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

15 May, 2003

Discovering the Art of

Number Theory

A Topical Guide

Julian F. Fleron, Ph.D.
Department of Mathematics
Westfield State College

Figures 1.2, 1.7, 2.1, 2.2, 2.5, 2.6, and 6.1 are copyrighted images. They are currently being used under fair use guidelines for educational purposes. Arrangements are being made for permissions for inclusion in a published version of this text. Other than these noted images, this entire text and its images fall under the copyright below:

Contents

Acknowledgements

This material was developed for use in the course Mathematical Explorations at Westfield State College.

I would like to take this opportunity to thank many fine faculty and students at Westfield State College for their insights, feedback, and inspiration. In particular, I would like to thank:

Students in MA110 - Mathematical Explorations played an active role in the genesis of this material and patiently worked through the original drafts as well.

Students in MA116 - Introduction to Mathematical Systems worked through the original drafts of some of this material.

Brandt Kronholm, who sparked my interest in partitions. He is one of those great students who you learn from more than you teach.

Mathematics faculty members Robert McGuigan, James Robertson, Philip K. Hotchkiss, and Larry Griffith who, in addition to being invaluable colleagues, were key sounding boards, offered critical feedback, and provided important inspiration.

Faculty members George Layng, Beth Rothermel, and Sharon Smith from the Westfield State College Reading and Writing Center provided important technical support and guidance.

Senior mathematics majors Gina Kennedy and Sarah Lewison who carefully helped me revise and edit final drafts of this work.

Dean Robert Martin and Vice President William Lopes for their ongoing encouragement.

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., Kris Hedblom, 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 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.

Somewhere something incredible is waiting to be known.

Carl Sagan

Live as if you were going to die tomorrow.
Learn as if you were going to live forever.

Mahatma Gandhi

Imagination is more important than knowledge.

Albert Einstein

Tell me and I'll forget.
Show me and I may not remember.
Involve me, and I'll understand.

Native American Saying[1]

[1] This wisdom has a long tradition and is attributed to many cultures, including ancient Chinese and Innuit.

PREFACE

Notes to the Explorer

Yes, that's you – you're the explorer. "Explorer?" Yes, explorer.

And these notes are for you…

I could have addressed you as "reader," but this is not a traditional book. Indeed, this book cannot be read in the traditional sense. For this book is really a guide. It is a map. It is a route of trail markers along a path through the world of mathematics. This book provides you, our explorer, our heroine or hero, with a unique opportunity to explore this path – to take a surprising, exciting, and beautiful journey along a meandering path through a mathematical continent named **number theory**.

"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 almost all mathematics textbooks, this book is not a transcribed lecture followed by dozens of exercises that closely mimic illustrative examples. Rather, each topic in this book begins briefly with a survey, narrative, or introduction followed by the much longer Investigations section. The Investigations form the heart of this book, this journey. In the form of a Socratic dialogue, the Investigations ask you to explore. They ask you to discover number theory. 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, 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 discovered each day than in any time in its long history. For example, the two biggest highlights along this path through number theory are mathematical discoveries that shook the mathematical world during the 1990's. In the time period between when these words were written and when you read them it is quite likely that 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 mathematical skills, mathematical reasoning, and mathematical applications. Arithmetical and statistical skills are useful skills everybody should possess. Who could argue with learning to reason? And we are all aware, to some degree or another, how mathematics shapes our technological society. But there is something more to mathematics than its usefulness and utility. There is its beauty. And the beauty of mathematics is one of its driving forces. As the famous mathematician **Henri Poincare** (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 both a liberal art and as a science. As a powerful science, mathematics shapes our technological society and serves an indispensable tool and language in many fields. But it is not our purpose to explore these roles of mathematics here. This has been done in many other fine, accessible books. (E.g. [COM] and [TaAr].) Instead, our purpose here is to journey down a path that values mathematics from 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** (427-347 B.C.). During the Dark Ages, classical knowledge was rescued and preserved by monasteries. Knowledge was categorized into the classical liberal arts and mathematics made up several of the seven categories.[2] 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 the contemporary classrooms and textbooks where the focus of attention has shifted solely to the training of qualified mathematical scientists. If you are a student of the liberal arts or if you simply want to study mathematics for its own sake, you should feel more at home on this exploration 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 human struggle and accomplishment. You will see many of the other arts in non-trivial roles: art and music to name two. There is also a fare share of philosophy and history. Students in the humanities and social sciences, you should feel at home here too.

Mathematics is broad, dynamic, and connected to every area of study in one way or another. There are places in mathematics for those in all areas of interest.

The great mathematician and philosopher **Betrand Russell** (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.

It is my hope that your discoveries and explorations along this path through number theory will help you glimpse some of this beauty. And I hope they will help you appreciate Russell's claim that:

[2] These were divided into two components: the *quadrivium* (arithmetic, music, geometry, and astronomy) and the *trivium* (grammar, logic, and rhetoric); which were united into all of knowledge by philosophy.

> … The true spirit of delight, the exaltation, 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, it is my hope that these discoveries and explorations enable you to make mathematics a real 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 served as beacons to people who have explored the continents of mathematics throughout history.

Mathematics is something that one *does*.

E.E. Moise

A mathematician, like a painter or poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas.

G.H. Hardy

Indeed, only a few are mathematically gifted in the sense that they are endowed with the talent to discover new mathematical facts. But by the same token, only a few are musically gifted in that they are able to compose music. Nevertheless there are many who can understand and perhaps reproduce music, or who at least enjoy it. We believe that the number of people who can understand simple mathematical ideas is not relatively smaller than the number of those who are commonly called musical, and that their interest will be stimulated if only we can eliminate the aversion toward mathematics that so many have acquired from childhood experiences.

Hans Rademacher and Otto Toeplitz

It is impossible to be a mathematician without being a poet in soul.

Sofia Kovalevskaia

The only way to learn mathematics is to do mathematics.

Paul Halmos

Number Theory

> Mathematics is the queen of the sciences and number theory the queen of mathematics.
>
> -- Carl Friedrich Gauss

> ...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*, 5 July, 1993.

Number theory is the name given by mathematicians to the study of whole numbers – 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** (1777-1855) that this is a very regal area. And you might be hesitant give it another look. Might $1 Million change your mind?

A Million Dollar Problem

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 5 primes. (Mathematicians usually exclude the number 1 as a prime.) In a letter dated 7 June, 1742 **Christian Goldbach** (1690-1764), a mathematician of little renown outside of this letter, wrote to **Leonhard Euler** (1707-1783), who we meet often across many areas of mathematics, that he had observed the following pattern:

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

On the basis of inductive evidence of this sort, Goldbach surmised, or, as mathematicians would say, *conjectured*, that each positive integer could be written as the sum of primes: two primes if it is even and three primes if it is odd.[3] This conjecture, known appropriately as **Goldbach's conjecture**, remains unsolved to this day despite tremendous efforts of mathematicians during the ensuing two and one-half centuries. As if the intellectual interest in solving a problem this long outstanding is not enough motivation, the Clay Mathematics Institute [CMI] has offered $1 Million dollars to anybody who can definitively resolve this conjecture![4] In other words, find an example where Goldbach's conjecture does not apply or prove that it will always work and $1 Million is yours.

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, by David Auburn [Aub], 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.[5]

In the Golden Globe winning and Oscar nominated movie A Beautiful Mind [How], the mathematical insights of Nobel prize-winning mathematician **John Nash** (1928-) are portrayed visually through whole number patterns seen in arrays of encrypted messages.[6] Although Nash's insights were extraordinary, an ability to discover patterns and relationships like this are critical to most mathematicians' work.

What Good Is This?

In our exploration of number theory, you might wonder "what good is this?" Some of the applications of number theory in the first few topics -- to art, architecure, biology, etc. – are immediate. *Fermat's Last Theorem*, *partition congruences*, and the content of later topics

---

[3] As mathematicians choose not to call 1 a prime, they typically ignore the first few cases. This is an instance where it makes more sense to consider 1 prime so no exclusions need to be made.

[4] Indeed, Goldbach's conjecture is one of seven *Millenium Prize Problems* in mathematics, each of which carries a reward of $1 Million from the Clay Mathematics Institute. [CMI]

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

[6] It should be noted that the movie took some dramatic license in these scenes. There is little evidence in the book on which the movie is based [Nas] that Nash worked with or thought about encryption of this sort.

have applications and implications whose explorations 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. In the Second World War the Allies superior encryption and decryption proved critical to their eventual victory. Central to the Allies effort were the roles of the Navajo "Code Talkers" in keeping classified U.S. transmissions secret and of British mathematicians, lead by the brilliant but persecuted **Alan Turing** (1912-1954), in deciphering the German *Enigma* codes.[7] In contemporary communication all classified and secure information is secured by encryption schemes like the *RSA algorithm* and the *Advanced Encryption Standard*[8] which are based squarely on patterns, methods, and algorithms from number theory. Without these number theoretic algorithms that are tested, developed, and refined by thousands of mathematicians and engineers, we could not send classified military information, we could not have secure ATM access, we could not have secure credit card transactions, we could not have secure email or Internet communication and data sharing, etc. In short, 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, §5], [Kah].)

Recent Breakthroughs

In addition to the numerous applications of number theory that pervade the Information Age, there have been many stunning breakthroughs in the more theoretical side of number theory during the past decade. In 1993, **Andrew Wiles** (1953-) shocked the world by providing 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 learn more of the story of Fermat's Last Theorem and the solution, an event that appeared on the front page of the *New York Times*[9]and resulted in Wiles being named as one of *People Magazine's* "25 Most Intriguing People of 1993". We will also learn about **Ken Ono's** (??) surprising extensions, just before the turn of the new millennium, of the Indian mathematician **Ramanujan's** (1887-1920) hundred year old work on *partition congruences*.

Although they just happened in the last decade, these mathematical breakthroughs will form key chapters in the long history of mathematics. This challenges the misperceptions of mathematics as a static, completed, archaic field, doesn't it?

---

[7] See Additional Investigations for more on the Navajo Code Talkers and Alan Turing.

[8] Beginning in May of 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.

[9] 24 June, 1993; the day after Wiles announced his proof at the end of three lectures he gave at a conference in Cambridge, England.

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. Yet none other than **G.H. Hardy** (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 in this chapter we will meet **Rhiannon L. Weaver** (??), a Penn State undergraduate who contributed a critical sequel to Ken Ono's work on partition congruences. And there is **Sarah Flannery** (1982 -), an Irish high school student who gained international acclaim by developing an encryption algorithm that could 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, <u>In Code: A Mathematical Journey</u> [Flan], is a wonderful account of the fascination that one can find in mathematics if one is provided with the opportunity and encouragement to explore it rather than the mundane task of memorizing and regurgitating it.

So here's your opportunity.

TOPIC 1

Fibonacci Numbers

All is number.

-- The Pythagoreans

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

Music is a hidden exercise in arithmetic, of a mind unconscious of dealing with numbers.

-- G.W. Leibniz

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 this counting, remarkable relationships and connections emerge. Some are merely 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.[10] When mathematicians see relationships and connections among numbers they seek to discover the underlying causal patterns and mechanisms. For mathematics is the science of patterns.[11]

A Remarkable Sequence of Numbers

In the world of botany a particularly compelling pattern of numbers emerges. Namely, when one counts 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 collection of numbers. Rather, the numbers 5, 89, 13, 34, 8, 21, 55, 144, and 3 occur repeatedly and almost exclusively. Arranged like this there might not seem anything striking other than the repeated occurrence of these numbers. But, in numerical order the numbers

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

[11] 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 one can do in a single statement. See the book [Dev1] of this name for a comprehensive discussion.

$$3, 5, 8, 13, 21, 34, 55, 89, \text{ and } 144$$

form a clear pattern. Each number is the sum of the two that come before it. Using this defining characteristic, it is easy to extend this pattern both forward and backward:

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

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

Universally 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 $f_2 = 1$. Notice that 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. It is interesting to note that the genesis of this sequence of numbers was not botanical despite its regular occurrence in this area. Instead, recorded history attributes this sequence of numbers to the solution of a typically hokey word problem in an important mathematical text by a mathematician nicknamed Fibonacci.

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** (circa 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 clearly 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 which 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.

Fibonacci's Problem

Despite his impact on the revival of mathematics and the acceptance of the Hindu-Arabic numeral system, Fiboanacci's notoriety comes via 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 the following:

> 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:

```
Month 1                     xy                      1 pair
                            |
Month 2                     XY                      1 pair
                            |    \
Month 3                     XY   xy                 2 pair
                       /    |    |
Month 4          xy         XY   XY                 3 pair
                 |     /    |    |    \
Month 5          XY    xy   XY   XY   xy            5 pair
```

Fig. 1.1 Fibonacci's Rabbits

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

Investigations

I. Fibonacci's Rabbits

1. Continue the breeding tree in Fig. 1.1 for three more months, checking that it yields the next three Fibonacci numbers. (Hint: You might find it useful to use different colors to distinguish mature versus juvenile rabbit pairs.)

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

We would like to know why this pattern 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 3) - 6) to explain why 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.)

Fig 1.2 Spirals in a Pinecone and a Sunflower

II: Fibonacci Spirals in Nature

Above are images of a pinecone and a sunflower. The seeds that make up both 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 eye 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 much the same way that you colored the clockwise family in 10). How many counter-clockwise spiral arcs are there?

12. Repeat 10) for the sunflower.

13. Repeat 11) for the sunflower.

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

15. Pinecones and sunflowers come in many different varieties, some more 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.

III: 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. Strangely, fertilized eggs result in worker bees while unfertilized eggs result in drones. That is, worker bees have a mother, the Queen, and a father, a drone. On the other hand, drones only have a mother, the Queen.

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 16) to determine the number of i) parents, ii) grandparents, iii) great-grandparents, iv) great-great-grandparents, and v) great-great-great-grandparents each 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 worker bee that goes back five generations.

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

In mentioning honeybees one would be remiss if they did not mention two other mathematical marvels involving honeybees. First, bees build their honeycomb in hexagonal cells because this *regular tessellation* provides the optimal storage for a given use of wax. I.e. bees are mathematicians of some merit.

More impressively, honeybees communicate the location of pollen sources via an intricate *waggle dance*. This dance was successfully translated only during middle of the twentieth century. The ability of the honeybee to communicate in such a sophisticated grammar remained a mystery until recently. In the mid 1990's 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.[12]

As Galileo said, “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.

IV: Plant Growth

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

Consider the growth of a plant. When a plant grows a new shoot it is likely that this shoot is not immediately ready to produce its own new shoot - it has to gain sufficient strength to support a new shoot. 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 month thereafter. One might expect that each shoot will behave in this same way. A plant with a growth pattern like this, four weeks after germination, will look as follows:

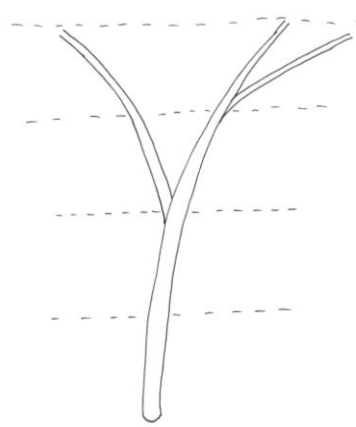


Fig. 1.3 A four week old Fibonacci Plant

20. Draw the plant in Fig. 1.3 after six weeks.

21. Draw this plant in Fig. 1.3 after nine weeks. (Note: You might use the same coloring techniques as you applied with the rabbits to help you.)

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

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

23. Explain why, in this situation, the number of shoots must always be a Fibonacci number.

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

V: Two Fibonacci Identities

One of the reasons for mathematicians' great fascination with Ficonacci numbers is the ubiquity of the relationships among them. In fact, there is an entire journal devoted to the Fibonacci numbers; it is called the *Fibonacci Quarterly*.

You will investigate two well-known identities here.

24. Determine the sum of the first three Fibonacci numbers; i.e. 1 + 1 + 2 = ?

25. Determine the sum of the first four Fibonacci numbers.

26. Determine the sum of the first five Fibonacci numbers.

27. Determine the sum of the first six Fibonacci numbers.

28. Determine the sum of the first seven Fibonacci numbers.

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

Pascal's triangle is the triangular array of numbers given below:

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
\iddots & & & \vdots & & \vdots & & & \ddots
\end{array}
$$

Fig. 1.4 Pascal's Triangle

Each entry in this triangular array is obtained by adding the two numbers in the previous row that are closest to the entry being obtained.

30. 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 $(x+y)^2$ one obtains $1x^2 + 2xy + 1y^2$ and these coefficients are exactly those in the third row of Pascal's triangle.

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

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

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

One cannot add the columns or diagonals of Pascal's triangle, 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.

34. What are the sums of the shallow diagonals just described?

35. What numbers make up the third shallow diagonal and what is the sum of these numbers?

36. What numbers make up the fourth shallow diagonal and what is the sum of these numbers?

37. What numbers make up the fifth shallow diagonal and what is the sum of these numbers?

38. 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 under *Polya block walking* in any book on *combinatorics* for a very interesting way to generate these patterns.

VI: The Mandelbrot Set

Pictured in Fig. 1.5, 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 **Benoit Mandelbrot** (1924-) who, as an IBM researcher in the 1970's, was the first to use computers to visually explore the complex mathematical objects that had been first investigated by the French mathematicians **Pierre Fatou** (1878-1929) and **Gaston Julia** (1893-1978). Fractals play a critical role in many natural and physical processes. A wealth of sophisticated, beautiful, interactive Internet sites on fractals are available as are accessible texts and texts that could be used in parallel with this text.[13]

---

[13] 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

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 such sites. One I would recommend is:

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.

