theorem is central to mathematics and its culture. As a homage to its importance, several hundred different proofs of this result have been constructed. In fact, entire books of different proofs have been assembled, one with over 350 different proofs![2] One notable proof was found by then Ohio Congressman **James A. Garfield** (American politician; 1831 - 1881) who went on to be the 20^{th} President of the United States.

2. Find another proof of the Pythagorean theorem. Understand how this proof works and rephrase it in your own words, providing all necessary details.

[2] The Pythagorean Propostion by E.S. Loomis, National Council of Teachers of Mathematics.

Figure 8.3: Plimpton 322.

8.3 Pythagorean Triples

Although we generally recite the Pythagorean theorem in its algebraic garb, we are no doubt aware of its clear links to geometry. The Greeks did not have algebra as we would think of it now; they thought of results like the Pythagorean theorem in purely geometric terms. However, it is also the case that the Pythagoreans believed that "all is number." The connection between the Pythagorean theorem and special relationships between certain numbers was not lost on the Greeks.

The numbers 3, 4, 5 are said to form a **Pythagorean triple** because they are positive integers that satisfy the Pythagorean theorem:

$$3^2 + 4^2 = 5^2 \text{ since } 3^2 + 4^2 = 9 + 16 = 25 = 5^2.$$

It is likely that you remember such triples from learning about the Pythagorean theorem.

8.3.1 Pythagorean Triples as Partitions

There is a close connection of Pythagorean triples to earlier results we have been considering in this book. Namely, 3^2+4^2 is a *square partition* of the square 5^2. Prior to this, we have been trying to find patterns among all partitions of a given type. For example, in Section 7.7 of Chapter 7 we showed that it is possible for every positive integer to be square partitioned by 4 of fewer squares. That's fine, but it is also interesting to consider whether there are numbers that can be partitioned in particularly nice ways.

Partitioning 5^2 as $1^2 + 1^2 + \ldots + 1^2$ is quite boring – any number can be square partitioned in such a way. In discovering Waring's problem previously, we looked at the minimum partitions. The number 5^2 has a much more interesting minimal partition

$$5^2 = 3^2 + 4^2.$$

This partition is the simplest possible square partition after the trivial $5^2 = 5^2$. Thus, $3, 4$, and

5 share a special relationship, a relationship that was studied in detail by ancient cultures. What other numbers share this special relationship?

8.3.2 Finding Pythagorean Triples

3. If you haven't already in earlier studies, make a table of the first twenty squares.

4. Use your table to find all Pythagorean triples involving positive integers none of which are greater than 20.

5. Explain how you know you have found all of the triples.

We'd like to learn as much as we can about Pythagorean triples. What can we find of interest? Well, for one thing, the Pythagorean triple $(3, 4, 5)$ is interesting because the numbers are consecutive.

6. Based on your search of the table of squares, do you think there is another ***consecutive Pythagorean triple***? Explain.

7. Denote the number a in $a^2 + b^2 = c^2$ by the unknown variable x. Suppose (a, b, c) is a consecutive Pythagorean triple. Express b and c in terms of the unknown x.

8. Use your expressions in Investigation **7** to express the Pythagorean theorem only in terms of the unknown x. Simplify your equation as much as possible.

9. Solve your equation to determine the unknown x.

10. What do these results tell you about the number of consecutive Pythagorean triples? Does it tell you this inductively or deductively? Explain.

11. Can a Pythagorean triple consist of all even numbers? Prove your result.

12. Can a Pythagorean triple consist of all odd numbers? Prove your result.

13. How many different Pythagorean triples do you think there are? Explain.

14. The Pythagorean triple $(3, 4, 5)$ is the most basic triple there is. It generates many other related triples. Find several of these triples, and explain how they are *generated* by the triple $(3, 4, 5)$.

15. Prove that there are in fact infinitely many Pythagorean triples in the family generated by $(3, 4, 5)$.

8.3.3 Characterizing Pythagorean Triples

Because no nontrivial integer can be factored from the numbers in the Pythagorean triple $(3, 4, 5)$ it is called a **primitive Pythagorean triple**.

16. Which of your Pythagorean triples in Investigation **4** are primitive?

17. Can all three numbers in a primitive Pythagorean triple be even? Explain.

18. What possibilities does this leave for the even/oddness of the terms in a primitive Pythagorean triple?

19. The "next" largest primitive Pythagorean triples are:

$$(7, 24, 25)\ (20, 21, 29)\ (12, 35, 37)\ (9, 40, 41)\ (28, 45, 53)\ (11, 60, 61).$$

What does this data suggest about the even/oddness of the terms in a Pythagorean triple?

