Survey of Mathematical Problems

Instructor's Guide

Harold P. Boas and Susan C. Geller
Texas A&M University

August 2006

Preface

> Everybody talks about the weather, but nobody does anything about it. Mark Twain

College mathematics instructors commonly complain that their students are poorly prepared. It is often suggested that this is a corollary of the students' high school teachers being poorly prepared. International studies lend credence to the notion that our hard-working American school teachers would be more effective if their mathematical understanding and appreciation were enhanced and if they were empowered with creative teaching tools.

At Texas A&M University, we decided to stop talking about the problem and to start doing something about it. We have been developing a Master's program targeted at current and prospective teachers of mathematics at the secondary school level or higher.

This course is a core part of the program. Our aim in the course is not to impart any specific body of knowledge, but rather to foster the students' understanding of what mathematics is all about. The goals are:

- to increase students' mathematical knowledge and skills;
- to expose students to the breadth of mathematics and to many of its interesting problems and applications;
- to encourage students to have fun with mathematics;
- to exhibit the unity of diverse mathematical fields;
- to promote students' creativity;
- to increase students' competence with open-ended questions, with questions whose answers are not known, and with ill-posed questions;

- to teach students how to read and understand mathematics; and
- to give students confidence that, when their own students ask them questions, they will either know an answer or know where to look for an answer.

We hope that after completing this course, students will have an expanded perspective on the mathematical endeavor and a renewed enthusiasm for mathematics that they can convey to their own students in the future.

We emphasize to our students that learning mathematics is synonymous with doing mathematics, in the sense of solving problems, making conjectures, proving theorems, struggling with difficult concepts, searching for understanding. We try to teach in a hands-on discovery style, typically by having the students work on exercises in groups under our loose supervision.

The exercises range in difficulty from those that are easy for all students to those that are challenging for the instructors. Many of the exercises can be answered either at a naive, superficial level or at a deeper, more sophisticated level, depending on the background and preparation of the students. We deliberately have not flagged the "difficult" exercises, because we believe that it is salutary for students to learn for themselves whether a solution is within their grasp or whether they need hints.

We distribute the main body of this Guide to the students, reserving the appendices for the use of the instructor. The material evolves each time we teach the course. Suggestions, corrections, and comments are welcome. Please email the authors at `boas@math.tamu.edu` and `geller@math.tamu.edu`.

Contents

Chapter 1

Logical Reasoning

1.1 Goals

- Know the meanings of the standard terms of logic: converse, contrapositive, necessary and sufficient conditions, implication, if and only if, and so on.
- Be able to recognize valid and invalid logic.
- Be able to construct valid logical arguments and to solve logic problems.
- Be aware that foundational problems (paradoxes) exist.
- Be able to identify and to construct valid proofs by the method of mathematical induction.

1.2 Reading

1. René Descartes, *Discourse on the Method of Rightly Conducting the Reason, and Seeking Truth in the Sciences*, excerpt from Part II; available from `gopher://wiretap.area.com:70/00/Library/Classic/reason.txt`.
2. René Descartes, *Philosophical Essays*, translated by Laurence J. Lafleur, Bobbs-Merrill Company, Indianapolis, 1964, pages 156–162.

3. Excerpt from *Alice in Puzzleland* by Raymond M. Smullyan, Penguin, 1984, pages 20–29.

4. Proofs without words from *Mathematics Magazine* **69** (1996), no. 1, 62–63.

5. Stephen B. Maurer, The recursive paradigm: suppose we already knew, *School Science and Mathematics* **95** (1995), no. 2 (February), 91–96.

6. Robert Louis Stevenson, "The Bottle Imp", in *Island Nights' Entertainments*, Scribner's, 1893; in the public domain and available on the world-wide web at `http://gaslight.mtroyal.ab.ca/bottleimp.htm`. (Compare the surprise examination paradox.)

1.3 Classroom Discussion

1.3.1 Warm up

Exercise 1.1. The Starship Enterprise puts in for refueling at the Ether Ore mines in the asteroid belt. There are two physically indistinguishable species of miners of impeccable reasoning but of dubious veracity: one species tells only truths, while the other tells only falsehoods.[1] The Captain wishes to determine the truth of a rumor that one of the miners has recently proved Goldbach's Conjecture.[2] What single question—answerable by "Yes" or "No"—can the Captain ask of an arbitrary miner in order to determine the truth?

1.3.2 The Liar Paradox

All Cretans are liars. Epimenides of Crete (attributed)

How are we to understand this statement? Apparently, it is true if and only if it is false.

The paradox has a number of different guises, for example:

Please ignore this sentence.

[1]Raymond Smullyan refers to such scenarios as "knights and knaves" and discusses many such in his puzzle books.

[2]Goldbach's Conjecture: every even integer greater than 2 can be expressed as the sum of two prime numbers.

An even sharper form is:

> This sentence is false.

Exercise 1.2. There is a non-paradoxical generalization of the preceding example to more than one sentence. Let n be an integer greater than 1, and consider the following list of sentences.

1. Exactly one statement on this list is false.

2. Exactly two statements on this list are false.

$\vdots$

n. Exactly n statements on this list are false.

Determine the truth or falsity of each statement on the list.

(This problem was published by David L. Silverman in the *Journal of Recreational Mathematics* (1969), page 29; cited in Martin Gardner, *Knotted Doughnuts and Other Mathematical Entertainments*, Freeman, 1986, Chapter Six.)

A version of the liar paradox attributed to P. E. B. Jourdain is a piece of paper that says on one side "The sentence on the other side is true" and on the other side "The sentence on the other side is false."

A version due to Bertrand Russell is:

> The village barber shaves those and only those villagers who do not shave themselves. Who shaves the barber?

The mathematical formulation of Russell's paradox is:

> Let S be the set whose elements are those sets that are not elements of themselves. Is S an element of itself?

G. G. Berry asked for a determination of "the least integer not nameable in fewer than nineteen syllables" (the quoted phrase consisting of eighteen syllables). Kurt Grelling asked if the adjective "heterological" is heterological (that is, not describing itself).

Self-referential paradoxes have appeared in popular literature. For example:

> "Can't you ground someone who's crazy?"
>
> "Oh, sure. I have to. There's a rule saying I have to ground anyone who's crazy."
>
> [. . .]
>
> There was only one catch and that was Catch-22, which specified that a concern for one's own safety in the face of dangers that were real and immediate was the process of a rational mind. Orr was crazy and could be grounded. All he had to do was ask; and as soon as he did, he would no longer be crazy and would have to fly more missions. Orr would be crazy to fly more missions and sane if he didn't, but if he was sane he had to fly them. If he flew them he was crazy and didn't have to; but if he didn't want to he was sane and had to. Yossarian was moved very deeply by the absolute simplicity of this clause of Catch-22 and let out a respectful whistle.
>
> Joseph Heller
> *Catch-22*

Here is another example:

> Well then, on this river there was a bridge, and at one end of it a gallows, and a sort of tribunal, where four judges commonly sat to administer the law which the lord of river, bridge and the lordship had enacted, and which was to this effect, "If anyone crosses by this bridge from one side to the other he shall declare on oath where he is going to and with what object; and if he swears truly, he shall be allowed to pass, but if falsely, he shall be put to death for it by hanging on the gallows erected there, without any remission." Though the law and its severe penalty were known, many persons crossed, but in their declarations it was easy to see at once they were telling the truth, and the judges let them pass free. It happened, however, that one man, when they came to take his declaration, swore and said that by the oath he took he was going to die upon that gallows that stood there, and nothing else. The judges held a consultation over the oath, and they said, "If we let this man pass free he has sworn falsely, and by the law he ought to die; but if we hang him, as he swore he was going to die on that gallows, and therefore swore the truth, by the same law he ought to go free."
>
> Miguel de Cervantes

Don Quixote
(John Ormsby, translator)

A common element of these paradoxes is their self-referential or circular property. For a complete resolution of Russell's paradox, we should have to go into set theory rather deeply. Intuitively, we need to rule self-referential statements out of bounds; or we need to accept that some apparently well-formed sentences are meaningless: neither true nor false. What, for example, are we to make of the following grammatical English sentence?