Notice that 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 the mathematical literature. In the figure above, the rear cusp of the Mandelbrot, 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 which splits into two branches. These three filaments play a critical role in this bud's mathematical significance so we will label this bulb 3.

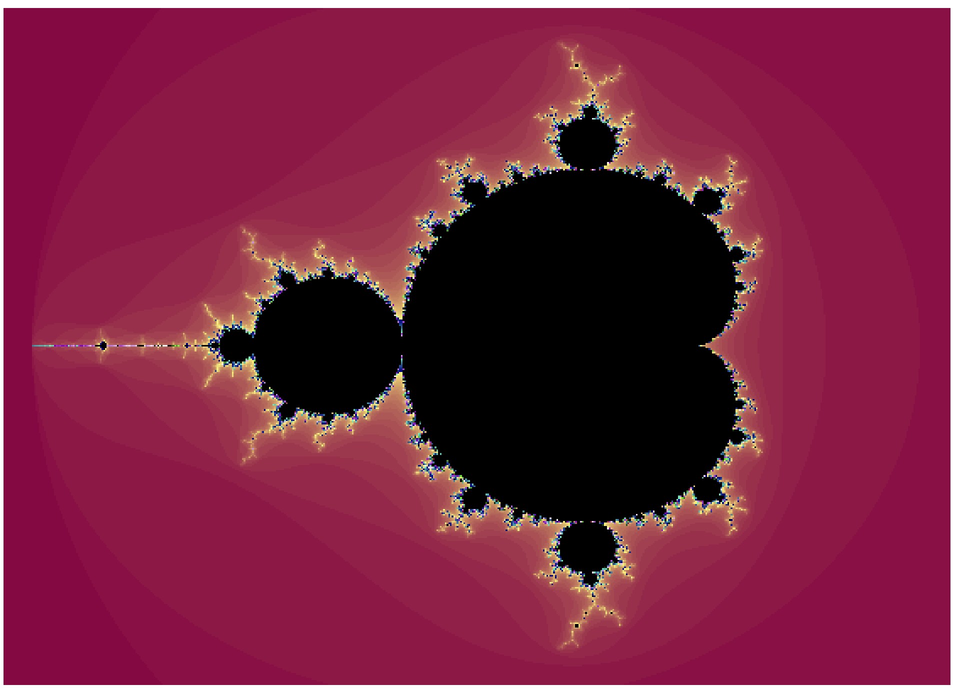


Fig. 1.5 The Mandelbrot Set

39. 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

---

Ann Connors Exploring Fractals site -- http://www.math.umass.edu/~mconnors/fractal/fractal.html are excellent places to start.

filaments that make up the starburst at the tip of this bulb. This number will be the label for this bulb.

40. Now locate the largest bulb between the bulb labeled 3 and the one you just found in investigation 39). 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.

41. Repeat 40), locating and labeling the largest bulb that appears between the bulbs you found in 39) and 40).

42. Repeat 40) again, locating and labeling the largest bulb that appears between the bulbs you found in 40) and 41).

43. Repeat 40) again, locating and labeling the largest bulb that appears between the bulbs you found in 41) and 42).

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

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

VII: Fibonacci Numbers Everywhere?

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

46. You have 2 hands. 2 is a Fibonacci number. What else about your hands exude Fibonacci numbers?

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

48. Consider the keys on a piano that make up an octave, as pictured in Fig. 1.6. Where do you see Fibonacci numbers here?

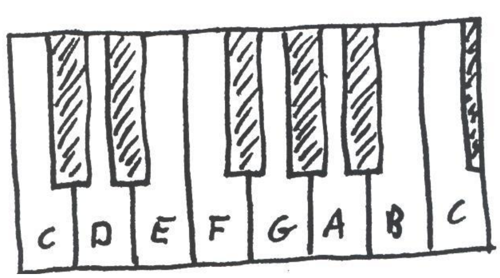


Fig. 1.6 An octave on a piano keyboard

49. 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.

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

The appearance of the Fibonacci numbers in the examples above seem spurious. In some cases they are. 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.[14] The patterns of music are harmoniously connected to the patterns of mathematics.

51. The mathematician **Richard Guy** (??) tells us "There aren't enough small numbers to meet the many demands made of them." How does this idea help us understand the apparently spurious appearance of Fibonacci numbers in our hands, in basketball, and in other surprising situations?

VIII: Phyllotaxis

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

[14] 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.

This resulting model is a model 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 of leaves. You should position your stem to stand vertically with the smallest leaf, leaf 6, at the top and the largest leaf, leaf 1, at the bottom.

52. Draw a top view of this 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 from your top view.

53. Determine the angle, measured counter-clockwise direction, between *successive leaves* (e.g. leaf 1 and leaf 2) in this arrangement.

54. Traverse the leaves in order, from 1 - 5, in a counter-clockwise fashion when viewed from above. Describe this path. For example, how many complete revolutions must you make before you arrive back at your starting place where the 6^{th} leaf will start the next tier of leaves? And how is your path illustrated on your model stem?

55. Use 54) to determine the fraction of a complete revolution between successive leaves. Compare with 53).

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

57. Determine the angle, measured clockwise direction, between successive leaves in this arrangement.

58. Traverse the leaves in order, from 1 - 5, in a clockwise fashion when viewed from above. Describe this path as in 54).

59. Use 58) to determine the fraction of a complete revolution between successive leaves. Compare with 57).

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

60. 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 counter-clockwise revolutions, when viewed from above, before you arrive back at your starting place where the 9^{th} leaf would start the next tier of leaves. Such an arrangement would be referred to as an arrangement with a **3/8 phyllotactic ratio**.

61. Draw a top view of this arrangement, much like you did in 52).

62. What would the angle between successive leaves in this arrangement have to be?

63. If you traverse the leaves in order, from 1 - 8, in a clockwise fashion when viewed from above, how many complete revolutions must you make before you arrive back at your starting place where the 9^{th} leaf will start the next tier of leaves? What do you notice about this number?

64. Will the 3/8 phyllotactic ratio result in a similar connection to the Fibonacci numbers that you described in 60)? Explain.

65. Would this leaf arrangement provide the same type of benefits to the plant as the 2/5 ratio did? If so, what specific attributes of the plant might determine whether a 2/5 or 3/8 ratio was more appropriate?

66. Describe an arrangement with a 5/13 phyllotactic ratio in detail. Must it continue the pattern we have observed in 60) and 64)?

67. What would the next such phyllotactic ratio be? Describe an arrangement with this ratio in detail. Must it continue the pattern we have observed in 60) and 64)?

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:

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 admit some caution however. As the important geometer **H.S.M. Coxeter** (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,... or 5, 2, 7, 9, 16,... Thus we must face the fact that phyllotaxis is really not a universal law but only a fascinatingly prevalent tendency."

68. Let us try to break away from the Fibonacci numbers and make an arrangement with a 4/10 phyllotactic ratio. Describe this arrangement and explain whether it would be as beneficial as those above or not.

69. Describe a phyllotactic ratio that does not involve Fibonacci numbers but nonetheless avoids the difficulty in 68). 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.

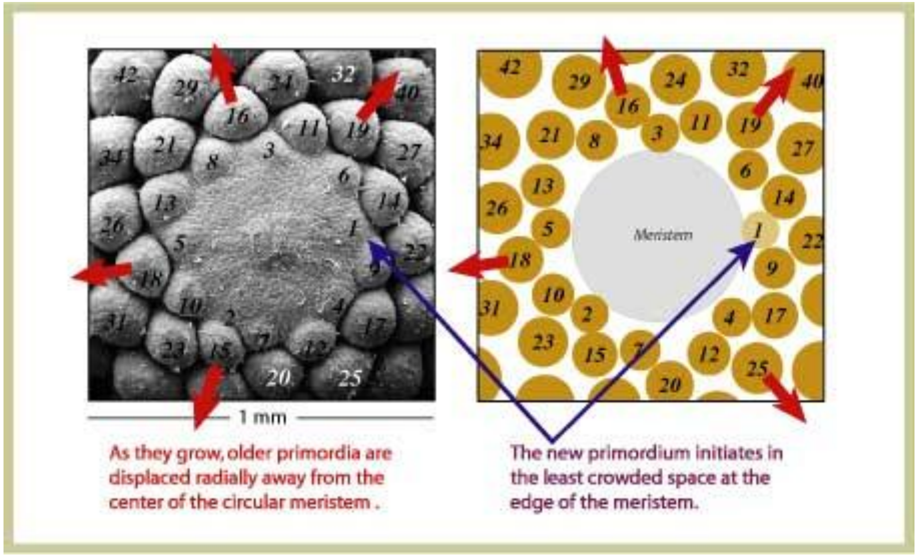


Fig. 1.7 Norway Spruce primordia development

IX. Fibonacci Spirals from Optimal Packing

As noted in Section I, objects like pinecones are made up of primordia which originate at a meristem and then move outward from the center of the meristem as new promordia develop. Mathematicians have long sought to understand the mechanics of this process and there has been much recent progress. An excellent description of some of this research, related on-line tutorials, and impressive interactive applets for exploration are available from Phyllotaxis - An Interactive Site for the Mathematical Study of Plant Pattern Formation which was developed at Smith College and is available at the URL www.math.smith.edu/~phyllo/index.html .

In this section we will briefly investigate one of the mechanisms for the development of spiral patterns. The photograph on the left of Fig. 1.7 is scanning electron micrograph of a Norway Spruce shoot. On the right is a schematic of this micrograph. The primordia are labeled according to age, those with higher numbers appeared longer ago. 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.

70. 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.

71. 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?

72. In looking at the schematic, you should see a pattern of spiral arcs in the counter-clockwise direction. On a copy of the schematic, color the arms of these spiral arcs just as you did in Section II. How many counter-clockwise spiral arcs are there?

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

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

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

76. 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 like you did above. How many of these 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].

77. 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 these lines to measure the angle between primordia 1 and primordia 2; primordia 2 and primordia 3; primordia 3 and primordia 4. How are these angles related to others that appear in this topic?

The angle you found in Investigation 77) is called the **Golden Angle**. It is a sibling of the Golden Ratio - our next topic.

TOPIC 2

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

> Mighty is geometry; joined with art, resistless.
>
> -- Euripedes

We are all familiar with the **counting numbers** 1, 2, 3, … We are also familiar with the **integers** ..., -2, -1, 0, 1, 2,… In working with circles and trigonometry we have all used the remarkable number **pi**, denoted by the Greek letter that it is named after: $\pi = 3.14159265...$ Many of us are familiar with the **base of the natural logarithm**, the number e = 2.71828182…,[15] 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 $i = \sqrt{-1}$ which 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*:

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

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!

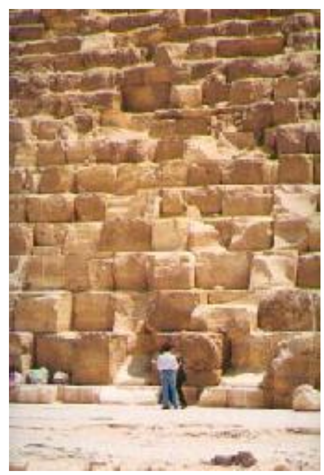


Fig. 2.1 The Great Pyramid of Khufu (Cheops); with a visitor for scale.

[15] We denote this constant by the letter e in honor of the Swiss mathematician Euler who was the first to investigate its remarkable properties.

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 da Vinci and Durer, in the music of Bartok and Bach, and psychological studies have even suggested that it is the most pleasing ratio there is -- perhaps explaining its use in architecture, art and music.[16] In fact, the Greek letter ϕ is used to denote this constant in honor of the Greek artist Phidias who used the Golden Ratio in his famous sculptures.[17]

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

Fig. 2.2 The Greek Parthenon

Division into Extreme and Mean Ratio

As noted above, the Golden Ratio is the number $\phi = \dfrac{1+\sqrt{5}}{2}$. 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[18]:

---

[16] See, for example, the section "Experimental Aesthetics" in Chapter V of The Divine Proportion by H.E. Huntely. There is considerable debate over the validity of these claims. See the Perspectives section of this topic for more details.
[17] Ibid, p. 25.
[18] One of the most famous and widely read books of all time.

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.

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 given 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 this division using straightedge and compass by following the steps in the diagram below:

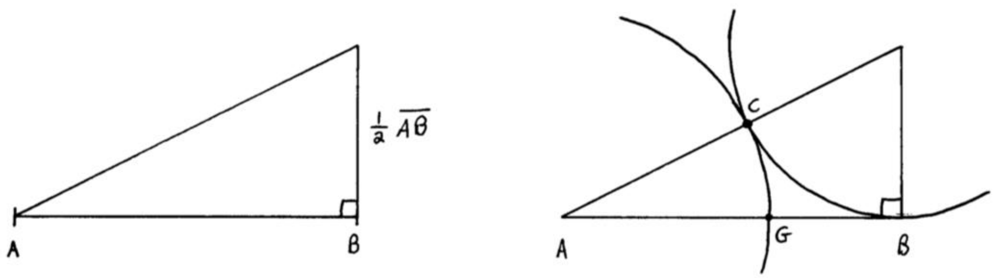


Fig. 2.3 Geometric derivation of the Golden Ratio.

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

$$\left(\overline{AB}\right)^2+\left(\frac{\overline{AB}}{2}\right)^2=\left(\overline{AG}+\frac{\overline{AB}}{2}\right)^2,\ \text{i.e. } \frac{5\left(\overline{AB}\right)^2}{4}=\left(\overline{AG}+\frac{\overline{AB}}{2}\right)^2.$$

Taking square roots and solving, we see that $\overline{AG}=\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}$. It follows that[19]:

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

$$\frac{\overline{AG}}{\overline{GB}}=\frac{\overline{AG}}{\overline{AB}-\overline{AG}}=\frac{\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}}{\overline{AB}-\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}}=\frac{\left(\frac{\sqrt{5}-1}{2}\right)\overline{AB}}{\left(\frac{3-\sqrt{5}}{2}\right)\overline{AB}}$$

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

$$=\left(\frac{\sqrt{5}-1}{2}\right)\cdot\left(\frac{2}{3-\sqrt{5}}\right)\cdot\frac{\overline{AB}}{\overline{AB}}=\frac{\sqrt{5}-1}{3-\sqrt{5}}=\frac{\sqrt{5}-1}{3-\sqrt{5}}\cdot\frac{3+\sqrt{5}}{3+\sqrt{5}}=\frac{2+2\sqrt{5}}{4}=\frac{1+\sqrt{5}}{2}\text{, as well.}$$

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

Now all this seems like a rather obtuse definition. But remember, π is defined as a ratio as well -- the ratio of a circle's perimeter to its diameter. So just give ϕ a little bit of time.

<u>Investigations</u>

I. 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 was not available to the ancient Greeks who used geometry as their universal language for mathematical analysis. However, we can find the Golden Ratio rather easily using basic high school algebra.

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

$$+\!\!\longrightarrow\!\!+\!\!\longrightarrow\!\!+$$

x 1

Fig. 2.4 Algebraic derivation of the Golden 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.

2. Use algebra to simplify the equation in 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 2) by hand, using a graphing calculator, spreadsheet, or computer algebra system.

4. Use your graph in 3) to determine how many solutions the equation in 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 2). Surprised?

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

Fig. 2.5 The United Nations Secretariat Building.

II. Nested Radicals

7. Use your calculator 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 were in 7)? If so, make a table of the values of the first ten repeated radicals correct to several decimals places. If not, explain why this process is limited.

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… 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…

9. …hazard a guess of the numerical identity of this infinite radical.

Let's see if we can determine the identity of this infinite object precisely.

10. Denote the unknown, infinitely-repeated radical by $x = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+...}}}}}$. 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 11) and earlier investigations to determine the value of x exactly. Does your answer agree with your guess in 9)? Explain.

III. 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

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

and even Bombelli's[20] remarkable

$$\sqrt{13} = 3 + \cfrac{4}{6+\cfrac{4}{6+\cfrac{4}{6+\cfrac{4}{6+...}}}}\ .$$

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

13. Convert the continued fraction $1+\cfrac{1}{1+\frac{1}{1}}$ into a standard fraction.

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

14. Convert the continued fraction $1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}$ into a standard fraction.

15. Convert the continued fraction $1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}}$ into a standard fraction.

16. Write the continued fraction that would come next in the pattern illustrated by investigations 13) - 15). Then convert this continued fraction into a standard fraction.

17. Write the continued fraction that would come next in the pattern illustrated by investigations 13) - 16). Then convert this continued fraction into a standard fraction.

18. Write the continued fraction that would come next in the pattern illustrated by investigations 13) - 17). Then convert this continued fraction into a standard fraction.

19. The numerators and denominators in the standard fractions that answer 13) - 18) form an important pattern. What pattern is this and how is it related to other material we have considered in this course?

20. Make a table that gives the decimal values of each of the fractions in 13) - 18) correct to several decimal places.

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

21. Does the data in 20) suggest a value for $1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}}$? Explain.

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

22. 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.

23. Simplify your equation in 22) to find an equation involving x that is fraction-free.

24. Use your answer in 23) and earlier problems to determine the value of x exactly. Does your answer agree with 21)? Explain.