A beautiful insight - which was known to Euclid, as is shown in his Elements, and Diophantus, as shown in his Arithmetica, is that the even term in a primitive Pythagorean triple encodes sufficient information about the triple that it almost allows us to completely determine the other terms. Namely, they knew that one splits the even term b as $b = 2mn$ and then forms $c = m^2 + n^2$.

20. Choose a dozen positive, even integers $b \geq 4$ and split them as $b = 2mn$, choosing positive integers m, n as you desire. Record your data in a table of the form shown in Table 8.1.

21. For each choice of b, m and n, form $c = m^2 + n^2$, adding your data to the table.

22. For each choice of b, m and n can you find a value of a so (a, b, c) is a Pythagorean triple? Add the appropriate values to the table.

23. Determine an appropriate formula for a in terms of m and n.

24. Prove that your algebraic formulas for a, b and c will always yield a Pythagorean triple.

25. Is every Pythagorean triple in your table primitive?

26. Show that at least six of the primitive Pythagorean triples that appear above arise from the parameterization you have rediscovered.

a	$b = 2mn$	m	n	$c = m^2 + n^2$	Is a, b, c Pythagorean triple?
	$4 = 2 \cdot 2 \cdot 1$	2	1	$5 = 2^2 + 1^2$	
	$6 = 2 \cdot 3 \cdot 1$	3	1	$10 = 3^2 + 1^2$	

Table 8.1: Data for parameterizing Pythagorean triples.

While the parameterization you rediscovered was known to Euclid and Diophantus, it was not known until much later that it indeed accounted it for all primitive Pythagorean triples. In fact, it does. This definitive result was, as far as we know, first established by Fibonacci in his 1225 A.D. text Liber Quadrotorum.

8.4 Fermat's Last Theorem

Earlier we worked not just with square partitions but with cubical partitions, as well. There is certainly a natural analogy. Namely, we can find positive integers a, b, and c such that $a^2+b^2 = c^2$. Can we find positive integers a, b, and c such that

$$a^3 + b^3 = c^3?$$

If we can, what can we learn about them? After this, there is nothing to stop us. We might as well ask whether there are solutions to $a^4 + b^4 = c^4$ and what we can learn about them. And then $a^5 + b^5 = c^5$. And so on.

Pierre de Fermat, who we've mentioned often in our investigations, asked exactly these questions. He asked these questions as he studied the Pythagorean Theorem from a translation of the important text Arithmetica which was written by Diophantus of Alexandria (circa 250 A.D.). Fermat had a habit of writing notes in the margins of this text as he read. He made many important discoveries that are recorded in this way; including, as we have already noted, observations about the sums of squares. It is unfortunate, but rarely did he write down proofs of these results. He was content simply to record these discoveries and share them with various correspondents with whom he shared mathematical interests.

We are thankful to Fermat's son Samuel for publishing, in 1670, an edition of Diophantus' Arithmetica which contained all of Fermat's marginalia in an appendix. Had Fermat's observations not been so preserved, number theory's progress might have been set back a century or more. These results were all subsequently investigated and, on the large, proved to be correct. All, that is, except his result on solutions to the equation $a^n + b^n = c^n$, which remained mysterious. For this reason, the result has since been referred to as *Fermats Last Theorem*.

Around 1637 Fermat scribbled the following (in)famous note in his copy of Arithmetica near Diophantus' results on Pythagorean triples:

> It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I have discovered a truly wonderful proof, *but the margin is too small to contain it.*

Fermat was claiming that Pythagorean triples were the beginning and end of the line - there were no other similar results. That is, no matter how hard one looked, one would never find nontrivial, whole number solutions to the **Fermat equation** $a^n + b^n = c^n$ when $n \geq 3$. This result has become known as **Fermat's last theorem**.

8.4.1 Fermat's Last Theorem for $n = 3$

Having taken care of the Pythagorean triples, we would like to move on to the higher powers that Fermat mentioned in his marginalia.

In Investigation Section **??** of Chapter **??**, we saw that there are only two cubical partitions of the cube 8: 2^3 and $1^3+1^3+1^3+1^3+1^3+1^3+1^3+1^3$. So 2^3 cannot be partitioned into the sum of two cubes.

27. Can the cube $27 = 3^3$ be partitioned into the sum of two cubes? Prove your result.

Figure 8.4: Pierre de Fermat.