Colorless green ideas sleep furiously. Noam Chomsky

The lesson of the above discussion is that if we are not to build our mathematics on a foundation of quicksand, then we had better have some rules about determining truth. We will return later to the axiomatic method. For the moment, we will be content with reviewing some basic procedures of logical analysis.

1.3.3 The Formalism of Logic

Exercise 1.3. Let P denote the statement "It is raining"; let Q denote the statement "It is Saturday"; let R denote the statement "We are studying"; and let S denote the statement "We are having a picnic." Using the letters P, Q, R, and S, and the symbols $\vee$ (disjunction), $\wedge$ (conjunction), and $\neg$ (negation), fill in as many lines as possible of the following table to be compatible with the sentence: "We always study when it rains, but we have a picnic on Saturdays when it is not raining."

	if	
	only if	
	is sufficient for	
	is necessary for	
	if and only if	
	$\Rightarrow$	
	$\Leftarrow$	
	$\Leftrightarrow$	

Exercise 1.4. Create your own examples similar to the one above.

Exercise 1.5. Demonstrate that the biconditional "$\Leftrightarrow$" is associative. This can be accomplished by completing the following truth table and observing that the last two columns are identical.

A	B	C	$A \Leftrightarrow B$	$B \Leftrightarrow C$	$(A \Leftrightarrow B) \Leftrightarrow C$	$A \Leftrightarrow (B \Leftrightarrow C)$

Exercise 1.6. Solve the problems from the "Who Is Mad?" chapter in Raymond Smullyan's *Alice in Puzzle-Land.*

Exercise 1.7. Negate the following statements.

1. $\forall x\, \exists y\, (P(x, y) \Rightarrow Q(x, y))$.
2. For all positive x and y, either $x^2 \geq y$ or $y^2 \geq x$.
3. Neither a borrower nor a lender be. William Shakespeare
   Hamlet I. iii. 75
4. Everything in the world is good for something. John Dryden
5. If God did not exist, it would be necessary to invent Him.
   (Si Dieu n'existait pas, il faudrait l'inventer.) Voltaire
6. There is only one thing in the world worse than being talked about, and that is not being talked about. Oscar Wilde
7. You can fool all the people some of the time, and some of the people all the time, but you can not fool all the people all of the time.
   Abraham Lincoln (attributed)
8. The House of Peers, throughout the war,
   Did nothing in particular,
   And did it very well. W. S. Gilbert

1.3.4 Mathematical Induction

Exercise 1.8. Read aloud the following excerpt from Scenes VII–VIII of Eugène Ionesco's "anti-play" *The Bald Soprano.*[3] There are five actors involved: Mr. Smith, Mrs. Smith, Mr. Martin, Mrs. Martin, and the Fire Marshall.

(*The doorbell rings.*)

MR. SMITH: Say, the doorbell is ringing.

MRS. SMITH: There must be somebody there. I'll go see. (*She goes to see. She opens the door and returns.*) Nobody. (*She sits down again.*)

MR. MARTIN: I'm going to give you another example . . . (*The doorbell rings.*)

MR. SMITH: Say, the doorbell is ringing.

MRS. SMITH: It must be somebody. I'll go see. (*She goes to see. She opens the door and returns.*) Nobody. (*She returns to her seat.*)

MR. MARTIN (*who has forgotten where he was*): Uh . . .

MRS. MARTIN: You were saying that you were going to give another example.

MR. MARTIN: Oh, yes . . . (*The doorbell rings.*)

MR. SMITH: Say, the doorbell is ringing.

MRS. SMITH: I am not going to open the door again.

MR. SMITH: Well, but there must be somebody there!

MRS. SMITH: The first time, there was nobody. The second time, again nobody. Why do you think there will be somebody now?

MR. SMITH: Because the doorbell rang!

MRS. MARTIN: That's not a reason.

MR. MARTIN: What? When one hears the doorbell ring, it's because there is somebody at the door who is ringing to have the door opened.

MRS. MARTIN: Not always, as you have just seen!

MR. MARTIN: But yes, most of the time.

MR. SMITH: Myself, when I go to someone's house, I ring the bell to get in. I think that everybody does the same, and each time the doorbell rings it's because there is somebody there.

[3] *La cantatrice chauve*, first performed May 11, 1950.

MRS. SMITH: That is true in theory. But in reality things happen differently. You have just seen so.

MRS. MARTIN: Your wife is right.

MR. MARTIN: Oh, you women! Always defending each other.

MRS. SMITH: All right, I'll go see. You can't say that I am stubborn, but you will see that there is nobody there! (*She goes to see. She opens the door and shuts it again.*) You see, there is nobody. (*She returns to her seat.*)

MRS. SMITH: Oh, these men who always want to be right and who are always wrong! (*The doorbell rings again.*)

MR. SMITH: Say, the doorbell is ringing. There must be somebody there.

MRS. SMITH (*in a fit of anger*): Don't send me to open the door again. You have seen that it is useless. Experience shows us that when the bell rings, it's because there is never anybody there.

MRS. MARTIN: Never.

MR. MARTIN: That's not certain.

MR. SMITH: It's even false. Most of the time, when the bell rings, it's because there is somebody there.

MRS. SMITH: He won't admit he's wrong.

MRS. MARTIN: My husband too is very stubborn.

MR. SMITH: There is somebody there.

MR. MARTIN: It's not impossible.

MRS. SMITH (*to her husband*): No.

MR. SMITH: Yes.

MRS. SMITH: I tell you no. At any rate, you are not going to bother me again for nothing. If you want to go see, go yourself!

MR. SMITH: I'm going. (*Mrs. Smith shrugs her shoulders. Mrs. Martin tosses her head.*)

MR. SMITH (*opening the door*): Oh! Comment allez vous? (*He glances at Mrs. Smith and at the Martins, who are all surprised.*) It's the Fire Marshall!

FIRE MARSHALL (*he has, of course, an enormous shiny helmet and a uniform*): Good day, ladies and gentlemen. (*They are still a bit stupefied. Mrs. Smith, angry, averts her head and does not respond.*) Hello, Mrs. Smith. You seem to be angry.

MRS. SMITH: Oh!

MR. SMITH: It's like this, you see ... my wife is a bit humiliated to have been wrong.

MR. MARTIN: There has been, Fire Marshall, an argument between Mrs. and Mr. Smith.

MRS. SMITH (*to Mr. Martin*): It's none of your business!
(*To Mr. Smith*): I beg you not to bring strangers into our family quarrels.

MR. SMITH: Oh, darling, it's not so serious. The Fire Marshall is an old family friend. His mother courted me, and I knew his father. He asked to marry my daughter if I ever had one. He died waiting.

MR. MARTIN: It's neither his fault nor yours.

FIRE MARSHALL: So, what's it all about?

MRS. SMITH: My husband was claiming ...

MR. SMITH: No, it was you who was claiming.

MR. MARTIN: Yes, it was her.

MRS. MARTIN: No, it was him.

FIRE MARSHALL: Don't get excited. Tell me about it, Mrs. Smith.

MRS. SMITH: All right, then. It troubles me to speak openly to you, but a Fire Marshall is also a confessor.

FIRE MARSHALL: Well?

MRS. SMITH: We were arguing because my husband said that when the doorbell rings, there is always somebody there.

MR. MARTIN: It's plausible.

MRS. SMITH: And I said that each time the doorbell rings, it is because nobody is there.

MRS. MARTIN: It might seem strange.

MRS. SMITH: But it is proven, not by theoretical demonstrations, but by facts.

MR. SMITH: It's false, because the Fire Marshal is there. He rang, I opened the door, he was there.

MRS. MARTIN: When?

MR. MARTIN: Why, just now.

MRS. SMITH: Yes, but it was only after the bell rang a fourth time that someone was there. And the fourth time doesn't count.