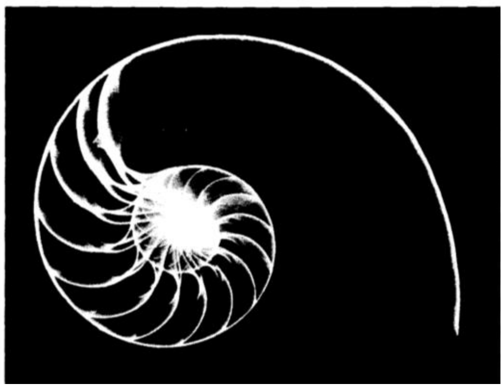


Fig. 2.6 Nautilus shell.

IV. Powers of ϕ

25. 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,…, 8.

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

27. What is even more surprising about these numbers?

In fact, 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 27).

28. In Topic 1 you were asked how hard it would be to determine the fiftieth Ficonacci number. Can you determine it now?

V. 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. The superstructure of the Parthenon forms a Golden Rectangle as does the face of "Mona Lisa" in one of the most well-known paintings of all time.

Below 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 in the rectangle.

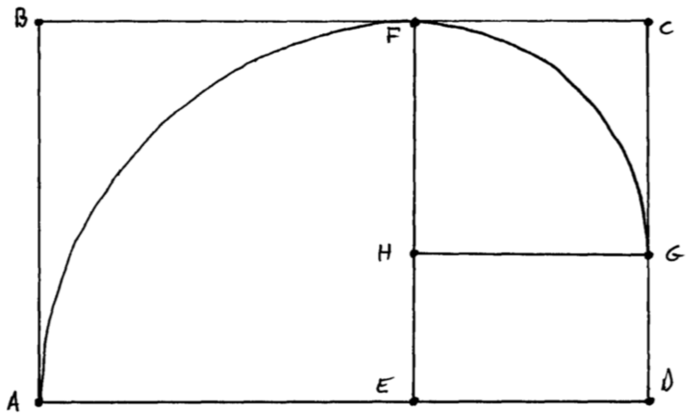


Fig. 2.7 First Stages of the Golden Spiral.

29. Is the rectangle ABCD a Golden Rectangle? Explain.

30. Is the smaller rectangle CDEF a Golden Rectangle? Explain in detail.

31. Is the even smaller rectangle DEHG a Golden Rectangle? Explain in detail.

32. Following the evident pattern, draw in another circular arc and another perpendicular. Is the even smaller rectangle that results a Golden Rectangle as well? Explain in detail.

33. Do you think you could repeat the process in 32) again and again? Is there any limit? Explain.

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

In fact, the shape that you drew in 34) is the shape of nautilus shells (see Fig. 2.6), one of many natural organisms whose growth is controlled by the Golden Ratio.[21] Additionally, the process that you carried out in 33) shows that, in some sense, Golden Rectangles are *fractals*.[22]

---

[21] See the Perspectives section at the end of this topic for details and references.
[22] Loosely speaking, a fractal is a geometric shape which reveals interesting fine structure, often self-similar in nature, which recurs indefinitely as it is magnified. Fractals have become quite popular and both non-technical

VI. Star Pentagrams

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

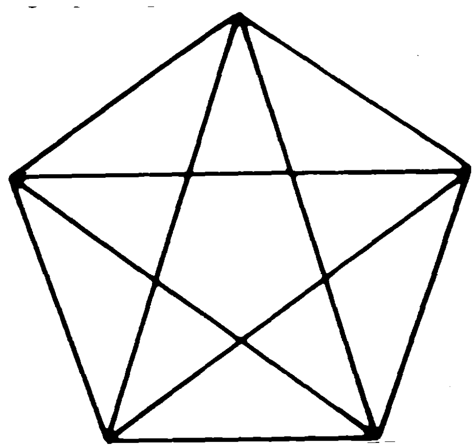


Fig. 2.8 Star Pentagram.

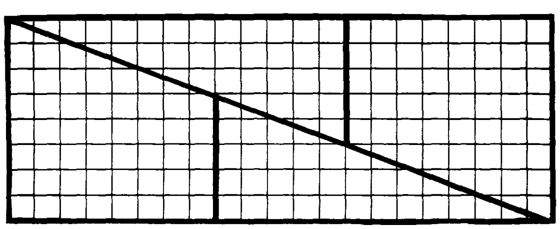
35. Measure each of the line segments of different length in the star pentagram and make a chart giving their lengths.

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

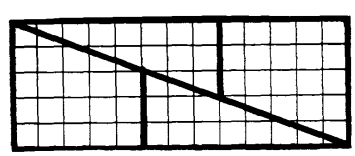
37. Could you draw another star pentagram somewhere within the given star pentagram? If so, provide an illustration. If not, explain why not.

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

VII. Magical Rectangles



Shape A



Shape B

Fig. 2.9 Magical rectangles.

print introductions and beautiful, dynamic Internet Java-scripts are widely available. (E.g. [Ste, Ch. 13], [FrPe], [Con], [Cool].)

Consider the similar figures in Fig. 2.9 above.

39. How are the dimensions of each of the pieces that comprise Shape A related to material we have recently been studying?

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

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

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

43. What are the areas of these square?

44. Are your answers to problems 41) and 43) compatible? Is this situation reasonable or even acceptable? Explain.

45. Can you construct other rectangles where this same behavior might take place? Explain.

Shape C below is similar to Shapes A and B above.

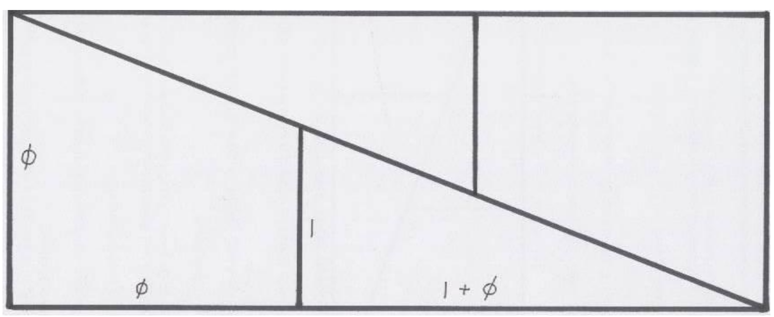


Fig. 2.10 Shape C: A golden, magical rectangle.

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

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

48. What is the area of this square?

49. Are your answers to problems 46) and 48) compatible? Explain. (Hint: Use your result from question 2) above to help you simplify if necessary.)

50. 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 confounding 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** (1892-1945) and Alfred Tarski (1902-1983) showed that it is theoretically possible to cut an orange into five pieces which 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. This apparent paradox, which is 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.

VIII. Perspectives on the Golden Ratio

51. 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 Fig. 2.5) 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.

52. In contrast to the debate about the occurrence of the Golden Ratio in the human world, the Golden Ratio does occur 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 a significant instance in which the Golden Ratio occurs in nature. Write a brief essay (appropriate to share with fellow students) which illustrates this occurrence of the Golden Ratio. You should include appropriate diagrams, some explanation of what natural function gives rise to the Golden Ratio, and reliable references.

IX. Galleries of Mathematics and Art; Mathematics and Nature

Hopefully the past two topics have given you the opportunity to see mathematics playing a central role in art and in nature. Enough connections between mathematics and both the arts and nature exist to fill up a whole college career, certainly more than can be hinted at in a single text. But part of the premise of this text is that you are the explorer. One way for your group of explorers (i.e. class) to learn more of the surprising and beautiful connections to the arts and nature is to create a gallery of posters - one done by each explorer.

Each explorer has the opportunity to choose a topic of particular interest: the spiral structure of DNA, M.C. Escher's hyperbolic tessellations, spirals in nature, the crystalline structure of snowflakes, the geometry of cubism, the mathematical mechanisms that determine animal coat patterns, origami, symmetry in quilting, the advent of perspective drawing, the mathematics of computer generated animation, mathematical structures in poetry, kaleidoscopes, the placement of guitar frets, fractals in musical compositions, the fourth dimension in modern art, or any other of thousands of topics that one can find quickly in print and Internet literature searches. Together, all of you get to see these varied connections of mathematics to the arts and nature.

For those of you who have not ever seen a poster session, they are widely used to publicize, announce, and/or present the results of research investigations. They are used in professional conferences (including virtually all conferences for mathematicians and scientists), college and university courses, and meetings of all kinds. They are useful because many posters can be displayed without the time and space limitations that traditional presentations impose. Additionally, it makes it easier for participants to browse and find research of interest.

At our college we have created galleries of posters. The posters are hung in Department of Mathematics hallways and classrooms for all to see - including students and faculty from other classes who are equally excited to see the many connections. Each poster hangs for a week or more until it is replaced by another student's poster. Over the course of the semester each student's poster has an opportunity to enlighten all those who pass by it. A sign-up sheet insures that all students choose different topics. Over the course of the semester this means a general group of explorers (class) can create a gallery of 30 more connections of mathematics to the arts and to nature!

To keep everybody involved, each poster is self-reviewed, peer reviewed, and reviewed by the teacher. They are evaluated in five categories, which your group may decide to adjust however you see fit. Our categories are:

- An interesting, accessible topic.
- An engaging description and/or illustration of the topic.
- Success in using the topic to aid in our efforts to illustrate the importance of mathematics in the arts or mathematics in nature.
- An appropriate collection of additional information interested readers can use to pursue the topic in greater depth. These may include: book, journal, audio, video, and other media and multi-media citations; Internet resources; museum holdings; maps of nature trails; event dates; etc.

- The physical construction of a high quality poster, including: appropriate design, pleasing visual layout, effectiveness, appropriate mix of media and information, effort, etc.

We have found this to be a wonderful way to share the surprise, beauty, and excitement of mathematics. We invite your group of explorers to try it as well.

TOPIC 3

Primes and Congruences

The positive integers stand there, a continual and inevitable challenge to the curiosity of every healthy mind.

-- G.H. Hardy

It will be another million years, at least, before we understand the primes.

-- Paul Erdos

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

Primes

You'll remember that in the introduction you 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 certainly composite since it is even. In fact, we can *completely factor* 462 as $462 = 2 \times 3 \times 7 \times 11$. 2, 3, 7, and 11 are all factors of 462, as are combinations of these numbers like 6, 14, and 77. This factorization of 462 is called complete because none of the factors can be broken down any further – they are all prime. Naturally, if we start with any composite number, we should be able to factor it, then factor the factors, and then factor these smaller factors, and continue in this way until all of the remaining factors are 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. While mathematicians have long known there are infinitely many primes (see Section 9 of Additional Investigations), they have no idea whether there are infinitely many twin prime pairs or not. In fact, this is a major open question in number theory – solve it and you are a mathematical celebrity.

In fact, not only can every positive integer be written as a product of one or more primes, but this representation is unique up to the order of its factors. This result is called the **Fundamental Theorem of Arithmetic**, and it is truly of fundamental importance. For what it says is that the prime numbers are, via multiplication, the building blocks of the positive integers. As the periodic table of elements serves as the building block for all chemical compounds, the primes serve as the basis for the positive integers.

Mathematicians have long tried to find precise patterns among the primes, and despite some success and fascinating stories like that of "The Twins" (see Investigation Section I 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 continues.

Mersenne Primes

The French monk Father **Marin Mersenne** (1588-1648) was a great facilitator of mathematical communication. He helped mathematics successfully escape from the Dark Ages that had stagnated intellectual life.

In the search for primes, Mersenne suggested that we consider numbers of the form

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

numbers which have since been called **Mersenne numbers** in his honor. Notice that the Mersenne numbers

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

$$M_3 = 2^3 - 1 = 7,$$

$$M_5 = 2^5 - 1 = 31, \text{ and}$$

$$M_7 = 2^7 - 1 = 127,$$

are all prime numbers. One might be tempted to think that the Mersenne numbers are prime whenever the exponent *n* is. But this is something that will require more investigation. (See Investigation Section II below.)

In their hunt for larger and larger primes, mathematicians have developed tests that computers can painstakingly apply in an attempt to determine whether specific Mersenne numbers are prime.

On December 5, 2001, the Great Internet Mersenne Prime Search (GIMPS) volunteers announced that Michael Cameron, a 20 year-old running the software Prime95 on his PC, had shown that the Mersenne number $2^{13,466,917} - 1$ was indeed prime. This prime number, the largest known to date, has 4,053,946 digits when written out in its integer form.

If you would like to be part of this search, and maybe become famous, you can download software at www.mersenne.org /prime.htm . This software runs in background in the lowest priority on your computer, using your computer's capabilities when you are not actively using them.

Fermat Numbers

In a letter to Mersenne, **Pierre de Fermat** (1601-1665), whose monumental contributions to number theory are explored in this and the next topic, 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 $2^{2^n}+1$ the n[th] **Fermat number** and denote it by $F_n = 2^{2^n}+1$. As Fermat noted,

$$F_0 = 2^{2^0}+1 = 3,$$
$$F_1 = 2^{2^1}+1 = 5,$$
$$F_2 = 2^{2^2}+1 = 17,$$
$$F_3 = 2^{2^3}+1 = 257, \text{ and}$$
$$F_4 = 2^{2^4}+1 = 65{,}537$$

are prime. But what about the next two, the whopping $F_5 = 2^{2^5}+1 = 4{,}294{,}967{,}297$ and $F_6 = 2^{2^6}+1 = 18{,}446{,}744{,}073{,}709{,}551{,}617$? Are they really prime?

Clearly it will be quite difficult to work with numbers this large. And there are numbers fabulously larger than this – numbers so large that it will never be physically possible for us to consider them directly, with electronic computers or otherwise – that are important to consider in number theory. Perhaps surprisingly, we can learn a great deal about such numbers indirectly.

Congruences: aka Clock Arithmetic

Fermat, then Euler, **Joseph-Louis Lagrange** (1736-1813), and **Adrien-Marie Legendre** (1752-1833), found clever methods to work with gigantic numbers of the sort considered above indirectly. 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."[23]

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

$$7+11 \equiv 6 \bmod 12$$

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

$$7+11 \equiv 18 \bmod 24.$$

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

$$7+23 \equiv 6 \bmod 24.$$

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

Gauss noticed that we can define congruences like this for any "clock". We say that $7+23 \equiv 6 \bmod 24$ 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 $a \equiv r \bmod m$ 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 **moduli**. In his Disquisitiones, Gauss showed that congruences form perfectly nice arithmetical systems where one can not only add numbers, but subtract and multiply numbers, as well.

Notice that there is a slight inconsistency with the mathematical definition and the description via clocks. Namely, using a clock we would say $5+7 \equiv 12 \bmod 12$ since 5 hours after 7 o'clock is 12 o'clock. Indeed, the numbers on a standard clock are 1 -12. In contrast, when we consider this congruence via remainders we have $5+7 \equiv 0 \bmod 12$ 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 which 0 taking the place of 12. While the mathematicians approach is more appropriate for a deep study of modular arithmetic, for our purposes here either convention will be appropriate.

Application of Congruences

In one of his remarkable insights, Euler "noticed" that the Mersenne number $M_{83} = 2^{83} - 1 = 9{,}671{,}406{,}556{,}917{,}033{,}397{,}649{,}408$ was not prime but rather had 167 as a factor. "Noticing" this is remarkable itself, it seems a unpleasant task to even check that 167 divides this gigantic number. Let's see how we can use congruences to do this.[24]

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 mod167? Well,

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

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

$$2^{16} \equiv 89^2 \pmod{167} \equiv 7921 \pmod{167} \equiv 72 \pmod{167}.$$

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

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

---

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

since $167 \times 169 = 28223$. So $2^{83} - 1 \equiv 1 - 1 \pmod{167} \equiv 0 \pmod{167}$. 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, would not be feasible.

Investigations

I. The Twins

A moving story of arithmetical insight is told by the noted psychologist Oliver Sacks in the chapter "The Twins" from The Man Who Mistook His Wife for a Hat (HarperPerrenial, 1990, pp. 195 - 213.) This story, which was loosely adapted as the main story line to the movie "Rain Man" and is also part of the movie "Awakenings", involves two autistic twins who spoke in prime numbers and recognized numbers and number relationships in everything. 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.

1. What does 37 have to do with 111?

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

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

The pattern of the prime numbers is one of mathematics' most closely held secrets, long sought with almost no progress. Said Euler,

> 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, it is possible that the secret of the primes was known to these twins, but has been lost through efforts made to prevent their "unhealthy communication together... in an appropriate, socially acceptable way," an effort that completely squashed their numerical powers.

II. Mersenne Numbers

4. Which of the Mersenne numbers M_2, M_3, M_4, M_5, and M_6 are prime? Explain.

5. Show that the seventh Mersenne number M_7 is prime.

6. Is the eighth Mersenne number M_8 prime? Explain.

7. Is the ninth Mersenne number M_9 prime? Explain.

8. Based on investigations 4) - 7) make a conjecture which gives conditions on the number *n* which allows you to predict whether the Mersenne number M_n is prime or not.

9. Use your conjecture in 8) to make a conjecture about the primality of the Mersenne number $M_n = 2^n - 1$ when the exponent *n* is even and greater than 2.

10. Notice that $(2^2+1)(2^2-1) = 5 \cdot 3 = 15$, $(2^3+1)(2^3-1) = 9 \cdot 7 = 63$, and, $(2^4+1)(2^4-1) = 17 \cdot 15 = 255$. Use this pattern to give a deductive proof of the conjecture in 9).

11. 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 10) bolster your faith in the validity of your conjecture on 8)?

12. Is the eleventh Mersenne number, $M_{11} = 2^{11} - 1 = 2047$, prime? What does this tell you about your conjecture in 8)?