28. Can the cube $64 = 4^3$ be partitioned into the sum of two cubes? Prove your result.

29. Can the cube $125 = 5^3$ be partitioned into the sum of two cubes? Prove your result..

30. Can the cube $216 = 663$ be partitioned into the sum of two cubes? Prove your result.

31. Can the cube $343 = 7^3$ be partitioned into the sum of two cubes? Prove your result.

32. Can the cube $512 = 8^3$ be partitioned into the sum of two cubes? Prove your result.

33. Do you think that there is *any* cube that can be partitioned into the sum of two other cubes? Explain.

In fact, by 1750 Euler had proven that Fermat was correct in the special case when $n = 3$: there are no positive integers which solve the Fermat equation $a^3 + b^3 = c^3$.

Seeing that one cannot ever cubically partition a cube into the sum of two cubes, it is natural to wonder whether three cubes might occasionally suffice. They can.

34. Show that 6^3 can be partitioned into the sum of three cubes.

8.4.2 Prizes for Solving Fermat's Last Theorem

Over time many prizes have been offered for solutions to Fermat's last theorem. For example, an English doctor named **Paul Wolfskehl** (German Doctor and Mathematician; 1856 - 1906), who became afflicted with a debilitating case of multiple sclerosis, credits the intrigue of Fermat's last theorem with keeping him from committing suicide. He bequeathed a large trust to be awarded to the first person to actually solve this problem.[3]

[3]For a detailed discussion see "Paul Wolfskehl and the Wolfskehl Prize," by Klaus Barner, *Notices of the American Mathematical Society*, vol. 44, no. 10, November 1997, pp. 1294-1303.

So numerous were the crackpot "solutions" that the work of judging these solutions overwhelmed the mathematicians in charge of the award. The noted number theorist **Edmund Landau** (German Mathematician; 1877 - 1938) had postcards printed which read, "Dear Sir of Madam: Your attempted proof of Fermat's theorem has been received and is herewith returned. The first mistake is on page [ ], line [ ]." Landau would give the "solutions" to his students to fill in the missing numbers.[4]

8.4.3 Fermat's Last Theorem for $n = 4$

After the integers (power 1), the squares (power two), and the cubes (power three) comes the **quartics**, numbers of the form m^4.

35. Make a table of the first dozen quartics.

36. Can any of these quartics be partitioned into the sum of two other quartics? Explain in detail.

37. Do you believe, as Fermat claimed, that no quartic can be partitioned into the sum of two quartics? Explain in detail.

In fact, Fermat himself gave a deductive proof in the special quartic case $n = 4$: there are no nontrivial, positive integers which solve the Fermat equation $a^4 + b^4 = c^4$. This proof was given in the margins of one of his texts, just like the statement of the full last theorem. Only this time the margin was large enough to contain the proof![5]

38. Why do you think Fermat chose to prove the special $n = 4$ case of his Last Theorem when he believed he had a proof of the more general result which includes the $n = 4$ case as a consequence?

8.4.4 Euler's Conjecture

39. Can the quartic $2401 = 7^4$ be partitioned into the sum of three quartics? Prove your result.

40. Can the quartic $4096 = 8^4$ be partitioned into the sum of three quartics? Prove your result.

41. Can the quartic $6561 = 9^4$ be partitioned into the sum of three quartics? Prove your result.

42. Do you think that there is *any* quartics that can be partitioned into the sum of three other quartics? Explain.

43. Use the following computations, done with the help of the mathematical software like Wolfram Alpha, to show that the quartic 353^4 can be partitioned as the sum of four quartics:

$$353^4 = 15,527,402,881$$
$$315^4 = 9,845,600,625$$
$$272^4 = 5,473,632,256$$
$$120^4 = 207,360,000.$$

[4] From Elementary Number Theory by Underwood Dudley, W.H. Freeman and Co., p. 136.

[5] "Fermat's Last Theorem and Modern Arithmetic," by K.A. Ribet and B. Hayes, *American Scientist*, vol. 82, March-April 1994, pp. 144-56.

44. Use your observations in this section to complete the following conjecture due to Euler:

Conjecture (Euler; 1769) The n^{th} power m^n of the positive integer m cannot be partitioned into the sum of other n^{th} powers, in a non-trivial way, using $\boxed{}$ terms.[6]

45. If Fermat's last theorem were known to be true, would the truth of Euler's conjecture follow as a consequence? Explain in detail, using specific exponents to illustrate the connections and/or differences.

46. If Euler's conjecture were known to be true, would the truth of Fermat's last theorem follow as a consequence? Explain in detail, using specific exponents to illustrate the connections and/or differences.