MRS. MARTIN: Always. Only the first three times count.

MR. SMITH: Fire Marshall, let me ask you a few questions.

FIRE MARSHALL: Go ahead.

MR. SMITH: When I opened the door and saw you there, was it indeed you who had rung?

FIRE MARSHALL: Yes, it was me.

MR. MARTIN: You were at the door? You rang to be let in?

FIRE MARSHALL: I don't deny it.

MR. SMITH (*to his wife, victoriously*): You see? I'm right. When the bell rings, it is because somebody is there. You can't say that the Fire Marshall is not somebody.

MRS. SMITH: Certainly not. I repeat that I speak only of the first three times, because the fourth time does not count.

MRS. MARTIN: When the bell rang the first time, was it you?

FIRE MARSHALL: No, it was not me.

MRS. MARTIN: You see? The bell rang, and nobody was there.

MR. MARTIN: Perhaps it was someone else?

MR. SMITH: Were you at the door a long time?

FIRE MARSHALL: Three quarters of an hour.

MR. SMITH: And you saw nobody?

FIRE MARSHALL: Nobody. I'm certain.

MRS. MARTIN: Did you hear the bell ring the second time?

FIRE MARSHALL: Yes, and again it was not me. And there was still nobody.

MRS. SMITH: Victory! I was right.

MR. SMITH (*to his wife*): Not so fast. (*To the Fire Marshall*) And what were you doing at the door?

FIRE MARSHALL: Nothing. I was standing there. I was thinking about a lot of things.

MR. MARTIN (*to the Fire Marshall*): But the third time ... it was not you who rang?

FIRE MARSHALL: Yes, it was me.

MR. SMITH: But when we opened the door, we did not see you.

FIRE MARSHALL: That's because I hid myself ... as a joke.

MRS. SMITH: Don't joke, Fire Marshall. The situation is too sad.

MR. MARTIN: To sum up, we still don't know, when the doorbell rings, whether there is someone there or not!

MRS. SMITH: Never anybody.

MR. SMITH: Always somebody.

FIRE MARSHALL: I will reconcile you. You are both partly right. When the doorbell rings, sometimes there is somebody, and other times there is nobody.
MR. MARTIN: That seems logical to me.
MRS. MARTIN: I think so too.
FIRE MARSHALL: Things are simple, really.

Exercise 1.9. Comment on the implications of the above scene for mathematical logic.

Exercise 1.10. What is the next term in the sequence 2, 3, 5, 9, . . . ?

The principle of induction says, intuitively, that if you can take a first step, and if you can always take another step—no matter how far you have gone already—then you can travel an arbitrary distance. The "domino effect" is the same phenomenon. The two common mistakes in creating an induction proof are (i) neglecting to check the basis step, and (ii) failing to make a completely general argument for the induction step.

The basis step is usually easy to confirm, but it is nonetheless a crucial part of the argument.

> A journey of a thousand miles begins with a single step.
>
> Chinese Proverb

> Who has begun, has half the job done.
> (*Dimidium facti qui coepit habet.*) Horace
>
> *Epistles* I. i. 40

An example of an inductive situation that founders for want of an initial step is the parable in the New Testament of the woman who is to be stoned for transgressing the Mosaic law; Jesus says:

> Let he who is without sin among you cast the first stone.
>
> *John* 8:7

The most familiar type of induction problem involves proving an equality. Proving an inequality can be trickier, because it is not obvious how to relate statement n to statement $(n + 1)$.

Exercise 1.11. Prove that $2^n > 2n + 1$ when n is an integer greater than 2.

In the next example, the induction statement is not a formula.

Exercise 1.12. In a round-robin tournament, each team plays every other team exactly once. Show that if no games end in ties, then no matter what the outcomes of the games, there will be some way to number the teams so that team 1 beat team 2, and team 2 beat team 3, and team 3 beat team 4, and so on.[4]

Here is an example of a formula with cases.

Exercise 1.13. 1. Find a formula for the nth positive integer that is divisible by neither 2 nor 3.

2. Show that the sum of the first n positive integers that are divisible by neither 2 nor 3 is

$$\begin{cases} \frac{3}{2}n^2 - \frac{1}{2} & \text{if } n \text{ is odd,} \\ \frac{3}{2}n^2 & \text{if } n \text{ is even.} \end{cases}$$

Exercise 1.14. Find the mistake in the following "proof."

Theorem. *All horses are the same color.*

"Proof" by induction. Let $P(n)$ be the proposition that all members of an arbitrary set of n horses are the same color.

Trivially $P(1)$ is true.

Suppose that $P(n)$ holds. If S is an arbitrary set of $n+1$ horses, and one is removed, the remaining n horses are the same color by the induction hypothesis. Since it does not matter which horse is removed, it must be that all $n+1$ horses are the same color.

By induction, $P(n)$ is true for every positive integer n, that is, all horses are the same color. □

Exercise 1.15. The previous example was a false "proof" of a false statement. Here is a false proof of a true statement; where is the mistake?[5]

Theorem. *The sum of the angles of a regular n-gon is* $180(n-2)°$.

[4] Problem paraphrased from Stephen B. Maurer and Anthony Ralston, *Discrete Algorithmic Mathematics*, Addison-Wesley, 1991, page 145.

[5] Example paraphrased from Stephen B. Maurer and Anthony Ralston, *Discrete Algorithmic Mathematics*, Addison-Wesley, 1991, page 171.

"Proof" by induction. The basis step ($n = 3$) is the well-known fact that the angles of a triangle sum to $180°$. Now suppose that the statement has been proved for a certain value of n (where $n \geq 3$). Given a regular $(n+1)$-gon, take three consecutive vertices and cut off the triangle they determine. The remaining n-gon has angle sum of $180(n-2)°$ by the induction hypothesis. Adding back the triangle increases the angle sum by $180°$ for a final total of $180(n-1)° = 180((n+1)-2)°$. $\square$

In the next exercise, it may not be obvious what statement n should be.

Exercise 1.16. Construct an induction proof of the proposition that every set (possibly infinite) of positive integers has a least element.

1.4 Problems

Problem 1.1. The philosopher Raymond Smullyan has written several puzzle books[6] featuring the island of knights and knaves, where knights speak only truths, and knaves speak only falsehoods. Since the knights are physically indistinguishable from the knaves, the visitor must exercise ingenuity to extract information from the inhabitants' statements.

1. For instance, is a native who states,[7] "This is not the first time I have said what I am now saying" a knight or a knave? See the footnote for a hint.[8]

2. Invent your own scenario of an encounter with the residents of the island of knights and knaves.

Problem 1.2. Pattern recognition is an element of games, of art, of mathematics. Much of modern science is an effort to find patterns in nature. Children of all ages enjoy guessing patterns.

[6]Some of his books featuring logic puzzles are *Satan, Cantor and Infinity*, Knopf, 1992, reprinted by Oxford University Press, 1993; *The Lady or the Tiger?*, Knopf, 1982, reprinted by Times Books, 1992; *Forever Undecided*, Knopf, 1987; *What Is the Name of This Book?*, Prentice Hall, 1978, reprinted by Penguin, 1981; *This Book Needs No Title*, Prentice Hall, 1980, reprinted by Simon & Schuster, 1986; *Alice in Puzzle-Land: A Carrollian Tale for Children Under Eighty*, Morrow, 1982, reprinted by Penguin, 1984; *To Mock a Mockingbird*, Knopf, 1985.

[7]Raymond Smullyan, *To Mock a Mockingbird*, Knopf, 1985, page 44.

[8]Can a knave or a knight make this statement for the second time?

You can amuse any class by asking for the rule generating the following sequence of letters:

$$\text{O, T, T, F, F, S, S, E, N, T, E, T, } \dots .$$

See the footnotes for a hint.[9]

The element of surprise often makes an amusing puzzle. Can you figure out the missing entry in the following sequence?[10]

$$10, 11, 12, 13, 14, 15, 16, 17, 20, 22, 24, 31, 100, \boxed{}, 10000$$

Hint: the sequence terminates—there are no more terms. See the footnote for a further hint.[11]

A great many special sequences of counting numbers may be found in Simon Plouffe and N. J. A. Sloane, *The Encyclopedia of Integer Sequences*, San Diego, Academic Press, 1995 (available online at `http://www.research.att.com/~njas/sequences/`).