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. It was not until 1947 that, with the help of the first desk calculators, the primality of all the numbers on this list were determined. Mersenne made only five mistakes out of these 257 numbers – a remarkable accomplishment since these numbers grow so fast, as we have already seen.

One of Mersenne's mistakes was with M_{67}. Mersenne claimed this number was prime. However,

> Edouard 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]

13. How many digits does M_{67} have?

14. How long do you think it might take you to calculate M_{67} by hand?

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

Cameron's record Mersenne prime, $M_{13,466,917}$, described in the text box above, contains 4,053,946 digits when written out in its integer form. The last digits of this number are:
...7729337577307522971483858142577664401546209333491130073855470256259071

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

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

18. 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.

III. Fermat Numbers

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

20. 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?

As discussed later in Topic 4, 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 eliminated the majority of potential factors by analyzing properties potentially successful divisors would be required to have. 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.

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

22. Which of the ten numbers in your answer to 21) are prime?

23. Check to see if any of the primes from your answer to 22) divide F_5. What does this tell you about F_5?

24. Would you be surprised to learn that mathematicians have shown that the next sixteen 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?

IV. (Modular) Arithmetic

25. Reduce each of the congruences below to a number smaller than the moduli, 3:

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

26. Do you see a pattern in your answers to 25)? If so, do you think it will continue indefinitely? Explain why.

27. Reduce each of the congruences below to a number smaller than the moduli, 4:

$$1^3 \pmod{4} \equiv ?$$
$$2^3 \pmod{4} \equiv ?$$
$$3^3 \pmod{4} \equiv ?$$
$$4^3 \pmod{4} \equiv ?$$
$$5^3 \pmod{4} \equiv ?$$
$$6^3 \pmod{4} \equiv ?$$
$$7^3 \pmod{4} \equiv ?$$
$$8^3 \pmod{4} \equiv ?$$
$$9^3 \pmod{4} \equiv ?$$

28. Do you see a pattern in your answers to 27)? If so, do you think it will continue indefinitely? Explain why.

29. Reduce each of the congruences below to a number smaller than the moduli, 5:

$$1^4 \pmod{5} \equiv ?$$
$$2^4 \pmod{5} \equiv ?$$
$$3^4 \pmod{5} \equiv ?$$
$$4^4 \pmod{5} \equiv ?$$

30. Do you see a pattern in your answers to 29)? If so, do you think it will continue indefinitely? Explain why.

31. Reduce each of the congruences below to a number smaller than the moduli, 7:

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

32. Do you see a pattern in your answers to 31)? If so, do you think it will continue indefinitely? Explain why.

33. Reduce each of the congruences below to a number smaller than the moduli, 31:

$$1^{30} \pmod{31} \equiv ?$$
$$2^{30} \pmod{31} \equiv ?$$
$$3^{30} \pmod{31} \equiv ?$$
$$4^{30} \pmod{31} \equiv ?$$

34. Do you see a pattern in your answers to 33)? If so, do you think it will continue indefinitely? Explain why.

35. You should see a pattern to the groups of questions above. See if you can make a conjecture about the identity of congruences of the form

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

under certain conditions on the numbers *a* and *n*.

V. Real Mathematical Magic

A topic in first algebra courses and forwarded email messages proclaiming mathematical "miracles" are algebra magic tricks. Pick a number. Add three to your number. Multiply by four. Now subtract twelve. Divide by four. Presto!! It's your original number. (See e.g. [Jac, pp. 40-43] for this and other number tricks.)

Much more miraculous is the following trick based on the Chinese Remainder Theorem, a result from modular arithmetic known to the ancient Chinese.

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

37. What is your number *x*, from 36), congruent to mod 3? Label your answer as c_1, so we have $x \equiv c_1 \ mod\ 3$.

38. What is your number x, from 36), congruent to mod 5? Label your answer as c_2, so we have $x \equiv c_2 \ mod\ 5$.

39. What is your number x, from 36), congruent to mod 7? Label your answer as c_3, so we have $x \equiv c_3 \ mod\ 7$.

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

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

42. Reduce m mod 105. Surprised?

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

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

45. What is your number x, from 44), congruent to mod 3? Label your answer as c_1, so we have $x \equiv c_1 \ mod\ 3$.

46. What is your number x, from 44), congruent to mod 7? Label your answer as c_2, so we have $x \equiv c_2 \ mod\ 7$.

47. What is your number x, from 44), congruent to mod 11? Label your answer as c_3, so we have $x \equiv c_3 \ mod\ 11$.

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

49. In the expression for m, in 48), what do you think gave rise to the numbers 77, 33, and 21? Explain.[25]

50. Reduce m mod 231. Surprised?

These tricks are direct applications of the *Chinese Remainder Theorem*, a much more general result from number theory that is critical in solving systems of congruences.

[25] The numbers 2, 3, and 10 in this expression are a bit more mysterious. They were chosen so that $77\times2\equiv1 (\text{mod } 3)$, $33\times3\equiv1 (\text{mod } 7)$, 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 $255{,}255=3\times5\times7\times11\times13\times17$ and then ask for the six necessary *moduli*.

TOPIC 4

Partitions

Read Euler, he is our master in all.

-- P.S. Laplace

"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

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

The Births of Modern Number Theory

Throughout this text the work of a great many mathematicians in number theory is mentioned. In every field of mathematics each new generation adds a new story to our understanding of mathematics, and each new generation has many players. Yet in number theory this large cast of players may be a bit misleading for the formative history of number theory is based overwhelmingly on the work of just three mathematicians: Pierre de Fermat, Leonhard Euler, and Carl Friedrich Gauss.

As **Andre Weil** (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].[26]

[26] 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.

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 a wonderful illustration that typifies mathematical growth and development.

However, mathematics is generally presented in schools in its final, polished form. The given topic is hundreds of years old, and generations of mathematicians and teachers have organized and reorganized it into a highly logical, streamlined form. It is certain, if not lifeless. The validity of its results were established via proofs long ago, as were its connections to other areas of mathematics. It is rare that students are provided the opportunity to explore the examples, problems, and issues from which an area of mathematics germinates.

But mathematics almost always begins with examples, problems, and compelling issues. A great deal of work is done before the patterns, insights, and conjectures of one generation are slowly replaced by the deductive proofs of another. And it is generally another generation hence that assembles all of this 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, many generations. He provided few if any proofs, writing his ideas in the margins of Diophantus' Arithmetica. It was Euler, a century later, that provided proofs and generalizations of many of Fermat's most important observations. And, a generation later, it was Gauss that brought the work of Euler together into 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.

Connections Between Fermat and Euler

Fermat Primes

We investigated Fermat primes, prime numbers of the form $2^{2^n}+1$, in Topic 3. Following the work of Euler, you showed that the Fermat primes were not, in fact, all primes. Indeed, we now know that of the first twenty-one Fermat numbers only the first four are primes. Given Fermat's renown, nobody seriously questioned his claim, and it was not until the arrival of Euler that we find someone with significant 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 19) – 23) in Topic 3, is one of the great mathematical discoveries.[27]

The (Mathematical) Key to Modern Encryption

In "(Modular) Arithmetic," Section IV of the Investigations for Topic 3, you studied congruences of the form $a^{n-1}\ (\mathrm{mod}\ n)$. The desired result in investigation 35) in that section is that

$$a^{n-1} \equiv 1\ (\mathrm{mod}\ n)$$

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." While this 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 Frenicle de Bessy** (1605-1675) on 18 October, 1640. Fermat was characteristically glib in providing justification. He told Frenicle, "I would send you the demonstration, if I did not fear its being too long." ([Bur, pp. 88-9])

It was left up Euler to supply the first proof of Fermat's Little Theorem, almost 100 years later, in 1736. But Euler did Fermat one better this time. Not only did he prove Fermat's Little Theorem, he showed that it could be generalized. That is, Fermat's Little Theorem is a special case of a much more general pattern. Euler's Theorem states:

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

whenever *a* and *n* have no common factors. ϕ here is the *Euler phi-function* which will have the value $n - 1$ whenever *n* is prime, thereby yielding Fermat's Little Theorem in that case.[28]

Fermat's Little Theorem, and its generalization to Euler's Theorem, are of no little significance. These results are the fundamental mathematical results on which all modern encryption schemes are based!

Primes and Squares

After the even prime number 2, all primes are odd. If you check, you will easily see that any odd number can 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 **4*k* – 1 primes**.

---

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

[28] In Topic 2 we used the Greek letter phi to denote the Golden Ratio. This same letter is being used here with a totally different meaning and it will always be clear from context which is being denoted for the Golden Ratio is a constant while phi is denoting a function here.

Here, via example, is what Fermat discovered (on Christmas day in 1640[29]) and Euler first proved. The number 29 is a prime, a $4k + 1$ prime since it can be written $29 = 4 \times 7 + 1$. But 29 can also be expressed as $29 = 2^2 + 5^2$. What about the next $4k + 1$ prime, 37? Well, $37 = 4 \times 9 + 1$ and $37 = 1^2 + 6^2$. And the next? $41 = 4 \times 10 + 1$ and $41 = 4^2 + 5^2$. Try a few yourself. What you will find is that every $4k + 1$ prime can be written as the sum of two squares. And it can only be written as the sum of two squares in one way. And what about the $4k - 1$ primes, you ask? Try a few: 3, 7, 11,… You will find that none of the $4k - 1$ primes can ever be written as the sum of two squares.

Sums of Squares

Fermat and Euler were interested in what they could learn about expressing any number as a sum of squares. As the $4k - 1$ primes show, more than two squares will sometimes have to be used. In Section IV of the Investigations for Topic 5, 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 a proof of his was never found. (Surprised?) 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?" Indeed, known as *Waring's Problem*, this is a natural question that is one of the foci of Topic 5 and Topic 6.

Fermat's Last Theorem

Fermat's Last Theorem is one of the two main foci of Topic 6. As mentioned in the introduction, the theorem is the most famous and long-standing problem in all of mathematics. It concerns 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 to the equation when the exponent is $n = 4$. The next documented progress was due to Euler who proved that there were no solutions to the equation when the exponent is $n = 3$. These two results drove mathematicians' quests for this holy grail for more than three centuries.

Partitions

Primality and factorization both arise in the context of multiplication. Of course, since the integers also have addition as an operation,[30] it is natural to wonder whether we can find

[29] [Bur, p. 242].

[30] 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

any patterns in the way integers can be represented as sums of other integers. The section above on sums of squares is one example.

An even simpler possibility is simply to write positive integers 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. But can we find a pattern to this non-uniqueness?

Decompositions of a positive integer into sums of positive integers are now known as **partitions**. Clearly, the partitions of two given above are the only ones, and 1 only has one partition, 1 = 1. Note that the partitions 2 + 1 and 1 + 2 of 3 are considered identical; order does not matter.

The first detailed study of partitions was taken up by Euler in response to queries from the mathematician **Philippe Naude'** (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.

Investigations

I. Enumerating Partitions

1. Find all of the partitions of 3.

2. Use your answer to 1) to complete the following table:

Integer; n	# Partitions; p(n)
1	1
2	2
3	

3. Based on the table in 2), how many partitions of 4 should there be?

4. What kind of reasoning are you using in your answer to 3)?

5. Find all the partitions of 4.

6. Does your result in 5) agree with your conjecture in 3)? What does this tell you about the reasoning that you used to make your conjecture?

---

are related) in which **Erveste Galois** (1811-1832), a famous mathematical prodigy who was killed in a dual at the age of 20, and **Niels Henrik Abel** (1802-1829), another prodigy who died from tuberculosis at age 27, were critical founding figures.

7. Use your answer to 5) to complete the following table:

Integer; n	# Partitions; p(n)
1	1
2	2
3	
4	

8. Find a pattern in the table in 7), and use this table to predict how many partitions of 5 there should be. What kind of reasoning are you using to make this prediction?

9. Find all the partitions of 5.

10. Does your result in 9) agree with your conjecture in 8)? What does this tell you about the reasoning that you used to make your conjecture?

11. Use your answer to 9) to complete the following table:

Integer; n	# Partitions; p(n)
1	1
2	2
3	
4	
5	

12. Find a pattern in the table in 11), and use this table to predict how many partitions of 6 there should be. What kind of reasoning are you using to make this prediction?

II. Counting Strategies

As the number we are investigating becomes larger and larger, the number of partitions increases quickly. To successfully find all the partitions, it is important to have a strategy to insure that none are missed.

13. Find, clearly describe, and then apply a strategy for finding the number of partitions of 6. (Hint: Your strategy can be organizational or mathematical. One mathematical approach uses partitions of a previous number to help build partitions of the next number.)

14. Does your result in 13) agree with your conjecture in 12)? What does this tell you about the reasoning that you used to make your conjecture?

15. Use your answer in 13) to complete the following table:

Integer; n	# Partitions; p(n)
1	1
2	2
3	
4	
5	
6	

16. Find a pattern in the table in 15), and use this table to predict how many partitions of 7 there should be. What kind of reasoning are you using to make this prediction?

17. Find all of the partitions of 7.

18. Does your result in 17) agree with your conjecture in 16)? What does this tell you about the reasoning that you used to make your conjecture?

19. Use your answer to 17) to complete the following table:

Integer; n	# Partitions; p(n)
1	1
2	2
3	
4	
5	
6	
7	

20. Find a pattern in the table in 19), and use this table to predict how many partitions of 8 there should be. What kind of reasoning are you using to make this prediction? (Hint: Consider the differences between successive rows in the table. These differences are called the **first differences** and are a discrete analogy of the *first derivative* which is a central topic in calculus.)

21. Find all the partitions of 8.

22. Does your result in 21) agree with your conjecture in 20)? What does this tell you about the reasoning that you used to make your conjecture?

III. 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. You should notice that none of your "patterns" really continue. Indeed, there is no "simple" pattern. It was not until 1934 that an explicit formula describing this pattern was found -- two centuries after partitions were first significantly considered.[31]

Fill in the missing partitions, being sure to check your results with others in your class.

Integer; n	# Parts; 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

23. Using the table above, find all integers whose number of partitions is a multiple of 5.

24. If you delete some of the numbers from your answer to 23), the remaining numbers fall in a regular pattern, called a *partition congruence mod 5*. Describe this pattern precisely.

25. Do you think that the pattern in 24) continues forever? Explain.

26. Following the example of 23) and 24), find and precisely describe a partition congruence mod 7.

---

[31] This discovery was made by **Hans Rademacher** (1892-1969). This formula is remarkably complex, providing, as a consequence, the "simple *asymptotic*" result that as the integer in question, denoted by the variable *n*, gets closer and closer to infinity the number of partitions of *n* gets closer and closer to $\dfrac{e^{\pi\sqrt{\frac{2n}{3}}}}{4n\sqrt{3}}$, a result which 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 via the *generating function* $\prod_{n=1}^{\infty}\dfrac{1}{1-x^n}$, which is an infinite product (!!) discovered by Euler. See Additional Investigations for more details.

27. Following the example of 23), 24), and 26), 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**, 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."[32]

IV. Amazing New Discoveries

While working through awkward, non-traditional passages in Ramanujan's notebooks in 1999-2000, the mathematician Ken Ono made a remarkable discovery - there are partition congruences for every prime number greater than 3! In other words, in addition to 5, 7, and 11 partition congruences, there are 13, 17, 19, 23,... partition congruences as well! Moreover, he proved this result while only explicitly finding <u>one</u> new partition congruence.

28. In his research Ken Ono only found 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 readily be programmed into computers to generate additional partition congruences.

29. Is it amazing that an undergraduate made such progress on this problem? Explain.

[32] Quoted in [Pet1].

INTERLUDE

Srinivas Ramanujan:

An equation for me has no meaning unless if expresses a thought of God.
-- Srinivas Ramanujan

Srinivasa Iyengar Ramanujan Iyengar, known to most simply as Ramanujan as the other components of his name are surnames borne of various traditions, was born on 22 December, 1887 in the small village of Erode, India. Legend tells Ramanujan's mother became pregnant several years after marriages only after her father prayed to the Goddess Namagiri to bless his daughter with offspring. The son of an accountant, Ramanujan was born into the Brahmin caste - the highest, and most orthodox Hindu, level of the Indian caste system. While he was deeply influenced by the traditions of this caste, his family, like most others in Southern India around this time, survived in relative poverty. Ramanujan was one of six children, three of whom died before their first birthdays. At age two Ramanujan contracted smallpox. Ramanujan survived. He would go on to live a short, often sickly, life. But Ramanujan's life was a life of extraordinary genius which would see him became India's foremost mathematician and a legend for the ages.

Ramanujan started school at age five. While "quiet and meditative", his mathematical abilities were recognized quite early. He had a great ability to repeat all of the formulas and theorems he had been taught. He could recite the digits of pi and the square root of two to as many places as listeners could bear to hear. The apparently critical moment in Ramanujan's mathematical development was at age 15 when he finally came into possession of a significant book of mathematics - A Synopsis of Elementary Results in Pure and Applied Mathematics by George S. Carr. This was a lengthy, two volume compendium that contained many of the important mathematical results through the middle part of the nineteenth century. It was hardly a text from which one could learn - it was very terse, almost dictionary like. Yet Ramanujan set out to understand and establish all of the results in this text on his own. His obsession with mathematics kept him from fulfilling the scholarships that he had won to government colleges. He was inseparable from the two large notebooks that he filled with his mathematical ideas. Ramanujan would later claim that his inspirations came in the form of dreams from the Goddess Namakkal.