8.4.5 Solutions to Special Cases of Fermat's Last Theorem

Since its statement, there was no progress in settling Euler's conjecture. The same is not true for Fermat's Last Theorem. As we said, Euler and Fermat had settled the $n = 3$ and $n = 4$ cases, respectively. Many decades later, in the 1820's, the French mathematician Legendre and the German mathematician **J.P.G. Lejeune Dirichlet** (German mathematician; 1805 - 1859) gave proofs of the $n = 5$ case. Dirichlet later gave a proof for $n = 14$ as well, partially rescuing his doomed efforts to prove the $n = 7$ case.

A remarkable breakthrough came in the 1820's when an unknown M. Leblanc proved that Fermat's last theorem holds whenever the exponent n is a special type of prime. These special primes are quite numerous, possibly even infinite, and include all of the primes $2, 3, 5, 11, 23, 29, 41, 53, 83, 89$. M. Leblanc, whose identity was unknown, became an immediate cause célébre!

M. Leblanc was, in fact, **Sophie Germain** (French mathematician; 1776 - 1831), a French woman who was not allowed to study at the universities because of her sex, but who had been secretly securing and studying notes from the classes of France's finest mathematicians. So remarkable were her results that the community of mathematics had no option but to except her into its circles. Said Gauss, considered one of the greatest mathematicians of all time,

> When a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men... succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of [number theory], then without doubt she must have the noblest courage, quite extraordinary talents and superior genius.

The special prime exponents which were at the heart of Germain's results are called *Germain primes* in her honor.

Progress on special cases of Fermat's last theorem continued.

Then, at a 1 March, 1847 meeting of the Paris Academy, the French mathematician **Gabriel Lame** (French mathematician and engineer; 1795 - 1870) announced that he had proven Fermat's Last Theorem. However, there was immediate controversy about the validity of the proof. There appeared to be gaps in the proof. The German mathematician **Ernst Kummer** (German mathematician; 1810 - 1893) not only found explicit examples where Lame's proof broke down, but he

[6] See, e.g., History of the Theory of Numbers, vol. II, by L.E. Dickson, New York, 1934.

was also able to repair the proof for infinitely many exponents, particularly those exponents that are now known as *regular primes*. Alas, there were still infinitely many exponents that remained to be checked.

As noted above, awards were offered for solutions to Fermat's last theorem. Later, computers helped push the search for counter-examples to exponents $n > 4,000,000$.[7] Yet, hundreds of years of searching left both Fermat's last theorem and Euler's conjecture unblemished – no counter-examples had been found – but unsolved, as well.

47. Given the long, fruitless search for counter-examples, do you suppose that mathematicians were content with the apparent truth of these conjectures? Explain.

8.4.6 A Breakthrough

48. Complete the following quintic partition of the quintic 144^5 into a sum of four terms using the computations below:

$$m^5 + 84^5 + 110^5 + 133^5 = 144^5$$

where

$$144^5 = 61,917,364,224$$
$$133^5 = 41,615,795,893$$
$$84^5 = 4,182,119,424.$$

The result in Investigation **48** was discovered by **L.J. Lander** (; -) and **T.R Parkin** (; -) in 1966.[8]

49. How do you think Lander and Parkin discovered the result?

50. What does the result tell us about Fermat's Last Theorem? What does it tell us about Euler's conjecture?

In 1988 **Noam D. Elkies** (American Mathematician and Chess Master; 1966 -) discovered[9] that

$$2,682,440^4 + 15,365,639^4 + 18,796,760^4 = 20,615,673^4.$$

In announcing this result, Elkies also noted that **Roger Frye** (; 1940 -) found the smallest such quartic partition of a quartic into a sum of three terms:

$$95,800^4 + 217,519^4 + 414,560^4 = 422,481^4.$$

51. What do these results tell us about Fermat's Last Theorem? What do they tell us about Euler's conjecture?

[7] See Ribet and Hayes article referenced above.

[8] "Counterexamples to Euler's Conjecture on Sums of Like Powers", L.J. Lander and T.R. Parkin, *Bulletin of the American Mathematical Society*, vol. 72, 1966, pp. 1079.

[9] "On $A^4 + B^4 + C^4 = D^4$", by N.D. Elkies, *Mathematics of Computation*, vol. 51, no. 184, October 1988, pp. 825-835.

52. Why didn't I leave out one of the terms and have you (re-)discover Elkies' or Frye's results as I did in Investigation **48** above?