Invent your own pattern recognition problem.

Problem 1.3.

1. Prove by induction that $\underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\cdots}}}}_{n}$ is irrational for each positive integer n.
2. Prove by induction that $\underbrace{\sqrt[2]{2+\sqrt[3]{3+\sqrt[4]{4+\cdots}}}}_{n}$ is irrational for each positive integer n.

Problem 1.4. Find a formula for the sum of the first n positive integers that are not divisible by 4, and prove it by induction.

Problem 1.5. What is wrong with the following "proof"?[12]

---

[9] This puzzle would be different in French.

[10] Martin Gardner, *Mathematical Magic Show*, Knopf, New York, 1977, revised edition published by the Mathematical Association of America, 1989, page 137.

[11] The missing entry is in base three.

[12] Example paraphrased from Stephen B. Maurer and Anthony Ralston, *Discrete Algorithmic Mathematics*, Addison-Wesley, 1991, page 172.

Theorem (false)**.** *There are 2^n sequences of 0's and 1's of length n with the property that 1's do not appear consecutively except possibly in the two right-most positions.*

"Proof". When $n = 1$, there two such sequences, so the theorem holds in the base case. Suppose the theorem holds for a certain integer n, where $n \geq 1$. We can create sequences of length $(n + 1)$ by appending either a 0 or a 1 to the right-hand end of a sequence of length n; in the case of appending a 1, we might produce a 11 at the right-hand end, but that is allowed. Hence there twice as many sequences of length $(n + 1)$ as there are of length n, so the theorem is proved because $2 \cdot 2^n = 2^{n+1}$. □

1.5 Additional Literature

- Jon Barwise and John Etchemendy, *The Liar: An Essay on Truth and Circularity*, Oxford University Press, 1987. (BC199.P2 B37 1987)

- Bryan H. Bunch, *Mathematical Fallacies and Paradoxes*, Van Nostrand, New York, 1982. (QA9 B847)

- Martin Gardner, *Mathematical Magic Show*, Knopf, New York, 1977, updated and revised edition published by the Mathematical Association of America, 1989.

- Joseph Heller, *Catch-22*, Simon and Schuster, New York, 1961. (PZ4 H47665 Cat)

- Patrick Hughes and George Brecht, *Vicious Circles and Infinity: A Panoply of Paradoxes*, Doubleday, Garden City, NY, 1975. (BC199.P2 H83)

- J. L. Mackie, *Truth, Probability and Paradox: Studies in Philosophical Logic*, Oxford University Press, 1973. (BC171.M24)

- Stephen B. Maurer and Anthony Ralston, *Discrete Algorithmic Mathematics*, Addison-Wesley, 1991.

- Simon Plouffe and N. J. A. Sloane, *The Encyclopedia of Integer Sequences*, San Diego, Academic Press, 1995. (QA246.5.S66 1995)

- W. V. Quine, *The Ways of Paradox and Other Essays*, revised and enlarged edition, Harvard University Press, 1976. (B945.Q51 1976)
- R. M. Sainsbury, *Paradoxes*, Cambridge University Press, 1988. (BC199 P2 S25 1988)
- Raymond M. Smullyan, *Alice in Puzzle-Land: A Carrollian Tale for Children Under Eighty*, Morrow, 1982, reprinted by Penguin, 1984.
- Raymond M. Smullyan, *Forever Undecided: A Puzzle Guide to Gödel*, Knopf, New York, 1987. (QA9.65.S68 1987)
- Raymond M. Smullyan, *Satan, Cantor and infinity*, Knopf, 1992, reprinted by Oxford University Press, 1993.
- Raymond M. Smullyan, *The Lady or the Tiger?*, Knopf, 1982, reprinted by Times Books, 1992.
- Raymond M. Smullyan, *This Book Needs No Title: A Budget of Living Paradoxes*, Prentice-Hall, Englewood Cliffs, NJ, 1980, reprinted by Simon & Schuster, 1986. (PN6361.S6 1980)
- Raymond M. Smullyan, *To Mock a Mocking Bird and Other Logic Puzzles*, Knopf, New York, 1985. (GV1507.P43 S68 1985)
- Raymond M. Smullyan, *What is the Name of This Book?*, Prentice Hall, 1978, reprinted by Penguin, 1981.
- Richard H. Thaler, *The Winner's Curse: Paradoxes and Anomalies of Economic Life*, Free Press (Macmillan), New York, 1992. (HB199.T47 1992)

Chapter 2

Probability

If this were played upon a stage now, I could condemn it as an improbable fiction.

William Shakespeare
Twelfth Night
Act III, scene 4

2.1 Goals

- Understand the notion of discrete probability.
- Be able to count cases using permutations and combinations.
- Be able to calculate discrete probabilities.
- Be able to apply your knowledge of probability to unfamiliar situations.

2.2 Reading

1. "Chance and Chanceability", Chapter VII, pages 223–264, of *Mathematics and the Imagination* by Edward Kasner and James Newman, Simon and Schuster, 1940. This selection is an introduction to probability.

2.3 Classroom Discussion

2.3.1 Warm up

Exercise 2.1. Either it will rain tomorrow, or it will not rain tomorrow. Therefore the probability that it will rain tomorrow is 1/2. What is wrong with this argument?

Exercise 2.2. The weather tomorrow is not a repeatable experiment, so what does it mean when the weather forecast is "30% chance of rain tomorrow"?

> Lest men suspect your tale untrue,
> Keep probability in view.
>
> John Gay
> 1688–1732
> *The Painter who pleased Nobody and Everybody*

2.3.2 Cards and coins

A typical sort of question in discrete probability is: "If two cards are dealt from a standard deck,[1] what is the probability that both are red?" Using the principle that probability is computed as the number of favorable situations divided by the number of all possible situations (assuming that all situations are equally probable), you could compute this probability as the fraction

$$\frac{\binom{26}{2}}{\binom{52}{2}} = \frac{25}{102} \approx 0.245$$

(where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the number of combinations of n things taken k at a time).

Exercise 2.3. Why—since half the cards are red—is the answer not just the product $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$?

> If he does really think that there is no distinction between virtue and vice, why, sir, when he leaves our houses let us count our spoons.
>
> Samuel Johnson
> *Life of Boswell*, Vol. ii, Chap. v, 1763

[1] You need to know that a standard deck of playing cards consists of four suits (spades ♠, hearts ♡, diamonds ♢, and clubs ♣), the spades and clubs being black and the hearts and diamonds being red, and each suit has thirteen cards (ace, two, three, . . . , ten, jack, queen, king).

Since the mathematical theory of probability had its beginnings in gambling games, it is historically appropriate to analyze a popular modern gambling game: poker. In the simplest version of poker, five cards are dealt from a standard deck.

Exercise 2.4. Begin determining the probabilities of being dealt the following poker hands. (Keep in mind that aces can count as either high or low.) You will finish this exercise for homework.

1. A *royal flush* consists of the five highest cards in one suit. Examples are ♠A ♠K ♠Q ♠J ♠10 and ♢A ♢K ♢Q ♢J ♢10.

2. A *straight flush* consists of five consecutive cards in the same suit (but excluding a royal flush). Examples are ♡K ♡Q ♡J ♡10 ♡9 and ♣10 ♣9 ♣8 ♣7 ♣6.

3. *Four of a kind* is all four cards of the same rank together with any other card. Examples are ♠J ♡J ♢J ♣J ♡3 and ♠7 ♡7 ♢7 ♣7 ♣10.