In the early part of 1909 Ramanjuan became quite ill. Later that year Ramanujan was married in an arranged marriage. He would not live with his wife, age nine, until she turned twelve. Throughout this time Ramanujan unwillingly accepted financial support from local benefactors so he could pursue his mathematics ruminations. One such benefactor described him as “Miserably poor... A short uncouth figure, stout, unshaved, not overclean, with one conspicuous feature - shining eyes... He never craved for any distinction. He wanted ... that simple food should be provided for him without exertion on his part and that he should be allowed to dream on.” When Ramanujan tired of this support he became an office clerk. But at each opportunity he sought to share his mathematical work with others who might be in a position to judge or appreciate it.

On the heals of several fortuitous introductions, Ramanujan was encouraged enough to write to G.H. Hardy - then a Fellow at Trinity College, Cambridge and who would become one of the twentieth century’s most famous mathematicians. Ramanujan’s letter, dated 16 January, 1913, is a picture of modesty:

> I beg to introduce myself to you as a clerk in the Accounts Department... I have no university education... but I am striking out a new path for myself... The results I get are termed by the local mathematicians as “startling”... [Yet] the local mathematicians are not able to understand me in my higher flights... I would request you to go through the enclosed papers. Being poor, if you are convinced that there is anything of value I would like to have my theorems published... Requesting to be excused for the trouble I give you, I remain, Dear Sir, Yours truly, S. Ramanujan.

The letter included more than 100 theorems that Ramanujan had discovered. They are fabulously intricate wonders such as:

$$1-5\left(\frac{1}{2}\right)^3+9\left(\frac{1\cdot 3}{2\cdot 4}\right)^3-13\left(\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\right)^3+\ldots=\frac{2}{\pi}$$

$$\int_0^\infty \frac{1+\left(\dfrac{x}{b+1}\right)^2}{1+\left(\dfrac{x}{a}\right)^2}\,\frac{1+\left(\dfrac{x}{b+2}\right)^2}{1+\left(\dfrac{x}{a+1}\right)^2}\cdots dx=\frac{1}{2}\sqrt{\pi}\,\frac{\Gamma(a+1/2)\,\Gamma(b+1)\,\Gamma(b-a+1/2)}{\Gamma(a)\,\Gamma(b+1/2)\,\Gamma(b-a+1)}$$

where the ellipsis ... means that the operation is continued indefinitely to infinity.

Hardy would later try to reconstruct what it felt like for a professional mathematician to receive a “letter like this from an unknown Hindu clerk.”

> The first question I asked myself was whether I could recognize anything. I had proved things rather like [equation] (1.7) myself, and seemed vaguely familiar with (1.8)... I thought that as an expert in definite integrals, I could probably prove (1.5) and (1.6), and did so, though with a good deal more trouble than I had expected...
>
> The series formulae (1.1) - (1.4) I found much more intriguing... [One is well-known,] but the others are much harder then they look...
>
> The formulae (1.10)-(1.13) are on a different level and obviously both difficult and deep... (1.10)-(1.12) defeated me completely; I had never seen anything in the least like them before. A single look at them is enough to show that they could only be written down by a mathematician of the highest class. They must be true because, if they were not true, no one would have had the imagination to invent them.

Hardy immediately arranged for Ramanujan to come to England. Yet the prejudices of India’s caste system made Ramanujan feel that he could not accept Hardy’s invitation to come to Cambridge. Moreover, Ramanujan’s mother would not give her consent. Hardy made every effort to encourage him to come to Cambridge, even enlisting his friends as allies. While he was able to sway Ramanujan, it was not until Ramanujan’s mother announced that “she had had a dream on the previous night, in which she saw her son seated in a big hall amidst a group of Europeans, and that the goddess Namagiri had commanded her not to stand in the way of her son fulfilling his life’s purpose.” On 17 March, 1914 Ramanujan sailed to England. In April he was admitted to Trinity College - a remarkable honor.[33]

But what would be done with Ramanujan? As Hardy remarked, “The limitations of his knowledge were as startling as its profundity.” How do you teach somebody whose mathematical talents in a few narrow areas far surpass those of all living mathematicians, but is completely ignorant of so many important areas of mathematics - even those that might aid in his own area of interest? But Hardy succeeded, and both mathematicians flourished under their collaboration. Hardy reported, “I learnt from his much more than he learnt from me... His flow of original ideas shewed no symptom of abatement.”

Yet outside of mathematics Ramanujan did not prosper as well. He had a very difficult time adjusting to life in England. He was a strict vegetarian. He cooked all of his food himself and had difficulty obtaining food that was compatible with his usual diet. The climate of England was totally different from his native India. The stone buildings of Trinity College were cold and damp. Never having encountered such cold, Ramanujan slept in his overcoat, wrapped in a shawl. It was not until a fellow Indian student at Trinity realized that Ramanujan did not understand the purpose of the many blankets spread neatly on his bed that Ramanujan learned to lift up the blankets and slide under them to keep warm. England joined

---

[33] To quote Ramanujan's biographer Kanigel [Kan], "Among all of the colleges of Cambridge University, Trinity was the largest with the most lustrous heritage, home to kinds, poets, geniuses. Issac Newton himself had studied there... Lord Byron had gone to Trinity. So had Tennyson, Thackeray, and Fitzgerald. So had the historian Macaulay, and the physicist Rutherford, and the philosopher Bertrand Russell. So had five English prime ministers."

World War I. Trinity College housed open air hospitals for wounded soldiers and adequate vegetarian food became harder to come by. Ramanujan was often sick. In the spring of 1917 he became particularly ill. He was diagnosed with tuberculosis and placed in a sanatorium. Despite his illness, his impact spread and his reputation grew. In May of 1918 he was elected as a Fellow to the Royal Society - one of the highest academic honors of the time. His election was all the more remarkable as it came on a first ballot, was the first time an Indian had been so honored, and it came at the remarkably young age of 30. Several other major honors were also bestowed on him during this year. These honors seemed to have buoyed his health for a short time and he continued to develop beautiful and important mathematical discoveries.

Early in 1919 his health worsened again. He returned to India where he died on 26 April, 1920 at the age of 33. He had no children. He was survived by his wife and his parents.

The richness of Ramanujan's mathematical legacy is in sharp contrast to trials of his brief and difficult life. Ramanujan's own published works are of sufficient importance to consider him one of the elite mathematicians of the twentieth century. But his impact did not stop there. He left many notebooks full of unpublished theorems, results, and ideas. These notebooks have been intensely studied by mathematicians and have resulted in hundreds of papers whose contributions are direct results of the work laid out by Ramanujan. Indeed, almost eighty years later, the notebooks of Ramanujan served as the impetus of the major new discovery by Ken Ono that you investigated in Topic 5. Ono says that while he "was familiar with a lot of what he had done through the writings of more modern mathematicians, I didn't suspect that I would learn anything from studying Ramanujan's notes." However, one mathematical identity, written in a particularly obtuse fashion, even for Ramanujan, struck Ono. "This can't be right." Yet it was. This one identity helped Ono establish "spectacular" results that are "the most important work on partition congruences since the epic work of Ramanujan" and among the most notable of the past decade. Ono "learned a valuable lesson. It sometimes really pays to read the original." [Pet1] Who knows how many other mathematical gems are still unearthed in Ramanujan's notebooks.

In his biography of Ramanujan, the biographer Kanigel [Kan] tells us Ramanujan's is:

> A story of one man and his stubborn faith in is own abilities. But it is not a story that concludes, *Genius will out* -- though Ramanujan's, in the main, did. Because so nearly did events turn out otherwise that we need no imagination to see how the least bit less persistence, or the least bit less luck, might have consigned him to obscurity. In a way, then, this is also a story about social and educational systems, and about how they matter, and how they can sometimes nurture talent and sometimes crush it. How many Ramanujans, his life begs us to ask, dwell in India today, unknown and unrecognized? And how many in America and Britain, locked away in racial or economic ghettos, scarcely aware of worlds outside their own?

Investigations

1. Perspectives on Ramanujan

The wonderful mathematical expositor **Martin Gardner** (??-) reminds us:

> Biographical history, as taught in our public schools, is still largely a history of boneheads; ridiculous kings and queens, paranoid political leaders, compulsive voyagers, ignorant general - the flotsam and jetsam of historical currents. The men who radically altered history, the great scientists and mathematicians, are seldom mentioned, if at all.

The story of Ramanujan offers a perfect context to study the historical connections between Britain and India, Indian culture, English culture, academic culture in the late nineteenth century, the impact of World War I on European daily life, differences in learning styles, and many other interesting issues. So bring the story of Ramanujan into your other classes to share. See if the world looks different seen through the lens of one of the great mathematicians of the twentieth century.

II. A Gallery of Contemporary Mathematicians

Throughout this text the names of mathematicians have appeared in bold. Hopefully this has come to help you see that mathematics is a very human science with a huge cast of characters. Mathematics is not simply the work of a few greats like Euclid, Pythagoras, Newton, and a few others whose names are well-known. As mathematical accomplishment grew dramatically in the twentieth century, its success and the identity of its pioneers became less and less well-known. Most people would be embarrassed if they could not name several influential twentieth century artists, authors, politicians, or even scientists. Yet few can name a twentieth century mathematician other than John Nash who was portrayed in a the hit Hollywood movie <u>A Beautiful Mind</u> [How]. This is quite unfortunate and is something your group of explorers (i.e. class) might consider addressing by creating a gallery of biographies of contemporary mathematicians - one done by each explorer.

You should see from the dates that follow the names of the mathematicians listed in this text that there is a huge case of twentieth century mathematicians. The biography section of the MacTutor History of Mathematics Archive (available at www-groups.dcs.st-and.ac.uk:80/~history/BiogIndex.html) has referenced biographies of over 400 mathematicians born since 1900 and hundreds more who were born before 1990 but whose major accomplishments were in the twentieth century.

For those of you who have not ever seen a poster session, they are widely used to publicize, announce, and/or present the results of research investigations. They are used in professional conferences (including virtually all conferences for mathematicians and scientists), college and university courses, and meetings of all kinds. They are useful because many posters can be displayed without the time and space limitations that traditional presentations impose. Additionally, it makes it easier for participants to browse and find research of interest.

At our college we have created a gallery of biographical posters each celebrating the life of contemporary mathematician. The posters are hung in Department of Mathematics hallways and classrooms for all to see - including students and faculty from other classes who are equally excited to see the many connections. Each poster hangs for a week or more until it is replaced by another student's poster. Over the course of the semester each student's poster has an opportunity to enlighten all those who pass by it. A sign-up sheet insures that all students choose different mathematicians. Over the course of the semester this means a general group of explorers (class) can create a gallery of 30 mathematicians to supplement the single biography that appears in this text.

To keep everybody involved, each poster is self-reviewed, peer reviewed, and reviewed by the teacher. They are evaluated in five categories, which your group may decide to adjust however you see fit. Our categories are:

- An informative presentation of biographical data.
- An engaging portrayal of the subject as a human being whose life and work everybody can learn from.
- Success in using the subject's biography to aid in our efforts to demonstrate that mathematics is a vital, living, dynamic, and humanistic discipline.
- Accessible description(s) of the subject's mathematical contributions, impact on the field of mathematics, leadership in the community of mathematicians, broader intellectual impact, and/or broader societal impact.
- A physical construction of a high quality poster, including: appropriate design, pleasing visual layout, effectiveness, appropriate mix of media and information, effort, etc.

We have found this to be a wonderful way to share the human component of mathematics. We invite your group of explorers to try it as well.

TOPIC 5

Power Partitions

The only way to learn mathematics is to do mathematics
-- Paul Halmos

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

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 he think.
-- John Dewey

Another Story about Gauss

Some of the remarkable accomplishments of the prodigy Gauss have already been told. We start here with another story of his mathematical precociousness.

It is sometimes reported that as a child of three Gauss corrected errors in his father's payroll calculations.[34] More often repeated, and more widely accepted, folklore involves a "busywork" problem that an elementary school teacher assigned Gauss and his schoolmates. The problem was to find the sum of the numbers between one and one-hundred and write the correct answer on their slate. In other words, on small slates the students were to compute the sum

$$1 + 2 + 3 + \ldots + 98 + 99 + 100.$$

Gauss answered almost immediately; 5050.

Mathematics Manipulatives

Gauss noticed a pattern that can be nicely illustrated by *mathematical manipulatives* – concrete, physical objects that are used for hands-on exploration – that are widely used in contemporary elementary mathematics classrooms.

The manipulatives used here are simply small cubes of a uniform size which can be snapped together; they are sold under the names **Multi-link Cubes®** and **Unifix Cubes®**. If

[34] See, e.g., [Bur, p. 510].

you have access to these manipulatives, you should grab a pile and explore with them as you read.

So we can provide illustrations, we begin with a smaller version of Gauss' problem -- find the sum of the numbers between one and eight. We can represent each of the *summands* concretely using the cubes:

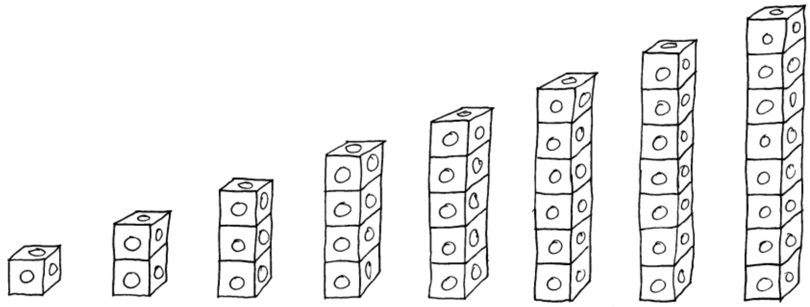


Fig. 5.1 The numbers 1 – 8 concretely as Multi-link Cubes®.

Snapping our cubes together, the sum of these numbers -- the answer to our problem -- is simply the number of cubes in the "staircase" pictured in Fig. 5.2. This does not seem like much help until one notices that if we take two of these staircases, then they will fit together perfectly into one rectangle. See Fig. 5.3. And it is a simple matter to find the number of cubes that make up this rectangle – it is simply the area of the rectangle: base (8) times height (9), which equals 72 cubes.

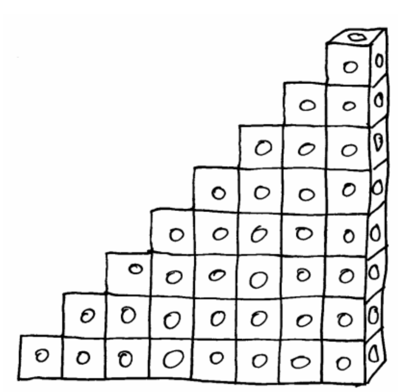


Fig. 5.2 The $1 + 2 + \ldots + 7 + 8$ staircase.

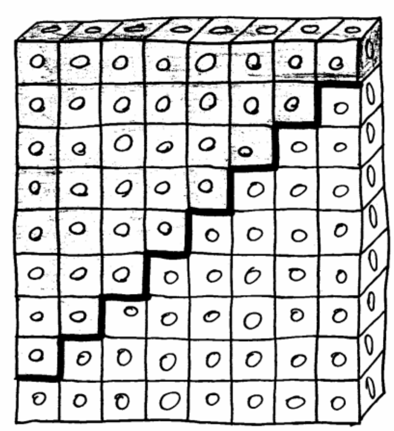


Fig. 5.3 Two $1 + 2 + \ldots + 7 + 8$ staircases.

Since we only wanted the number of cubes in one staircase, our answer is half this many. In other words, using these manipulatives we have just shown that

$$1+2+3+4+5+6+7+8=\frac{8\times 9}{2}=\frac{72}{2}=36.$$

Of course, finding the sum of the first eight numbers is not a lofty undertaking. What is important about this example is the idea or strategy on which it is based for the idea can be applied to many variations of this problem - the least of which is Gauss' problem. Go ahead; use this idea to show that Gauss was right, that

$$1 + 2 + 3 + ... + 98 + 99 + 100 = 5050.$$

What other Gauss-like challenges might you find eight- and nine-year old children solving in contemporary mathematics classrooms with their brightly colored manipulatives? Well, you might find them determining the sums of any of the following *arithmetic series*:

$$1 + 4 + 7 + ... + 34 + 37 + 40 = ?$$

$$1 + 5 + 9 + ... + 93 + 97 + 101 = ?$$

$$5 + 8 + 11 + ... + 21 + 24 + 27 = ?$$

Try it on your own with manipulatives. Examples like these should help you gain a sense of how empowering simple mathematics manipulatives, like little, colored, attachable cubes, are.

And, while you have a pile of manipulative cubes in front of you, you might also consider a question that will be one of the main foci of the next topic:

> Can you make a large cube out of your cubes that can be rearranged into exactly two smaller cubes using no extra pieces and with none left over?

Proofs Without Words

Anyone who has lived through a high-school geometry course, where the dominant mode of communication was the veritable *two-column proof*, might agree with English astronomer Sir Arthur Eddington (1882-1944) who said:

> Proof is an idol before which the mathematician tortures [her]himself.

Yet, a much more appropriate view of proof is that of Andrew Gleason who said:

> Proofs really aren't there to convince you that something is true -- they're there to show you why it is true,

or of Gian-Carlo Rota 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 style of mathematical proof that is much more convincing than two-column geometry proofs is something mathematicians call *Proofs Without Words*.