53. How do you think Elkies and Frye discovered their results? Explain.

In fact, Elkies and Frye relied on increasingly sophisticated mathematical developments in *analytic number theory* that had been building for some thirty years. These developments include *elliptic curves*, *modular forms*, and *Galois representations* and are the result of the dedicated work of many contemporary mathematicians over many decades, including: **Yutaka Taniyama** (Japenese mathematician; 1927 - 1958), **Goro Shimura** (Japanese mathematician; 1930 -), Elkies, Frye, **Robert Langlands** (Canadian mathematician; 1936 - ,) **Gerd Faltings** (German mathematician; 1954 -), **Jean-Pierre Serre** (French mathematician; 1926 -), **John Coates** (Australian mathematician; 1945 -), **Peter Sarnak** (South African mathematician; 1953 -), **Nicholas Katz** (American mathematician; 1943 -), **Karl Rubin** (American Mathematics Professor; 1956 -), **Barry Mazur** (American mathematician; 1937 -), **Ken Ribet** (American mathematician; 1948 -), **Richard Taylor** (English mathematician; 1962 -), and lastly Andrew Wiles. While progress was certainly being made, few held out hope that a proof of Fermat's last theorem was within reach.

8.4.7 A Truly Remarkable Proof

On 20 June, 1993 Andrew Wiles, a Professor of Mathematics at Princeton University, was scheduled to give three hour-long lectures over three consecutive days at an international mathematics conference at Cambridge University in England. Wiles was a noted mathematician who had increasingly withdrawn from research circles over the prior seven years, publishing only a few papers and risking the loss of important research funding.

Yet his first lecture sped his ascent back into the mathematical limelight. He had, in virtual isolation, made groundbreaking contributions to analytic number theory. Emails and phone calls circled the world - "Come to Cambridge to hear Wiles' lectures; something big is up." The crowds grew the second day and packed the lecture hall the third day. As his third lecture neared its conclusion, Wiles proceeded through the final few logical arguments that completed the proof of his major result - a result which had a remarkable consequence. Namely, among other things, his work established the truth of Fermat's Last Theorem. Wiles completed his proof, wrote the statement of Fermat's last theorem onto the chalkboard, and then modestly turned to the astonished audience to modestly announce, "I think I'll stop here."[10]

The amazing news was instantly circulated world-wide via email and phone messages. Wiles' picture and a lengthy story graced the front page of the next day's *New York Times*. Stories appeared in *Time*, *Newsweek*, and print media throughout the world. Wiles was named one of the year's "25 Most Interesting People" by *People Magazine*.

But the perfect ending to the enigmatic theorem of Fermat was yet to unfold. For like the fate that befell Lame and so many other mathematicians throughout its near 350-year history, Wiles 200-page proof succumbed to a logical defect as it was checked by experts. For months he struggled, finally breaking his silence with a 4 December, 1993 email to the mathematical community:

[10]The story briefly described here is captured powerfully in the Nova documentary The Proof [LySin], which is highly recommended, and the corresponding trade book Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem [SinLy].

Figure 8.5: The end of Andrew Wiles' third lecture.

> In view of the speculation on the status of my work on the Taniyama-Shimura conjecture and Fermat's Last Theorem I will give a brief account of the situation. During the review process a number of problems emerged, most of which have been resolved, but one in particular that I have not settled. The key reduction of (most cases of) the Taniyama-Shimura conjecture to the calculation of the Selmer group is correct. However, the final calculation of a precise upper bound for the Selmer group in the semistable case (of the symmetric square representation associated to a modular form) is not yet complete as it stands. I believe that I will be able to finish this in the near future using the ideas explained in my Cambridge lectures.

But Wiles was unable to fill this gap.

Desperate and in the position of "doing mathematics in that kind of rather over-exposed way [which] is certainly not my style and I have no wish to repeat," Wiles enlisted the help of his former student Richard Taylor.

On 3 April, 1994 another email stunned the world. It announced that Noam Elkies had found a counter-example to Fermat's Last Theorem with exponent $n > 100,000,000,000,000,000,000$ In other words, not only was Fermat wrong, but Wiles' gap must be fatal – his proof was incorrect. After a few days of turmoil, it became clear that the email was the result of an April Fools' Day joke from the Canadian mathematician **Henri Darmon** (Canadian mathematician; 1965 -) which had gotten out of hand, spreading like a computer virus.