4. A *full house* consists of three of a kind together with a pair. Examples are ♠K ♢K ♣K ♢3 ♣3 and ♡5 ♢5 ♣5 ♡10 ♣10.

5. A *flush* is five cards all of the same suit (but excluding all of the previous cases). Examples are ♣A ♣7 ♣5 ♣3 ♣2 and ♠K ♠Q ♠10 ♠9 ♠7.

6. A *straight* is a sequence of five cards in order in mixed suits. Examples are ♠A ♡K ♡Q ♠J ♣10 and ♠5 ♡4 ♡3 ♣2 ♡A.

7. *Three of a kind* means three cards of the same rank and two extra cards (but excluding all of the previous cases). Examples are ♠A ♡A ♢A ♡9 ♣7 and ♠3 ♡3 ♢3 ♣K ♢10.

8. *Two pairs* means two separate pairs and an extra card (but excluding all of the previous cases). Examples are ♢K ♣K ♡7 ♣7 ♠9 and ♠10 ♣10 ♡6 ♢6 ♣4.

9. *One pair* means two cards of the same rank and three other cards (but excluding all of the previous cases). Examples are ♠A ♡A ♠6 ♢5 ♣3 and ♢9 ♣9 ♣10 ♢8 ♣3.

10. *Nothing* is any other hand not previously enumerated.

If a "fair coin" is tossed, it has probability $\frac{1}{2}$ of landing heads up, and probability $\frac{1}{2}$ of landing tails up. Actual United States coins are not precisely fair, because one side is slightly hollowed out to form a relief image. The lighter side with the head is slightly more likely to land facing up. Similar considerations apply to the dice accompanying children's games: the side with six pips hollowed out is more likely to land up than the opposite heavier side with only one pip hollowed out. (This effect is noticeable in the third decimal place.)

There are many probability problems dealing with coins (or dice) that have been weighted, so that the probabilities are different from the ordinary uniform distribution. In such cases, computing the number of favorable outcomes divided by the number of possible outcomes is no longer a valid way to find the probability of an event (because the outcomes are not equally likely). Instead, one has to add the probabilities of the individual outcomes.

Exercise 2.5. If one coin has been weighted so that it comes up heads with probability $\frac{1}{3}$, and a second coin has been weighted so that it comes up heads with probability $\frac{1}{4}$, what is the probability that when the two coins are tossed, one of them comes up heads and the other one comes up tails?

Let the worst come to the worst. Miguel de Cervantes
1547–1616
Don Quixote, Part i, Book iii, Chap. v

2.4 Problems

Problem 2.1. The problem of computing probabilities of results of coin tosses for coins weighted in a specified way can be difficult, but it is routine in the sense that all such problems use the same principle. Mathematically more challenging is the *inverse problem* of determining the weights needed to produce specified probabilities. Three solutions are conceivable: more than one set of weights will work, exactly one set of weights will work, or no set of weights will work.

1. Can you weight two coins in such a way that if the two coins are tossed, the three possible outcomes (both heads, both tails, or one head and one tail) all have probability $\frac{1}{3}$? The two coins do not have to be weighted the same as each other.

2. What about three coins? Can you weight them so that the four possible outcomes (all heads, two heads and one tail, one head and two tails, all tails) are equally likely?

3. Can you generalize to an arbitrary number of coins?

Problem 2.2. This problem was discussed by Sir Arthur Eddington:[2]

> If A, B, C, D each speak the truth once in three times (independently), and A affirms that B denies that C declares that D is a liar, what is the probability that D was speaking the truth?

Problem 2.3. This problem sometimes goes by the name of "the secretary problem."

A hat has 100 slips of paper in it with different real numbers written on them. The numbers are all different, but they need not be integers: they could be -17π, or $10^{\sqrt{2}}$, or $-22/7$.

You reach into the hat, pull out slips of paper one at a time, and look at each number. At any point, you may choose to stop. (If you get to the last slip, you stop automatically.) If the last slip you draw has the largest number on it (largest of all 100 numbers, both the numbers you have drawn and the numbers that are left in the hat), then you win \$10. Otherwise you win nothing.

1. What is a reasonable strategy to use for playing this game? How should you decide when to stop?

2. What is a reasonable amount to pay for the privilege of playing this game? Ten cents? Fifty cents? One dollar? Two dollars?

Remarks

1. You may want to get started by considering a similar problem in which there are only a small number of slips of paper, say four.

2. It is rather difficult to find an exact solution to the problem, but you should be able to make some estimate of the expected value that is in the right ballpark.

[2] *New Pathways in Science*, MacMillan, New York, 1935, page 121; but his solution is disputed by other authors.

3. There is an extensive literature about this problem and its relatives. In its traditional formulation, the problem concerns a business executive who is interviewing 100 secretaries for a job and wants to hire the best one. Hence the name of "the secretary problem."

2.5 Additional Literature

- Richard Durrett, *The Essentials of Probability*, Duxbury Press, Belmont, CA, 1994. This is an undergraduate textbook.
- Sir Arthur Eddington, *New Pathways in Science*, MacMillan, New York, 1935. This is the source for "Eddington's problem."
- Edward Kasner and James Newman, *Mathematics and the Imagination*, Simon and Schuster, New York, 1940, chapter VII.
- T. H. O'Beirne, *Puzzles and Paradoxes*, Oxford University Press, 1965.

Chapter 3

Graph Theory

I see my way as birds their trackless way.
I shall arrive,—what time, what circuit first,
I ask not; but unless God send his hail
Or blinding fire-balls, sleet or stifling snow,
In some time, his good time, I shall arrive:
He guides me and the bird. In his good time.

Robert Browning
1812–1890
Paracelsus, Part i

3.1 Goals

1. Understand the notions of Eulerian graph, Hamiltonian graph, planar graph, and dual graph.

2. Learn about Euler's formula, its proof, and its consequences.

3. Become familiar with some famous problems of mathematics, such as the traveling salesman problem, the Königsberg bridge problem, and the four-color problem.

4. Experience the fun of discovering and creating mathematics.

3.2 Reading

1. Richard J. Trudeau, *Dots and Lines*, Kent State University Press, 1976, pages ix–27. This introduces the notion of a graph and gives some examples.

2. William Dunham, *The Mathematical Universe*, Wiley, New York, 1994, pages 51–63. This is a biographical piece about Euler.

3. James R. Newman, *The World of Mathematics*, Volume One, Simon and Schuster, New York, 1956, pages 570–580. This is a commentary on and a translation of Euler's original paper on the seven bridges of Königsberg.

4. Sir Edmund Whittaker, "William Rowan Hamilton," *Scientific American*, May 1954, reprinted in *Mathematics in the Modern World*, Freeman, San Francisco, 1968, pages 49–52. This is a biographical piece about Hamilton.

5. Alan Tucker, The parallel climbers puzzle, *Math Horizons*, Mathematical Association of America, November 1995, pages 22–24.

6. Frank Harary, *Graph Theory*, Addison-Wesley, 1969, chapter 1, pages 1–7.

7. Richard J. Trudeau, *Dots and Lines*, Kent State University Press, 1976, chapter 4, pages 97–116.

8. *The Traveling Salesman Problem*, edited by E. L. Lawler, J. K. Lenstra, A. H. G. Rinnooy Kan, and D. B. Shmoys, Wiley, New York, 1985, pages 1–15. This is a historical piece by A. J. Hoffman and P. Wolfe on the traveling salesman problem.

9. Norman L. Biggs, E. Keith Lloyd, and Robin J. Wilson, *Graph Theory 1736–1936*, Oxford University Press, 1976, chapter 6, pages 90–108. This is a historical piece including Kempe's famous false proof of the four-color theorem and Heawood's correction.

10. Ralph P. Boas, Möbius shorts, *Mathematics Magazine* **68** (1995), no. 2, 127.

3.3 Classroom Discussion

How sweet a thing it is to wear a crown,
Within whose circuit is Elysium
And all that poets feign of bliss and joy! William Shakespeare
King Henry VI
Part III, Act i, scene 2

3.3.1 Examples of graphs

cyclic The cyclic (or circuit) graph C_n is a connected graph having n vertices each incident to exactly two edges.

complete The complete graph K_n has n vertices each of which is adjacent to all the other vertices. The graph K_n has $n(n-1)/2$ edges.

bipartite A bipartite graph has two sets of vertices, say red and blue, and every edge of the graph has one red vertex and one blue vertex. The complete bipartite graph $K_{m,n}$ has m red vertices, n blue vertices, and an edge for each of the mn red-blue pairs of vertices.