Let's add up consecutive odd numbers starting at 1,

$$1 = 1$$
$$1 + 3 = 4$$
$$1 + 3 + 5 = 9$$
$$1 + 3 + 5 + 7 = 16.$$

Notice a pattern? All of the answers are squares! You can use Multi-link Cube® staircases here as we did above since each of these series is an arithmetic series. But you can also use Multi-Link Cubes® in a different way to see why the sum of each of these series must be a square:

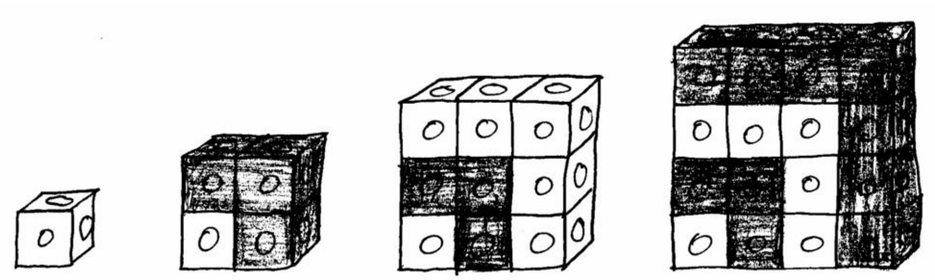


Fig. 5.4 Proof without Words – Sums of Odds.

Certainly, this proof lives up to the ideal of Gleason and Rota. While they use mathematics manipulatives that would make Maria Montessori proud, they should not be considered a learning tool only for the young. "Proof without Words" is a regular column in some of the most widely read mathematics journals, and two full length books containing exemplary examples of these proofs have been published.[35]

Closer to our study of partitions, one finds many proof without words type arguments in mathematical texts and research papers. For example, we can represent partitions graphically:

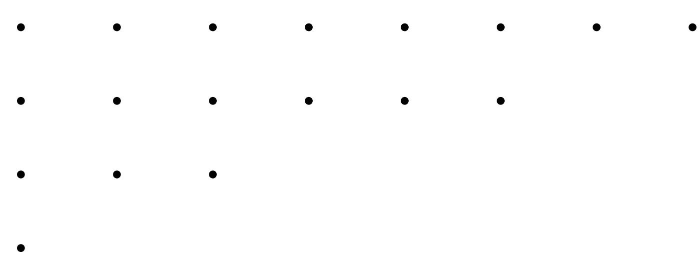


Fig. 5.5 Two partitions of 18.

Fig. 5.4 gives two partitions of the number 18: 18 = 8 + 6 + 3 + 1 reading horizontally and 18 = 4 + 3 + 3 + 2 + 2 + 2 + 1 + 1 reading vertically. These partitions are called *conjugate*

[35] The journals are *American Mathematical Monthly*, *Mathematics Magazine*, and *The College Mathematics Journal*. The books are <u>Proofs without Words</u> and <u>Proofs without Words II</u> both edited by Roger B. Nelsen. All are published by the Mathematical Association of America.

partitions. Figures such as this provide the critical insight in proving the *Rogers-Ramanujan Partition Identity*.[36] In Hardy and Wright's classic text [HaWr] diagrams such as:

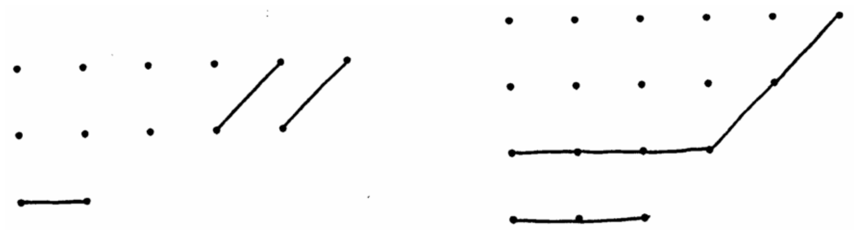


Fig. 5.6 Partition diagrams.

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 figure:

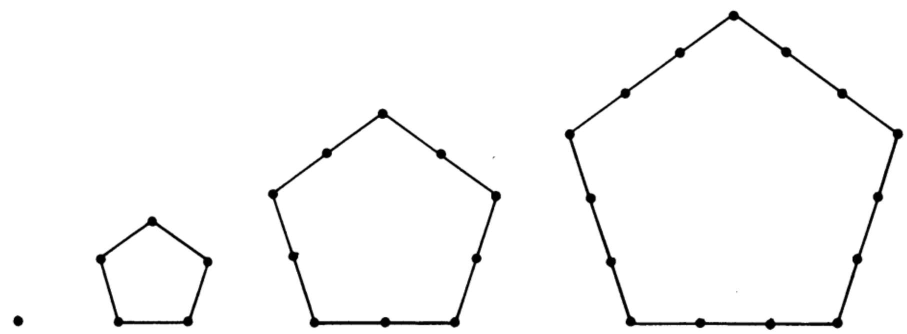


Fig. 5.7 Pentagonal numbers.

Mathematicians, it seems, would be perfectly at home in a progressive, elementary school mathematics classroom with young children exploring all sorts of patterns via Multi-link Cubes®.

Investigations

I. Interesting Numbers

Earlier in this chapter we read about the great English mathematician G.H. Hardy and the prodigy Srinivas Ramanujan. As noted, 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.

[36] 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.

It is the smallest number that is expressible as the sum of two cubes in two different ways."

1. Make a table of the first dozen cubes.

2. Use this table to write the number 1729 as the sum of two cubes.

3. Use this table to write the number 1729 as the sum of two cubes different from those used in investigation 2).

4. Are your solutions to investigations 2) and 3) partitions? If so, is there a word that would describe precisely what type of partitions they are?

5. How remarkable is it that Ramanujan knew this about the number 1729? What does it tell you about his fluency with numbers?

II. Square Partitions

In the story above about the number 1729 Ramanujan was concerned with both the *number* of cubes used to provide a sum of 1729 and the *number* of ways in which this can 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.

6. The numbers $1=1^2$, $4=2^2$, $9=3^2$,... are called *perfect squares*. Define the term *perfect square*.

7. Write out 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**.

8. Find all of the square partitions of the numbers 1 - 8.

9. Use your answers to 8) to complete the following table:

Integer; n	# Square Partitions; s(n)
1	1
2	1
3	1
4	
5	
6	
7	
8	

10. Find a pattern in the number of square partitions and use it to predict the number of square partitions for the numbers 9 - 12.

11. Find all of the square partitions of 9.

12. Does your result in 11) agree with your conjecture in 10)? What does this tell you about the type of reasoning you used to make this prediction?

13. If you continued to look for patterns in the square partitions, how successful do you think your efforts might be in comparison to those in Topic 4 for regular partitions? Explain.

III. Cubical Partitions

14. Find all of the cubical partitions of the numbers 1 - 18.

15. Use your answers to 14) to complete the following table:

Integer; n	# Cubical Partitions; c(n)
1	1
2	1
3	1
4	
⋮	
18	

16. Do you think there is an indefinitely repeating pattern in the number of cubical partitions? 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 these not yet answered after intensive study. So let us turn to a different problem suggested by the story of Ramanujan and 1729.

IV. Minimal Square Partitions

In the story above about Ramanujan, 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 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, … are quite special for they have square partitions where only one term needs to be added: e.g. $1 = 1^2$, $4 = 2^2$, and $9 = 3^2$. 8 is not a perfect square, but it has a square partition with two terms; i.e. it can be written as the sum of two squares: $8 = 2^2 + 2^2$.

17. 3 is not a perfect square; can it be written as the sum of two squares? If not, what is the smallest number of squares needed to write 3 as a sum of squares?

18. 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		

19. Is there a clear pattern to the number of terms in the minimum square partitions? Explain.

20. What was the largest number of terms that were needed from all of the minimum square partitions in the table in investigation 18)?

Let us call the number which answers investigation 20) **Waring's number for square partitions** and denote 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.

21. Does the number 19 have a square partition involving W_2 or fewer terms?

22. Does the number 32 have a square partition involving W_2 or fewer terms?

23. Does the number 57 have a square partition involving W_2 or fewer terms?

24. Does the number 79 have a square partition involving W_2 or fewer terms?

25. Does the number 187 have a square partition involving W_2 or fewer terms?

26. 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** (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.

27. 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** (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 Bachet never had a full proof and Fermat, writing in the margins of a copy of Diophantus' book <u>Arithmetica</u>, *wrote that he had a proof but never wrote it down*.

In 1772 Lagrange published a full proof which 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.[37]

28. Complete the statement of Lagrange's theorem on square partitions below:

<u>Theorem</u> (Lagrange; 1772) Every positive integer can be written as the sum of ______________________________ squares.

V. 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 the like. In fact, this *generalization* was first explicitly considered by the English mathematician **Edward Waring** (1741-1793) in 1770 in his book <u>Meditationes Algebraicae</u>. His conjecture, that a similar result holds for all power partitions, has become known as **Waring's problem**. We explore it for cubical partitions below.

29. Use your results from investigations above 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
⋮	⋮	⋮
18		

30. Is there are clear pattern to the number of terms in the minimum cubical partitions? Explain.

[37] E.g. Chapter 12 of [Bur].

31. What was the largest number of terms that were needed from all of the minimum cubical partitions in the table in investigation 29)?

Just as above, let us call the number we are looking for **Waring's number for cubical partitions** and denote it by W_3.

32. Do you think that the number you found in investigation 31) is W_3? Explain.

33. Does the number 43 have a cubical partition involving the number of terms considered in 31) or fewer?

34. Does the number 81 have a cubical partition involving the number of terms considered in 31) or fewer?

35. Does the number 107 have a cubical partition involving the number of terms considered in 31) or fewer?

36. Do you think you know what W_3 is? Explain.

37. Does the number 23 have a cubical partition involving the number of terms considered in 31) or fewer? If not, what is the number of terms in the minimum cubic partition?

38. Does the number 239 have a cubical partition involving the number of terms considered in 31) or fewer? If not, what is the number of terms in the minimum cubic partition?

39. Do you think you know what W_3 is? Explain.

40. Would it surprise you if I told you that it had been proven deductively that 23 and 239 were the only positive integers that required this many terms to be cubically partitioned? Explain.

In fact, it was proven in 1939 by **Leonard Eugene Dickson** (1874-1954) that you will never need more cubes to cubically partition any positive integer than you needed in investigations 37) and 38) above.[38] In other words, we know exactly what W_3 is. And, if it wasn't for the two anomalies 23 and 239, the number you found in investigation 31) would be W_3.

VI. Solving Waring's Problem

Waring's problem concerns higher and higher powers ad infinitum and we have seen that the work of many prominent mathematicians only settled the problem up to the power

[38] 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.

$n = 4$. 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** (1862-1943), one of the twentieth century's greatest mathematicians. Hilbert "solved" Waring's problem by *proving* that there is always a number W_n so that every positive integer can be partitioned by W_n or fewer n^{th} powers. Interestingly, Hilbert's proof was an *existence proof* – it proved that these W_n existed for every n without telling you what the W_n actually were!

41. 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.

42. Fill in the following chart for the first three Waring numbers:

Partitions	Waring Number, W_n
Integer	$W_1 =$
Square	$W_2 =$
Cubic	$W_3 =$

43. Use 42) to make a conjecture about the remaining Waring numbers.[39]

44. In fact, it was determine in 1986 that the fourth Waring number is $W_4 = 19$. Does this result agree with your conjecture in 43)? Do you have any confidence that you might be able to find a pattern in the Waring numbers considering this new information? Explain.

45. While mathematicians believe they finally have found a pattern, albeit a fabulously complicated one, that does predict the full pattern, they have been unable to completely prove this result.[40] Is this surprising to you? Explain.

46. What does investigation 45) suggest to you about how much is known about the positive integers, the "simplest" part of mathematics?

[39] Determined precisely only in 1986!

[40] The pattern is $W_n \approx 2^n + \text{Int}((3/2)^n) - 2$. This pattern is explored more fully in the section "Euler's formula for Waring numbers" in the Additional Investigations.

TOPIC 6

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

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 sequence of figures below, which actually provide a deductive proof of this theorem.[41] Although this theorem is, by name, attributed to

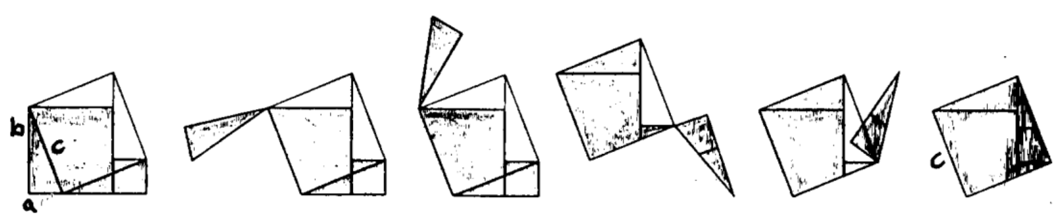


Fig. 6.1 Proof without words: The Pythagorean Theorem

the most famous of all mathematicians -- Pythagoras -- it was well-known by many other ancient cultures. The Babylonian clay tablet known as Plimpton 322, which dates to about 1700 B.C., shows clearly that this culture was aware of the *Pythagorean* theorem more than one-thousand years before the birth of Pythagoras.

[41] From Discovering Geometry by Michael Serra, Key Curriculum Press, 1997.

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![42] One notable proof was found by Ohio Congressman James A. Garfield who went on to be the 20^{th} President of the United States.

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.

Pythagorean Triples as Partitions

There is a close connection of such triples to earlier results we have been considering in this section. 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 <u>all</u> partitions of a given type. For example, in Investigation Section IV of Topic 5 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 $1^2 + 1^2 + ... + 1^2$ is quite boring -- any number can be square partitioned in such a way. In discovering Waring's problem in the previous Topic, 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? You will investigate this question below.

[42] <u>The Pythagorean Propostion</u> by E.S. Loomis, National Council of Teachers of Mathematics.

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. 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 *Fermat’s 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 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**.

Investigations

I. Pythagorean Triples

1. Explain why the figures that make up Fig. 6.1 provide a deductive proof of the Pythagorean theorem, supplying any missing details as necessary.

2. Use your table of squares from Investigations Section II from Topic 5 to find all Pythagorean triples involving positive integers none of which are greater than 20.

3. In investigation 2) you should have found 6 Pythagorean triples. Have you found these triples inductively or deductively? Explain.

II. Consecutive and Other Special Pythagorean Triples

We'd like to learn as much as we can about Pythagorean triples. It is natural to look for patterns.

The Pythagorean triple 3, 4, 5 is interesting because the numbers are consecutive.

4. Based on your search of the table of squares in investigation 2), do you think there is another *consecutive* Pythagorean triple? Explain.

5. 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.
6. Use your expressions in investigation 5) to express the Pythagorean theorem only in terms of the unknown x. Simplify your equation as much as possible.

7. Solve the equation in investigation 6) to determine the unknown x.

8. What do your results from investigations 4) – 7) tell you about the number of consecutive Pythagorean triples? Does it tell you this inductively or deductively? Explain.

9. Can a Pythagorean triple consist of all even numbers? Explain.

10. Can a Pythagorean triple consist of all odd numbers? Explain.

11. How many different Pythagorean triples do you think there are? Explain.

12. 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.

13. Extending the pattern in problem 12, find a dozen Pythagorean triples in the family *generated* by 3, 4, 5.

14. Denoting a by $3x$, where x is any positive integer, prove deductively that there are in fact infinitely many Pythagorean triples in the family generated by 3, 4, 5.

III. Characterizing Pythagorean Triples

In their studies of Pythagorean triples both Euclid, in his Elements, and Diophantus, in his Arithmetica, investigated what amounted to the following algebraic parameterizations:

$$a = 2mn \qquad b = m^2 - n^2 \qquad c = m^2 + n^2,$$

where $m > n$ are both positive integers.

15. Complete the following chart based on the parameterizations given above.

m	n	$a = 2mn$	$b = m^2 - n^2$	$c = m^2 + n^2$	a, b, c = Pythagorean triple?
2	1	4	3	5	Yes
3	1				
3	2				
4	1				
⋮	⋮				
5	4				

16. Do you believe that this pattern will continue indefinitely? On what type of reasoning are you basing your conclusion?

17. Prove algebraically that the parameterizations yield a Pythagorean triple for every appropriate value of m and n.

18. Do you think that the parameterization above accounts for all possible Pythagorean triples? Check all of the Pythagorean triples you found in Investigation 2) and see whether they are accounted for by this parameterization.

The parameterization above was known before the birth of Christ. However, it was not known until much later that it indeed accounted it for all *primitive* Pythagorean triples. This definitive result was, as far as we know, first established by Fibonacci in his 1225 A.D. text Liber Quadrotorum.

IV. 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 V of Topic 5, 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.

19. Can the cube $27 = 3^3$ be partitioned into the sum of two cubes? Explain.

20. Can the cube $64 = 4^3$ be partitioned into the sum of two cubes? Explain.

21. Can the cube $125 = 5^3$ be partitioned into the sum of two cubes? Explain.

22. Can the cube $216 = 6^3$ be partitioned into the sum of two cubes? Explain.

23. Can the cube $343 = 7^3$ be partitioned into the sum of two cubes? Explain.

24. Can the cube $512 = 8^3$ be partitioned into the sum of two cubes? Explain.

25. Do you think that there is <u>any</u> 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 $a^3 + b^3 = c^3$.

Since 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.

26. Show that 6^3 can be partitioned into the sum of three cubes.

Over time many prizes have been offered for solutions to Fermat's Last Theorem. For example, an English doctor named **Paul Wolfskehl** (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.[43]

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** (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 them to his students to fill in the missing numbers."[44]

[43] 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.