Wiles and Taylor made no progress through the summer. But on Monday, 19 September, 1994, the breakthrough came. In Wiles' own words:

> I was trying to convince myself that it didn't work, just seeing exactly what the problem was. Suddenly, totally unexpectedly, I had this incredible revelation. I, I realized what was holding me up was exactly what would resolve the problem I'd had in my Iwasawa theory attempt three years earlier. It was the most, the most important moment of my working life. It was so indescribably beautiful, it was so simple and so elegant and I just stared in disbelief for twenty minutes. Then during the day I walked round

> the department, I'd keep coming back to my desk and looking to see if it was still there. It was still there... My original approach to the problem from three years before would make it exactly work. So out of the ashes seemed to rise the true answer to the problem. So the first night I went back and slept on it, I checked through it again the next morning and by 11 o'clock I was satisfied. I went down and told my wife, "I've got it, I think I've got it, I've found it." It was so unexpected, she, I think she thought I was talking about a children's toy or something, said, "Got what?" And I said, "I've fixed my proof, I, I've got it." [11]

On 25 October, 1994 the world was treated to the final email in history's chapter of Fermat's last theorem. It noted,

> As of this morning, two manuscripts have been released: "Modular Elliptic Curves and Fermat's Last Theorem, by Andrew Wiles and "Ring Theoretic Properties of Certain Hecke Algebras," by Richard Taylor and Andrew Wiles. The first one (long) announces a proof of, among other things, Fermat's last theorem, relying on the second one (short) for one crucial step... While it is wise to be cautious for a little while longer, there is certainly reason for optimism.

In fact, these two articles make up an *entire issue* (vol. 142, 1995) of the prestigious *Annals of Mathematics*, the first article on pages 443-551 and the second on pages 553-72.

8.4.8 Perspectives on These Historic Accomplishments

54. The title of this chapter is "The World's Greatest Mathematics Problem." Which problem do you think this refers to: The Pythagorean theorem, Pythagorean triples, partitions, Euler's conjecture, or Fermat's Last Theorem? Explain.

55. Suppose I had asked you to write a brief essay on the working life of a mathematician when you first began this course and to rewrite it having worked through this book, watched the video "The Proof," and completed the other mathematical investigations from this course. How might your essays have compared? In other words, are there important ways that your views have been reinforced or have been changed?

56. As a current student of mathematics, a prospective parent, and a citizen of the technology-driven twenty-first century, are there lessons that you can take and use from the story of Fermat's Last Theorem?

57. Wiles spent eight years working in virtual isolation on Fermat's last theorem. What do you think about his efforts? Do his efforts compare with the efforts of professionals in other areas? Explain how they do or why they do not.

[11] [LySin].

8.5 Further Investigations

8.5.1 Parity of Primitive Pythagorean Triples

In and around Investigation **18** the question of the ***parity*** - even or odd - the terms in primitive Pythagorean triples is investigated. A proof that there is only one possible parity for the c term is outlined here.

F1. Square several odd numbers. What is the remainder of when this square is divided by 8?

F2. Using the fact that any odd number can be written as $2n+1$ where n is an integer, prove self-evident conjecture in Investigation **1**.

F3. If both a and b are odd what is the remainder when a^2+b^2 is divided by 4? Explain.

F4. Prove that a^2+b^2 cannot be the square of another integer, proving that there is no primitive Pythagorean triple with a, b odd and c even.

8.5.2 Euclid's Parameterization for Pythagorean Triples

The splitting $b = 2mn$ and formation of $c = m^2 + n^2$ to parameterize Pythagorean triples is not given much motivation above. It is not complicated to do so with some reasonable algebra skills, as is outlined here.

F5. Since we want $a^2 + b^2 = c^2$, $b^2 = c^2 - a^2$. Factor the right-hand side of this equation.

F6. Explain why this allows one to conclude

$$\frac{c+a}{b} = \frac{b}{c-a}.$$

Since c, a, b are integers, $\frac{c+a}{b}$ can be reduced to its lowest terms - call this reduced fraction $\frac{m}{n}$.