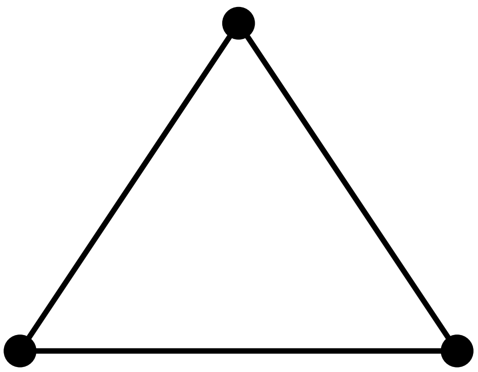
utilities The utilities graph is the complete bipartite graph $K_{3,3}$.

Platonic The Platonic graphs are formed by the vertices and edges of the five regular Platonic solids: the tetrahedron, the cube (hexahedron), the octahedron, the dodecahedron, and the icosahedron.

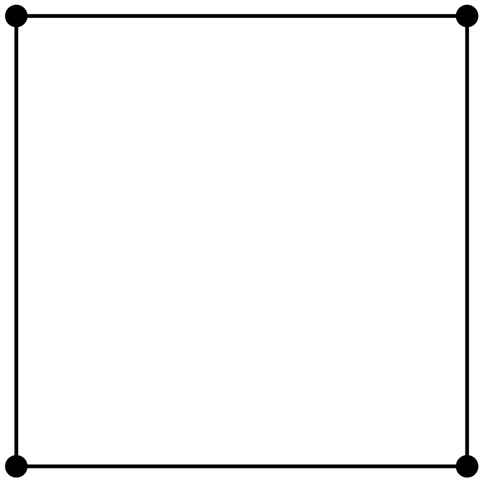
3.3.2 Eulerian graphs

Happy is the person who finds wisdom, and the person who gets understanding, for the gain from it is better than gain from silver and its profit better than gold. She is more precious than jewels, and nothing you desire can compare with her. Long life is in her right had; in her left hand are riches and honor. Her ways are ways of pleasantness, and all her paths are peace. *Proverbs* 3:13-17

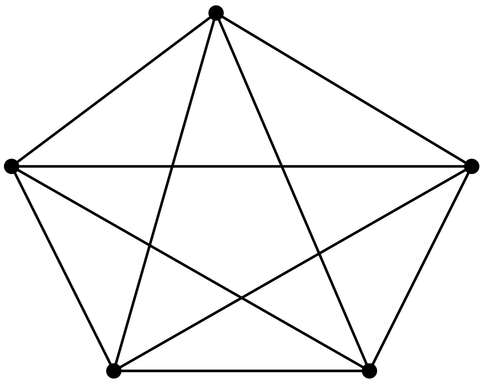
A graph is called *Eulerian* if there is a closed path in the graph that traverses each edge once and only once. Finding such a path is sometimes called the *highway inspector problem.* It is also the problem of tracing a graph without backtracking and without lifting the pencil from the paper.