[44] From <u>Elementary Number Theory</u> by Underwood Dudley, W.H. Freeman and Co., p. 136.

V. 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.

27. Make a table of the first dozen quartics.

28. Can any of the quartics in the table in 27) be partitioned into the sum of two other quartics? Explain in detail.

29. 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 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![45]

30. 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?

VI. Euler's Conjecture

31. Can the quartic $2401 = 7^4$ be partitioned into the sum of three quartics? Explain.

32. Can the quartic $4096 = 8^4$ be partitioned into the sum of three quartics? Explain.

33. Can the quartic $6561 = 9^4$ be partitioned into the sum of three quartics? Explain.

34. Do you think that there is <u>any</u> quartics that can be partitioned into the sum of three other quartics? Explain.

35. Use the following computations, done with the help of the mathematical software *Scientific Workplace*, to show that the quartic $353^4 = 15{,}527{,}402{,}881$ can be partitioned as the sum of four quartics:

$$353^4 = 15{,}527{,}402{,}881$$
$$315^4 = 9{,}845{,}600{,}625$$
$$272^4 = 5{,}473{,}632{,}256$$
$$120^4 = 207{,}360{,}000$$

36. Use your observations in investigations 25), 26), 29), and 31) – 35) to complete the following conjecture due to Euler:

[45] "Fermat's Last Theorem and modern arithmetic", by K.A. Ribet and B. Hayes, *American Scientist*, vol. 82, March-April 1994, pp. 144-56.

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 ____________________________ terms.[46]

37. If Fermat's Last Theorem is true, does the truth of Euler's conjecture follow as a consequence? Explain in detail, using specific exponents to illustrate the connections and/or differences.

38. If Euler's conjecture is true, does the truth of Fermat's Last Theorem follow as a consequence? Explain in detail, using specific exponents to illustrate the connections and/or differences.

VII. 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** (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 celebre!

M. Leblanc was, in fact, **Sophie Germain** (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. At a 1 March, 1847 meeting of the Paris Academy, the French mathematician **Gabriel Lame** (1795-1870)

[46] See, e.g., History of the Theory of Numbers, vol. II, by L.E. Dickson, New York, 1934.

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** (1810-1893) not only found explicit examples where Lame's proof broke down, but he 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 $n > 4{,}000{,}000$.[47] 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.

39. Given the long, fruitless search for counter-examples, do you suppose that mathematicians were content with the apparent truth of these conjectures? Explain.

VIII. A Breakthrough

40. Complete the following quintic partition into a sum of four terms of the quintic 144^5 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 40) was discovered by **L.J. Lander** (??) and **T.R. Parkin** (??) in 1966.[48]

41. How do you think Lander and Parkin discovered the result illustrated in investigation 40)?

42. What does the result in investigation 40) tell us about Fermat's Last Theorem? What does it tell us about Euler's conjecture?

In 1988 **Noam D. Elkies** (1966 -)[49] discovered that

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

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:

---

[47] See Ribet and Hayes referenced above.

[48] "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.

[49] "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.

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

43. What do these results tell us about Fermat's Last Theorem? What do they tell us about Euler's conjecture?

44. 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 40) above?

45. 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** (1927 – 58), **Goro Shimura** (1930 -), Elkies, Frye, **Robert Langlands** (1936 -), **Gerd Faltings** (1954 -), **Jean-Pierre Serre** (1926 -), **John Coates** (1945 -), **Peter Sarnak** (1953 -), **Nicholas Katz** (1943 -), **Karl Rubin** (1956 -), **Barry Mazur** (??), **Ken Ribet** (1948 -), **Richard Taylor** (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.

IX. A Truly Remarkable Proof[50]

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 Oxford, 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."

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*.

[50] 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].

Stories appeared in *Time*, *Newsweek*, and print media throughout the world. Wiles was named one of *People Magazines* "25 Most Interesting People."

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:

> 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** (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."[51]

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
> 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.

X. Perspectives on These Historic Accomplishments

46. The title of this lesson 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.

47. 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?

48. 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?

49. 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.

[51] [LySin].

Additional Investigations

(??Development ongoing??)

What follows is a collection of additional investigations. They are topics that are adjacent to the path pursued in the body of this text, they simply were not included there either for the sake of judiciousness or due to the fact that some are a bit more sophisticated.

These additional investigations can be used for many purposes: to supplement the investigations in the body of the text, for assigned homework, for quizzes or exams, and/or for further investigation.

To avoid confusion, the numbering has been changed in this section. Subsection headings use Arabic numerals and questions are listed with lower case Roman numerals. The investigations appear in an order that is compatible with the topics in the text.

1. Goldbach's Conjecture

i. Make a table and show that Goldbach's conjecture is valid for each of the even numbers 30 – 50.

ii. Make a table and show that Goldbach's conjecture is valid for each of the odd numbers 31 – 51.

iii. Does Goldbach's conjecture hold for each of the even numbers 100, 102, 104, and 106?

iv. Does Goldbach's conjecture hold for each of the even numbers 101, 103, 105, and 107?

v. If we are searching for prime numbers, is our task easier when we look among larger or smaller numbers? Explain in detail.

vi. What are the implications of your answer to v) to Goldbach's conjecture?

??Give references. Thing about Vinogradov's result.

2. Alan Turing

Alan Turing was one the twentieth century's more important mathematicians, making fundamental contributions to 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 forunate that the authorities did not know during the war that [Alan] Turing was a homosexual; otherwise, the Allies might have lost the war.[52]

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.

3. The Navajo Code Talkers

In addition to Alan Turing and other British mathematicians at Bletchley Park that broke the German *Enigma* codes, 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 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 Navajos translate the messages into Navajo before they were then encrypted using mathematical algorithms. Congressional Gold Medals were recently awarded to the 29 Code Talkers that developed the code.

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.[53] Write a brief, two- to three-page biographical essay, addressed to fellow students, that describes your findings.

4. Secret Codes

A rudimentary introduction to the breaking of secret messages, using guided discovery investigations as is done in this text, is given in "The breaking of ciphers and codes: An application of statistics," Chapter 9, Lesson 2 of Mathematics a Human Endeavor by Harold Jacobs (W.H. Freeman, 1994). Complete this lesson.

5. A "Forumla" for the Partition Function

In the Section III of the Investigations for Chapter 4 it is noted that in 1934 Hans Rademacher discovered an exact formula for the values of the partition function. This

---

[52] From "Cryptanalysis in World War II -- and Mathematics Education," *Mathematics Teacher*, Oct. 1984, by Peter Hilton.

[53] 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 Code Talkers by Doris A. Paul, Dorrance Publishing, 1998.

formula is an exact version of the asymptotic formula discovered by Hardy and Ramanujan in 1918 which is given by:

$$p(n) \approx \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{4n\sqrt{3}}.$$

i. Use a graphing calculator, computer algebra system, or spreadsheet to complete the following table (using the values of *p(n)* from Chapter 4):

n	*p(n)*	$\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{4n\sqrt{3}}$
1	1	
2	2	
3	3	
4	5	
$\vdots$	$\vdots$	$\vdots$
45	89,134	

ii) How do the values for *p(n)* and the Hardy/Ramanujan function appear to be on your table? Does this give you confidence that this result is correct?

iii) Use the Hardy/Ramanujan function to approximate *p(100), p(1000), p(10000),* and *p(1000000).* How useful is the Hardy/Ramanujan function in obtaining approximate values for these numbers?

iv) What do you think about the form of the Hardy/Ramanujan function? Do you have an idea how somebody might arrive at such a formula? Do you have an idea how they might prove that in fact gets closer and closer, asymptotically, to the correct value of the partition function as n gets larger and larger?

6. A "Generating Function" for the Partition Function

Well before Rademacher's formula Euler discovered a generating function for the partition function. In other words, Euler discovered a way to generate the number of partitions one after another, at least theoretically.

Euler's result is

$$1 + p(1)x + p(2)x^2 + p(3)x^3 + p(4)x^4 + p(5)x^5 + \ldots = \prod_{n=1}^{\infty} \frac{1}{1-x^n}.$$

If we can make sense of the thing on the right, an infinite product, then we can simply read off the values of the partition function; *p(3)* is the coefficient of x^3, etc.

So what is this quantity on the right? It is a shorthand for

$$\left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^2}\right)\left(\frac{1}{1-x^3}\right)\left(\frac{1}{1-x^4}\right)\left(\frac{1}{1-x^5}\right)\cdots$$

which turns out, remarkably, to be the same as

$$(1+x+x^2+x^3+x^4+\ldots)(1+x^2+x^4+x^6+x^8+\ldots)(1+x^3+x^6+x^9+x^{12}+\ldots)$$

$$\times(1+x^4+x^8+x^{12}+x^{16}+\ldots)(1+x^5+x^{10}+x^{15}+x^{20}+\ldots)\cdots$$

This looks like FOIL from hell, infinite multiplication of infinite series! But it helps that there are 1's in each of these infinite series. If you multiply the 1 from each of these, you get 1. This is the 1 that is the first term in Euler's result. Now what? Well, there is only one x term – in the first infinite series. So take this x term and multiply it by the 1 from each of the other infinite series. You get exactly one x. And, $p(1)=1$. So the x–term in Euler's infinite product is just $p(1)x$, as he claimed.

i. Mimicking the approach above, find all x^2 terms that would arise from the infinite expansion of the infinite products above. Show that your result is $p(2)x^2$.

ii. Mimicking the approach above, find all x^3 terms that would arise from the infinite expansion of the infinite products above. Show that your result is $p(3)x^3$.

iii. Mimicking the approach above, find all x^4 terms that would arise from the infinite expansion of the infinite products above. Show that your result is $p(4)x^4$.

iv. Do you begin to see why Euler's result might be true?

v. How useful is Euler's result in actually calculating values of the partition function? In other words, would Euler's result help you determine $p(20)$, $p(45)$, or any of the values in Investigation iii) of Section 5 above? Explain.

In fact, modern computer algebra systems can help you to use Euler's result to determine values of the partition function until the size of the numbers begin to strain computer limits.

7. Euler's Formula for Waring Numbers

As noted, mathematicians believe they have a formula for the Waring numbers. The formula, which is in fact due to Euler, is given by

$$W_n \approx 2^n + Int((3/2)^n) - 2$$

where Int means we take only the integer part of the fraction enclosed in parentheses and the approximation symbol ≈ is used as the validity of this expression has not been completely established. As an example,

$$W_4 \approx 2^4 + Int((3/2)^4) - 2 = 16 + Int(81/16) - 2 = 16 + Int(5\ 1/16) - 2 = 16 + 5 - 2 = 19,$$

as expected.

Euler only proposed the expression in question as an upper bound for the *Wn*. He certainly did not have enough evidence to connect it to all the *Wn*. It was 1912 before the value of W_3 was definitively established to be the value predicted by Euler's expression. This is 142 years after Lagrange established the value of W_2, slow progress indeed!! In 1936 Eugene Dickson and S. Pillai independently proved that Euler's expression does in fact give the correct value of *Wn* provided that

a) $n > 6$, and

b) the numerical inequality $Frac((3/2)^n) \leq 1 - (3/4)^n$ holds.

(*Frac* means that we take only the fractional part of the fraction enclosed in parenthesis.) In other words, determining each value of W_n has been reduced to showing that a simple numerical inequality holds!

i. Use Euler's formula to make a conjecture about the value of W_5.

ii. Determine whether the inequality above holds for $n = 5$ and explain what this tells you about the validity of your conjecture in i).

iii. Use Euler's formula to make a conjecture about the value of W_{10}.

iv. Determine whether the inequality above holds for $n = 10$ and explain what this tells you about the validity of your conjecture in i.

v. Computers have checked that the inequality above holds for values of n at least up to 471,600,000. Suppose that you wanted to be the first person to definitively establish the correct value of one of the Waring numbers. How could you do this? Explain.

vi. How technically complicated would it be to succeed in your efforts in v)? Explain.

vii. Does it seem reasonable that the inequality $Frac((3/2)^n) \leq 1 - (3/4)^n$ is centrally related to Waring's problem? Explain in detail.

viii. Is it strange that it is the cases of the smaller exponents n = 3, 4, 5, and 6 that do not conform to Euler's inequality while the larger exponents all do? Explain.

The correct values of W_4, W_5, and W_6 were established in 1986, 1964, and 1940 respectively. While this might seem a strange way for mathematical developments to proceed, it is not unheard of. One of the most famous outstanding problems in mathematics, and in fact another of the $1 Million Millenium Prize Problems that were mentioned in the Introduction, is the *Poincare Conjecture*. A conjecture from topology, a type of geometry where continuous distortions are allowed[54], the Poincare conjecture says that in each of the dimensions the only surfaces that behave like spheres are spheres. This result was established in 1960 by **Stephen Smale** (??) for dimensions $n \geq 5$. It has since been established for dimension four as well. Despite intense work by mathematicians and the lure of a $1 Million prize, the only dimension where this conjecture remains unestablished is $n = 3$ -- precisely the dimension in which we live.

8. Banach-Tarski Theorem and Other Paradoxes of the Infinite

?? Get stuff from Phil and do some of the other stuff on the infinite. Get Internet sites. Do 0.9999999 stuff. See what can be lifted from the infinite text. Start of with some of the cool quotes.
"The Banach Tarski Theorem" by Robert M. French, Mathematical Intelligencer, vol. 10, no. 4, Fall 1988, pp. 21-8.

9. Infinitude of the Primes

In this section we would like to investigate the number of prime numbers. This investigation is adapted from an approach that is due to the ancient Greeks and is included as a theorem in Euclid's Elements. This approach, which establishes a definitive result, is among the most famous proofs in all of mathematics.

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

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

ii) Do you think that the pattern in i) will continue indefinitely? If it does, what type of reasoning are you using and what may you conclude about the number of primes?

iii) 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.

iv) Repeat iii) for $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17+1=$.

[54] See e.g. [Jac, Ch. 10] for a guided discovery investigation of topology.

v) You should notice that the prime factors are all larger than the primes used in forming the numbers in iii) and iv). Prove that if you form the number $N_n = 2 \cdot 3 \cdot 5 \cdots p_n + 1$, where 2, 3, 5, ..., p_n are consecutive prime numbers, that none of these primes divide N_n.[55]

vi) Explain how v) enables you to prove the following:

> **Theorem** Let $N_n = 2 \cdot 3 \cdot 5 \cdots p_n + 1$ be the product formed from the product of the consecutive primes 2, 3, 5, ..., p_n. Then either:
> a) N_n is prime, or,
> b) N_n is divisible by some prime larger than p_n.

vii) Suppose that there were only finitely many primes. Then there would have to be a largest prime. Denote this largest prime by $p_{Largest}$. Use the result in vi) can be used to arrive at a contradiction - a state of affairs that is logically impossible.

viii) Explain how vii) enables you to conclude that there must be infinitely many primes.

xi) Does it seems strange to you that you were able to prove that there were infinitely many primes without providing a way of explicitly generating prime numbers indefinitely? Explain.

10. Distribution of the Primes

One of the opening quotes of Topic 3 was by the enigmatic Paul Erdos[56] who said "It will be another million years, at least, before we understand the primes." One way of understanding the primes would be able to explain precisely how they are distributed among the natural numbers. In 1896 **Jacque Salamon Hadamard** (1865-1963) and **Charles Jean Gustave Nicolas Baron de la Vallee Poussin** (1866-1962) independently proved the celebrated **Prime Number Theorem**. This theorem says that as you go farther and farther out in the number line the number of primes in the first n numbers is approximately equal to the quantity $\dfrac{n}{\log_e n}$. While this completely explains how the primes are distributed in average

[55] You should be careful with you use of calculators at this point. For example, Texas Instruments graphing calculators like the TI-82, TI-83, and TI-83 Plus will tell you that the number $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 + 1 = 6469693231$ is divisible by 3 which it certainly isn't. Reflecting on why this may happen is interesting.

[56] Erdos was one of the most cherished mathematician of this century. He was an eccentric vagabond who never having a permanent residence but simply traveled from mathematical conference to mathematical conference. He was fond of saying "A mathematician is a machine for turning coffee into theorems." He called little children "epsilons" after the Greek letter that mathematicians often use to denote small numbers. His work was so prolific that mathematicians are awarded Erdos numbers which measure their degree of separation from Erdos in terms of publications. This author is proud to have an Erdos number of 3. For more information on Erdos and Erdos numbers see the book <u>My Brain is Open: The Mathematical Journeys of Paul Erdos</u> by Bruce Schechter, Touchstone Books, 2000 and online Erdos Number Project site www.acs.oakland.edu/~grossman/erdoshp.html.

as we approach infinity, their behavior over any finite stretch is high volatile and poorly understood. The investigations below consider some of the strange behavior in the distribution of the primes.

i) In Topic 3 twin primes were introduced. Find a dozen examples of twin primes, one with numbers which are greater than 200.

ii) As the numbers increase in size, do you think it will be harder easier to find primes? What about twin primes?

The **Twin Prime Conjecture** is a conjecture which suggests that the number of twin primes is infinite. Mathematicians have believed this conjecture for centuries, but have made virtually no progress in proving it. However, there seems to be significant progress made in the past year.[57]

Consider the following numbers:

$$\begin{gathered}
2\times3\times4\times5\times6\times7\times\cdots\times10^6+2,\\
2\times3\times4\times5\times6\times7\times\cdots\times10^6+3,\\
2\times3\times4\times5\times6\times7\times\cdots\times10^6+4,\\
2\times3\times4\times5\times6\times7\times\cdots\times10^6+5,\\
\vdots\\
2\times3\times4\times5\times6\times7\times\cdots\times10^6+10^6.
\end{gathered}$$

iii) Show that the numbers in this sequence are consecutive numbers. How many numbers are there in this sequence?

iv) Show that each of the numbers in this sequence in composite.