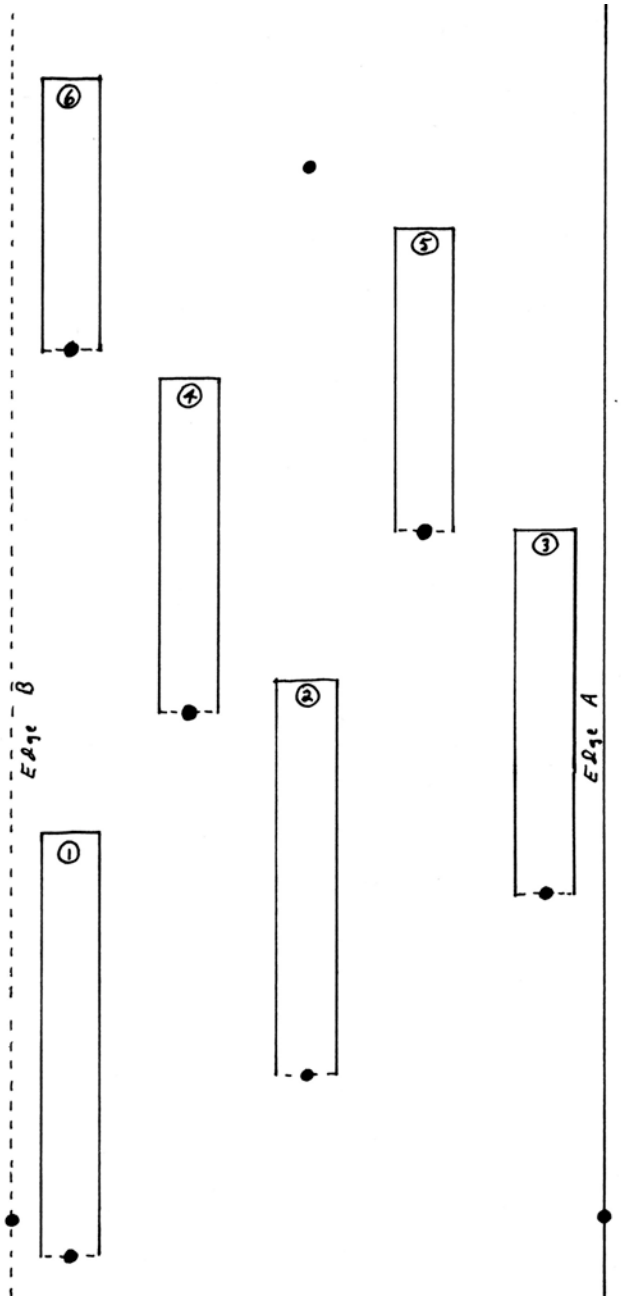
F7. Explain why $\frac{c-a}{b} = \frac{n}{m}$.