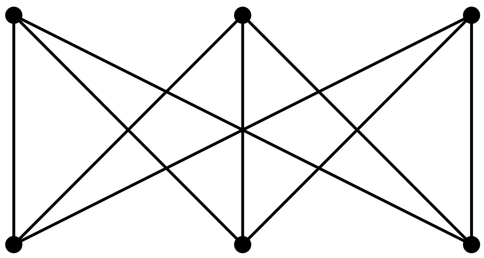
C_3 or K_3



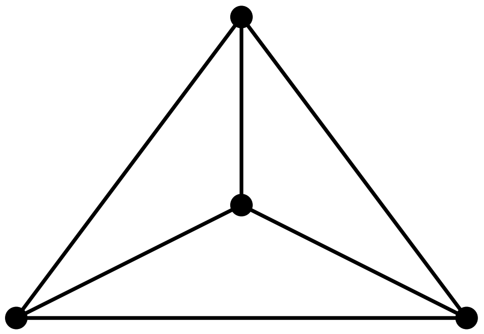
C_4 or $K_{2,2}$



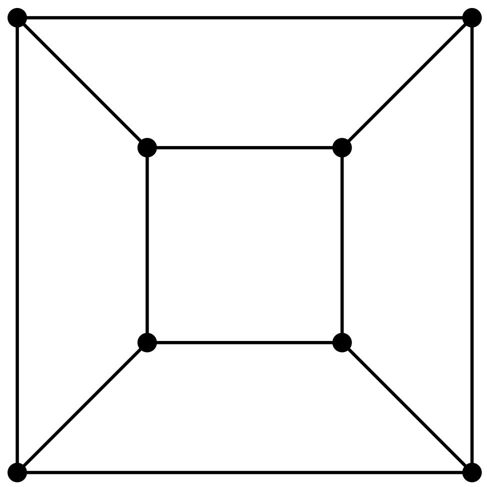
K_5



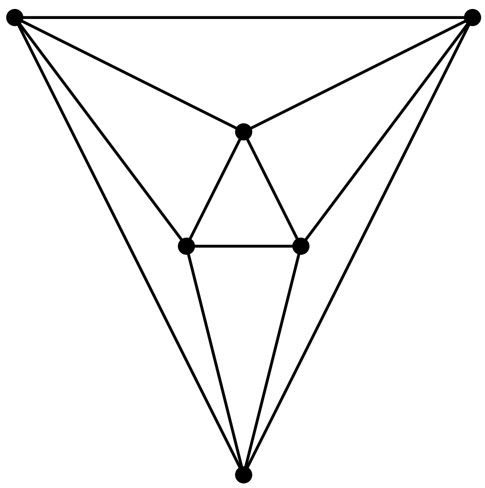
Utilities $K_{3,3}$



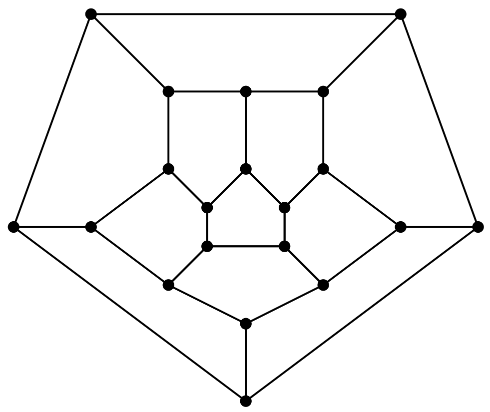
tetrahedron



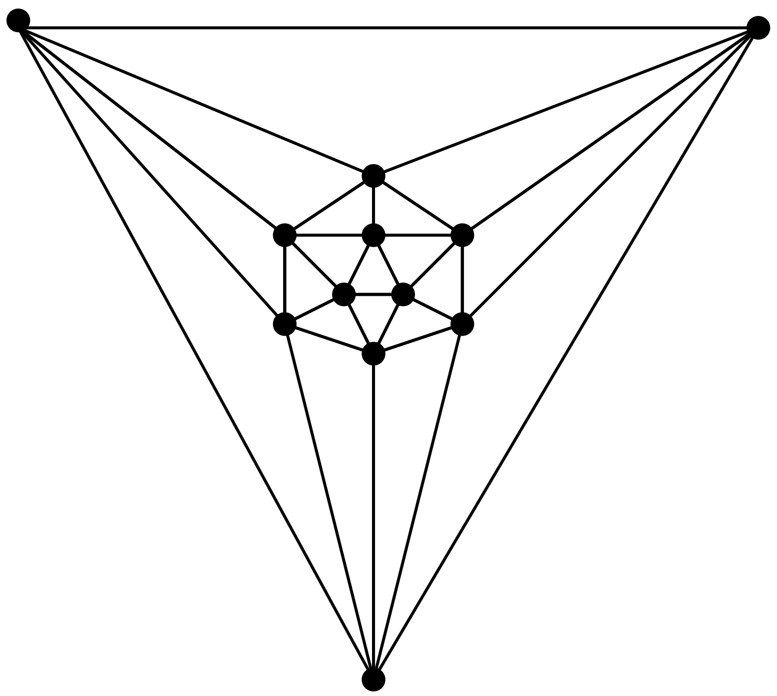
cube



octahedron

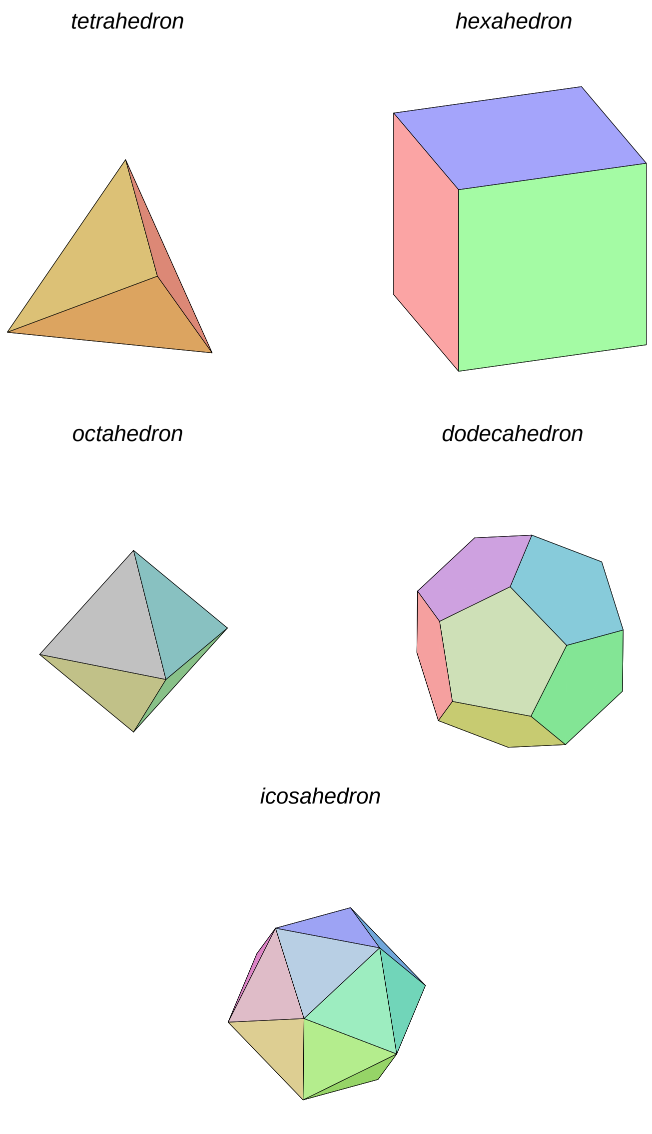


dodecahedron



icosahedron

Platonic Solids



Exercise 3.1. Which of the examples of graphs in section 3.3.1 are Eulerian? For those that are, find Eulerian paths.

Euler's seminal paper on the problem of the Königsberg bridges gives a necessary condition for a graph to be Eulerian: each vertex should have even degree. Euler implies, but does not prove, that the condition is also sufficient.

Exercise 3.2. Show that Euler's condition is sufficient by finding an algorithm for constructing Eulerian paths.

Hint: if you start anywhere and begin traversing edges at random, what could go wrong?

A *map* is a special kind of connected planar graph: one which cannot be broken into two pieces by removal of a single edge. (Such an edge is a *bridge*.) In particular, a map cannot have a dangling edge. The *faces* of a map are the connected components of its complement. The surrounding "ocean" (the unbounded component of the complement) is ordinarily counted as a face.

The famous four-color theorem states that the faces of an arbitrary map can be colored with (at most) four colors in such a way that no two faces sharing an edge have the same color. It is an interesting problem to determine which maps can be colored with fewer than four colors.

Evidently there are no interesting maps that can be colored with one color (for such maps are all ocean).

Exercise 3.3. Which maps can be colored with two colors?

3.3.3 Hamiltonian graphs

> While fancy, like the finger of a clock,
> Runs the great circuit, and is still at home.
>
> William Cowper
> 1731–1800
> *The Task*, Book iv
> The Winter Evening, line 118.

A graph is called *Hamiltonian* if there is a closed path in the graph that includes each vertex (other than the vertex that is the common start and end of the path) once and only once.

Exercise 3.4. Which of the examples of graphs in section 3.3.1 are Hamiltonian? For those that are, find Hamiltonian paths.

It is noteworthy that finding a characterization of Hamiltonian graphs (analogous to Euler's theorem for Eulerian graphs) is an unsolved problem.[1] Many theorems about Hamiltonian graphs say, roughly speaking, that if a graph has "enough" edges, then it is Hamiltonian.

Exercise 3.5. Show that a complete graph is Hamiltonian, for $n \geq 3$.

Exercise 3.6. If new edges are added to a Hamiltonian graph (without changing the set of vertices), then the resulting graph is still Hamiltonian.

Exercise 3.7. Prove *Dirac's theorem*: if the degree of each vertex in a graph is at least half the total number of vertices, then the graph is Hamiltonian. (It is assumed that there are at least three vertices, and that there are no multiple edges or loop edges).

Hint: Proof by contradiction. If the graph is not Hamiltonian, add edges until it is "just barely" non-Hamiltonian. Take a non-closed path through all the vertices and examine the collections of vertices adjacent to the beginning and the end of the path.

3.3.4 Euler's formula

A graph is said to be **planar** is it can be drawn in the plane with no edges crossing. Note that is often more convenient to draw them with edges crossing, so just looking a a graph with crossings doesn't determine whether or not it is planar.

A graph is said to be **simple** if it has no multiple edges nor loops.

Exercise 3.8. For those examples of graphs in section 3.3.1 that happen to be planar, count the number v of vertices, the number e of edges, the number f of faces, and then compute the quantity $v - e + f$.

Exercise 3.9. Euler's formula says that $v - e + f = 2$ for every connected planar graph.

1. Find a proof of Euler's formula by induction on the number of faces.

2. Find a proof of Euler's formula by induction on the number of edges.

[1] It is known that the problem of determining whether or not a given graph contains a Hamiltonian cycle is an NP-complete problem.

Exercise 3.10. Deduce the following facts from Euler's formula.

1. $e \leq 3v - 6$ for every simple, connected, planar graph with at least three vertices.

2. The complete graph K_5 on five vertices is not planar.

3. Every simple planar graph has a vertex of degree at most five.

3.3.5 Coloring graphs

> As geographers, Sosius, crowd into the edges of their maps parts of the world which they do not know about, adding notes in the margin to the effect that beyond this lies nothing but sandy deserts full of wild beasts, and unapproachable bogs. Plutarch
> *Life of Theseus*

If G is a planar graph, we form the *dual graph* by placing a vertex in each face of G, and for each edge of G that is incident to two faces, we make an edge in the dual graph that joins the vertices inside the two incident faces. For bridge edges of G, we get a loop edge in the dual graph.

Exercise 3.11. Determine the duals of the five Platonic graphs. (They turn out to be Platonic graphs again.)

Since maps have no bridge edges (by definition), the dual of a map is particularly simple to write down. It is clear that face colorings of maps correspond to vertex colorings of their dual graphs, so it is enough to study vertex coloring problems (which are technically simpler than face coloring problems).

Exercise 3.12. For each Platonic graph, determine the number of colors needed to color its faces so that adjacent faces are different colors; also determine the number of colors needed to color its vertices so that adjacent vertices are different colors.

Exercise 3.13. Prove by induction on the number of vertices that every planar graph is (vertex) six-colorable.