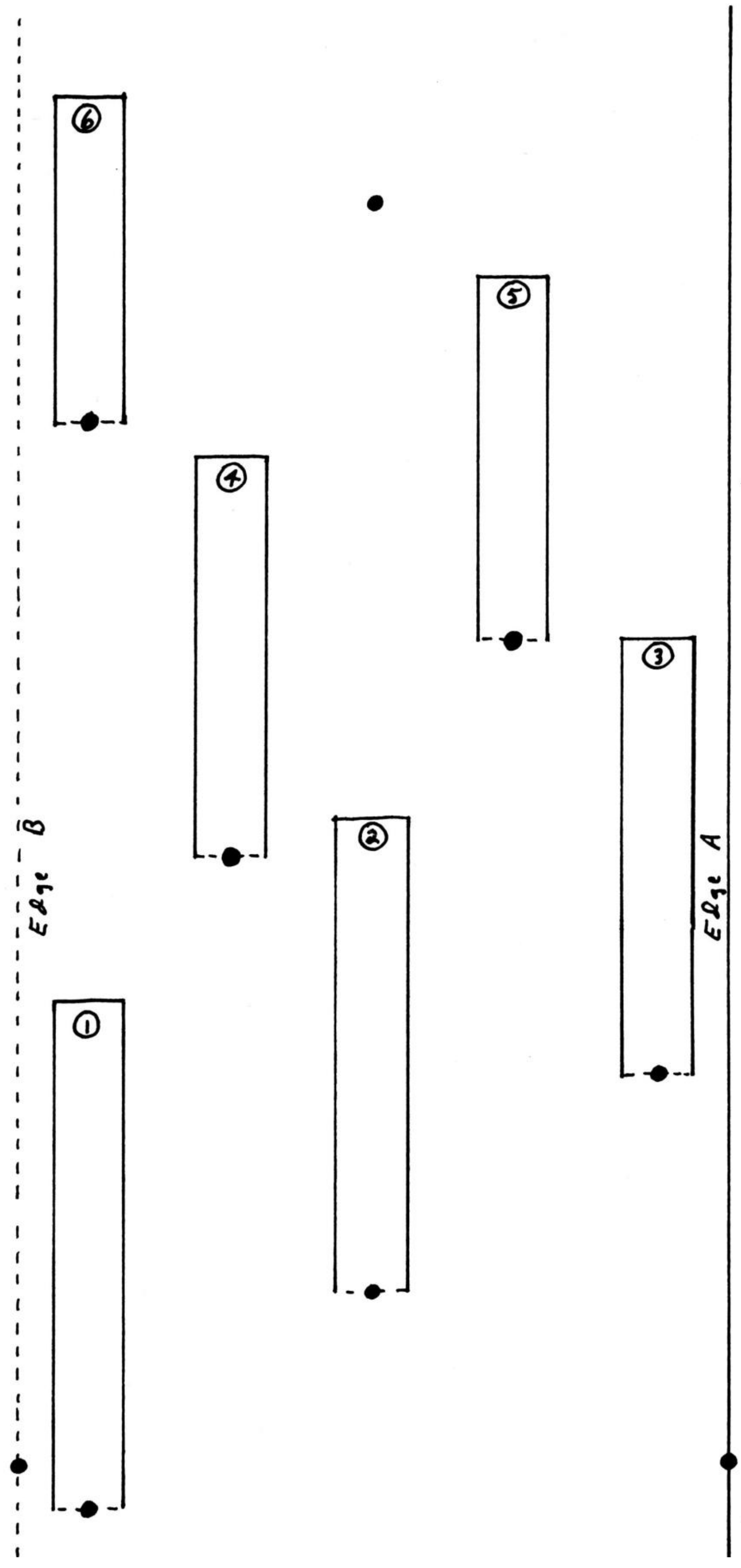
v) How do your answers in iii) and iv) contrast with the twin prime conjecture? What does this contrast tell you about the distribution of the prime numbers?

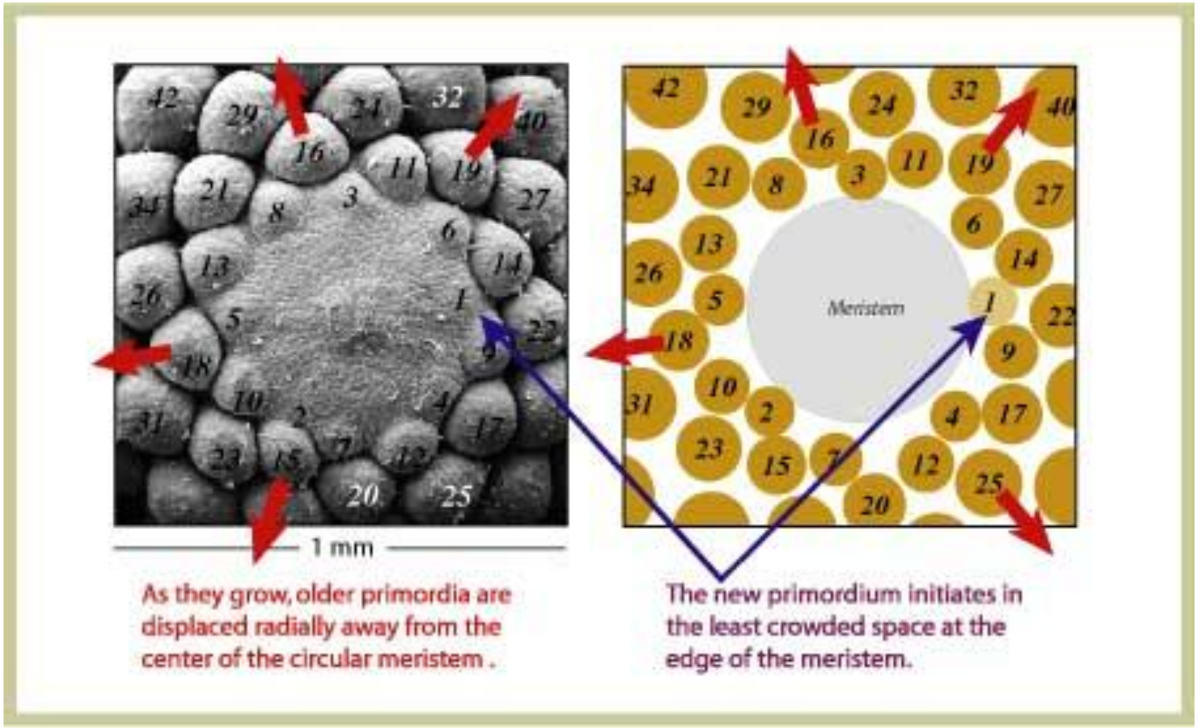
[57] On 21 March, 2003 the American Institute for Mathematics issued a press release which stated that the work of Dan Goldston and "Cem Yildirim, places mathematicians closer to the tantalizing goal of identifying the frequency and location of 'twin primes'."

Appendix

Fig 1.2 Spirals in a Pinecone and a Sunflower

Fig. A.2 2/5 Phyllotactic Ratio





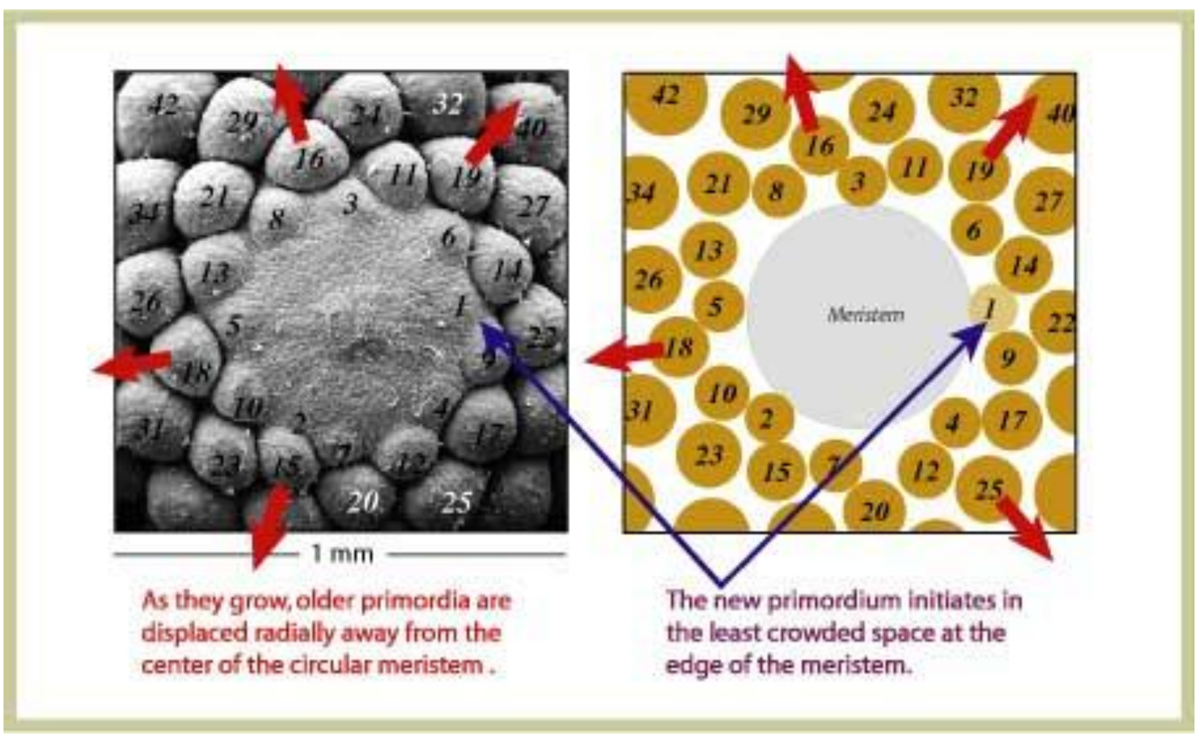


Fig. 1.7 Norway Spruce primordia development

NUMBER THEORY REFERENCES

Print

[AhOn] Scott Ahlgren and Ken Ono, "Addition and Counting: The arithmetic of partitions," *Notices of the American Mathematical Society*, vol. 48, no. 9, pp. 978-84.

[Ald] H.L. Alder, "Partition identities -- from Euler to the present," *American Mathematical Monthly*, vol. 76, no. 7, Aug.-Sept., 1969, pp. 733-46.

[Apo] T. Apostol, "Partitions," Ch. 14 of Introduction to Analytic Number Theory, Springer-Verlag, 1995.

[Beu] Albrecht Beutelspacher (transl. J. Chris Fisher), Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hidin and Safegaurding Described Without any Arcane Skullduggery but not Without Cunning Waggery for the Delectation and Instruction of the General Public, Mathematical Association of America, 1994.

[Bur] David M. Burton, Elementary Number Theory, McGraw-Hill, 1998.

[CoGu] John Conway and Richard Guy, The Book of Numbers, Springer-Verlag, 1996.

[Dud] Underwood Dudley, Elementary Number Theory (2^{nd} ed.), W.H. Freeman and Co., 1978.

[Dun1] William Dunham, Journey Through Genius: The Great Theorems of Mathematics, John Wiley & Sons, 1990.

[Dun2] William Dunham, Euler: The Master of Us All, Mathematical Association of America, 1999.

[Flan] Sarah Flannery and David Flannery, In Code: A Mathematical Journey, Workman Publishing, 2001.

[FrPe] Michael Frame and David Peak, Chaos Under Control: The Art and Science of Complexity, W.H. Freeman & Co., 1994.

[Gar] Martin Gardner, Codes, Ciphers, and Secret Writing, Dover, 1984.

[Gle] Vicki Glembocki, "The genius factor," *The Penn Stater*, July/August 2000, p. 28.

[HaWr] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 1980 (repreinted).

[Har] G.H. Hardy, A Mathematician’s Apology, Cambridge University Press, 1992 (reprinted).

[Kah] David Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Scribner, 1996.

[Kan] Robert Kanigel, The Man Who Knew Infinity: The Life and Genius of Ramanujan, Charles Scribner's Sons, 1991.

[Mau] R. Daniel Mauldin, "A generalization of Fermat's Last Theorem: The Beal conjecture and prize problem," *Notices of the American Mathematical Society*, vol. 44, no. 11, Dec. 1997, pp. 1436-7.

[Moz] C.J. Mozzochi, The Fermat Diary, American Mathematical Society, 2000.

[Nas] Sylvia Nasar, A Beautiful Mind: The Life of Mathematical Genius and Nobel Laureate John Nash, Touchstone Books, 2001.

[Ono] Ken Ono, "Disctribution of the partition function modolo m," *Annals of Mathematics*, vol. 151, 2000, pp. 293-307.

[Pau] Doris A. Paul, The Navajo Code Talkers, Dorrance Pub. Co., Inc., 1973.

[Pet1] Ivars Peterson, "The power of partitions: Writing a whole number as the sum of smaller numbers springs a mathematical surprise," *Science News*, vol. 157, 17 June, 2000, pp. 396-7.

[Pet2] Ivars Peterson, "Surprisingly square: Mathematicians take a fresh look at expressing numbers as the sums of squares," *Science News*, vol. 159, 16 June, 2001, pp. 382-3.
[Sin] Simon Singh, The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography, Doubleday, 1999.
[SinLy] Simon Singh and John Lynch, Fermat's Enigma : The Epic Quest to Solve the World's Greatest Mathematical Problem, Walker & Co., 1997.
[SinRi] Simon Singh and Kenneth Ribet, "Fermat's last stand," *Scientific American*, Nov. 1997, pp. 68-73.
[Wil] Andrew Wiles, "Modular elliptic curves and Fermat's Last Theorem," *Annals of Mathematics*, vol. 142, 1995, pp. 443-551.

Internet

[CMI] Clay Mathematics Institute, www.claymath.org/ .
[Con] Mary Ann Connors, "Exploring fractals," www.math.umass.edu/%7Emconnors/fractal/fractal.html .
[Cool] CoolMath4Kids, "Fractals," www.coolmath4kids.com/fractals.html .

Movies, Videos, and Performances

[Aub] David Auburn, Proof, 2000. www.proof-mtc.com .
[Note: This is the full-length Broadway play, not the NOVA documentary on the solution of FLT.]
[How] Ron Howard (Dir.), A Beautiful Mind, Universal Studios and DreamWorks LLC, 2000. www.abeautifulmind.com .
[LeRo] Joanne Sydney Lessner and Joshua Rosenblum, Fermat's Last Tango, York Theatre Company, 2000. Video available from www.claymath.org/ .
[LySin] John Lynch (Writer, Prod.) and Simon Singh (Dir.), The Proof, WGBH Educational Foundation, 1997. www.pbs.org/wgbh/nova/proof/wiles.html .
[Note: This is the NOVA documentary on the solution of FLT, not the Broadway play.]

GENERAL MATHEMATICS REFERENCES

1980 was the year that I entered high school and also the year that Carl Sagan's book (and corresponding television series) Cosmos became a best seller. That book drew me to the sciences and thus played a pivotal role in the direction of the remainder of my academic life.

Hopefully your exploration of number theory has renewed and/or piqued your interest in mathematics – somehow touching your life as Cosmos touched mine. Thankfully there is a rapidly growing collection of print and Internet resources that attempt to do for mathematics what Carl Sagan's Cosmos did for astronomy and physics – provide compelling and accessible overviews of their remarkable subjects. Below is a selected list of such resources that you can use in a variety of ways to nurture your interest in mathematics and begin new explorations.

Books

[COM] COMAP, For All Practical Purposes: An Introduction to Contemporary Mathematics, W.H. Freeman & Co., 1997.

[CRS] Richard Courant, Herbert Robbins, and Ian Stewart, What is Mathematics?, Oxford Univ. Pr., 1996.

[DaHe] Philip J. Davis and Reuben Hersh, The Mathematical Experience, Mariner Books, 1998.

[Dev1] Keith Devlin, Mathematics: The Science of Patterns, W.H. Freeman & Co., 1997.

[Dev2] Keith Devlin, Mathematics: The New Golden Age, Columbia Univ. Pr., 1999.

[FaSt] David W. Farmer, Groups and Symmetry: A Guide to Discovering Mathematics, American Mathematical Society, 1995.

[FaSt] David W. Farmer and Theodore B. Stanford, Knots and Surfaces: A Guide to Discovering Mathematics, American Mathematical Society, 1996.

[Jac] Harold Jacobs, Mathematics: A Human Endeavor, W.H. Freeman & Co., 1994.

[KaNe] Edward Kasner and James Newman, Mathematics and the Imagination, Dover, 2001.

[Pap] Theoni Pappas, The Joy of Mathematics, Wide World Publ. Tetra, 1989.

[Ste] Ian Stewart, What Shape is a Snowflake?, W.H. Freeman & Co., 2001.

[TaAr] Peter Tannenbaum and Robert Arnold, Excursions in Modern Mathematics, Prentice Hall, 2001.

Internet

[MAA] Mathematical Association of America, MAA Online Columns, //www.maa.org/news/columns.html .

[Wei] Eric Weisstein, World of Mathematics, mathworld.wolfram.com/ .