F8. Evaluate the sum $\frac{c+a}{b} + \frac{c-a}{b}$ to demonstrate

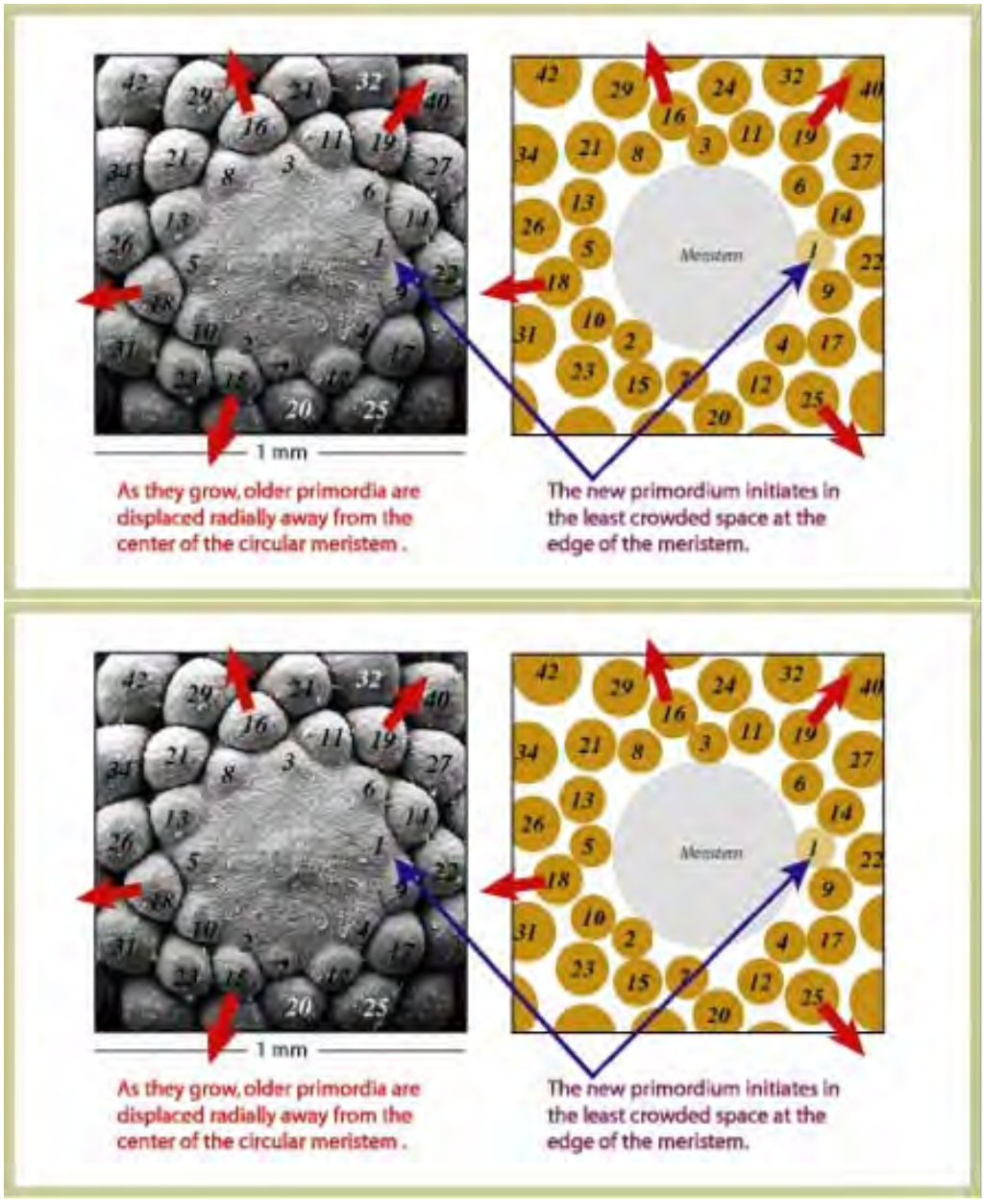
$$\frac{c}{b} = \frac{m^2+n^2}{2mn}.$$

Appendix

This page intentionally left blank.


6
5
4
3
2
1
Ellie B
Ellie A

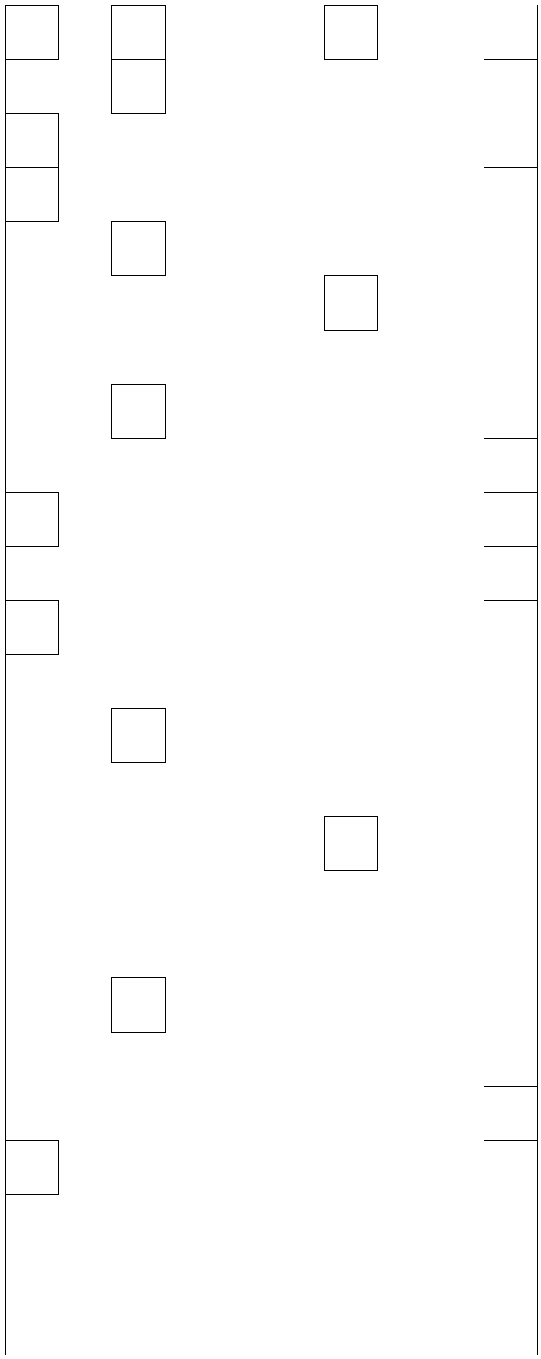
This page intentionally left blank.


1 mm
As they grow, older primordia are displaced radially away from the center of the circular meristem .
The new primordium initiates in the least crowded space at the edge of the meristem.
Meristem
1 mm
As they grow, older primordia are displaced radially away from the center of the circular meristem .
The new primordium initiates in the least crowded space at the edge of the meristem.
Meristem

This page intentionally left blank.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230
231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250

This page intentionally left blank.



This page intentionally left blank.

Index