3.4 Problems

> It is a melancholy of mine own, compounded of many simples, extracted from many objects, and indeed the sundry contemplation of my travels, in which my often rumination wraps me in a most humorous sadness.
>
> William Shakespeare
> *As You Like It*, Act iv, scene 1

Problem 3.1. The complete tripartite graph $K_{r,s,t}$ consists of three sets of vertices (of sizes r, s, and t), with an edge joining two vertices if and only if the vertices lie in different sets.

1. How many edges does $K_{r,s,t}$ have?

2. Under what conditions on r, s, and t is $K_{r,s,t}$ an Eulerian graph?

Problem 3.2. Turán's extremal theorem: If a graph (with no loops and no multiple edges) has $2k$ vertices, but contains no triangles, then the graph has at most k^2 edges. Give a proof by induction, and show by example that this upper bound is attained.

Problem 3.3. In any gathering of six people, there must be either three people who all know each other, or three people who are all strangers to each other. Prove this, and reformulate it as a statement about graphs.

Problem 3.4. Let G be a graph (with no loops or multiple edges). Define the *line graph* $L(G)$ to be the graph having one vertex for each edge of G, two vertices of $L(G)$ being joined by an edge if and only if the corresponding edges of G have a common vertex.

1. Prove that if G is Eulerian, then so is $L(G)$.

2. Is the converse true? Prove or give a counterexample.

3. Characterize the graphs that are isomorphic to their line graphs.

Problem 3.5. Show that the line graph of an Eulerian graph is Hamiltonian.

Problem 3.6. The *mail carrier problem* asks for necessary and sufficient conditions on a graph for the existence of a closed path that includes each edge of the graph exactly twice. (A mail carrier must traverse both sides of each street.) Solve the problem.

Problem 3.7. At a dinner party, there are $2n$ guests to be seated at a round table. Each guest knows n of the other guests. Show that it is possible to seat the guests so that each is between two acquaintances.

Problem 3.8. Characterize the graphs admitting a path that is simultaneously Eulerian and Hamiltonian. Exhibit, on the other hand, a graph not of this type that is nonetheless simultaneously Eulerian and Hamiltonian.

Problem 3.9. Apply Euler's formula $v - e + f = 2$ to prove that the only regular polyhedra are the tetrahedron, the cube, the octahedron, the dodecahedron, and the icosahedron. (A regular polyhedron has congruent regular polygons for faces, and all of its vertex angles are equal.)

Problem 3.10.

1. Show that the (nonplanar) utilities graph $K_{3,3}$ can be drawn on the surface of a torus (donut) in such a way that no edges cross.
2. Show that the (nonplanar) complete graph K_5 on five vertices can be drawn on the surface of a torus in such a way that no edges cross.

Problem 3.11. Prove by induction on the number of vertices that every planar graph is (vertex) five-colorable. This can be done by adapting Kempe's false proof of the four-color theorem, or by using the fact (Exercise 3.10) that a planar graph cannot contain K_5.

3.5 Additional Literature

1. Martin Aigner, Turán's graph theorem, *American Mathematical Monthly* **102** (1995), 808–816.
2. Fred J. Rispoli, Applications of subgraph enumeration, in *Applications of Discrete Mathematics*, edited by John G. Michaels and Kenneth H. Rosen, McGraw-Hill, 1991, chapter 14, pages 241–262.

Chapter 4

Number Theory

In numbers warmly pure and sweetly strong.

William Collins
1720–1756
Ode to Simplicity

4.1 Goals

1. Recall or learn basic facts about the integers.
2. Appreciate the breadth of easily stated, unsolved problems that exist in number theory, especially problems about the integers.
3. Learn about Fermat's Little Theorem, Euler's ϕ function, and Euler's generalization of Fermat's Little Theorem.
4. Learn about and know how to use the Chinese Remainder Theorem to solve systems of equations exactly.

4.2 Reading

Then feed on thoughts, that voluntarie move
Harmonious numbers.

John Milton
1608-1674
Paradise Lost, Book III, lines 37–38

1. Ian Richards, "Number Theory," in *Mathematics Today: Twelve Informal Essays*, pages 37–63, edited by Lynn Arthur Steen, Springer-Verlag, 1978.

2. Ivars Peterson, "A Shortage of Small Numbers," in *Islands of Truth: A Mathematical Mystery Cruise*, pages 152–161, Freeman, 1990.

3. Victor Klee and Stan Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Dolciani Mathematical Expositions, No. 11, Mathematical Association of America, 1991, pages 173–181 and 203–214.

4. Robert Gray, "Georg Cantor and transcendental numbers," *American Mathematical Monthly* **101** (1994), no. 9, 819–832.

5. David M. Bloom, "A one-sentence proof that $\sqrt{2}$ is irrational," *Mathematics Magazine* **68** (1995), no. 4, 286.

6. Vincent P. Schielack, Jr., "Math Bite: A quick counting proof of the irrationality of $\sqrt[n]{k}$," *Mathematics Magazine*, **68** (1995), no. 5, 386.

7. Ivan Niven, "A simple proof that π is irrational," *Bulletin of the American Mathematical Society*, **53** (1947), 509.

8. Excerpts from Ivan Niven, *Irrational Numbers*, Mathematical Association of America, 1967, pages 16–27, 117–118, and 131–133.

9. Excerpt on Fermat theorems, in *A source book in mathematics, 1200-1800*, edited by Dirk Jan Struik, Harvard University Press, 1969, 1987, reprinted by Princeton University Press, pages 26–29.

10. Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, third edition, Addison-Wesley, 1992, pages 166–170 (the perpetual calendar).

11. Sue Geller, "Exact Solutions to Linear Systems," 1997.

4.3 Classroom Discussion

4.3.1 Basic Number Theory

As yet a child, nor yet a fool to fame,
I lisp'd in numbers, for the numbers came. Alexander Pope
1688-1744
Epistle to Dr. Arbuthnot, Prologue to the Satires, line 127

Theorem (Fundamental Theorem of Arithmetic)**.** *Suppose x is an integer larger than* 1*. Then x can be written uniquely in the form*

$$x = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m},$$

where the p_i are prime numbers ordered so that $p_1 < p_2 < \cdots < p_m$, and the n_i are positive integers.

Exercise 4.1. Prove the Fundamental Theorem of Arithmetic by induction.

You are familiar with various classes of numbers: the integers $\mathbf{Z}$, the rational numbers $\mathbf{Q}$, the real numbers $\mathbf{R}$, and the complex numbers $\mathbf{C}$. We know that $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. Often we separate the real numbers into the rational numbers and the irrational numbers, but there are two other common designations for real (and complex) numbers: *algebraic* and *transcendental*.

Definition. A (complex) number is called *algebraic* if it is a root of some polynomial with integer coefficients.

For example, 2, $\sqrt{2}$ and $i = \sqrt{-1}$ are algebraic since they are roots of the polynomials $x - 2$, $x^2 - 2$, and $x^2 + 1$ respectively. Notice that if a number α is a root of a polynomial $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with rational coefficients, then α is also the root of a polynomial with integer coefficients: namely $d \cdot p(x)$, where d is the least common multiple of the denominators of $a_0, a_1, \dots, a_n$.

Definition. A (complex) number is called *transcendental* if it is not algebraic.

Showing that a number is transcendental is the same as showing that it is not the root of any polynomial with integer coefficients. Since it is time consuming (not to say impossibly long!) to check every polynomial, one uses a proof by contradiction to show that a number α is transcendental. Suppose that α is algebraic: then ...? The trick is to find a contradiction. These proofs are generally not easy.

You are probably aware that e and π are transcendental numbers. It is somewhat easier to prove the weaker statement that e and π are irrational numbers. You will explore this in the reading.

> Take care of Number One. — Modern saying

Exercise 4.2. The first expedition to Mars found only the ruins of a civilization. The explorers were able to translate a Martian equation as follows:

$$5x^2 - 50x + 125 = 0 \qquad \therefore \quad x = 5 \text{ or } x = 8.$$

This is strange mathematics! The value $x = 5$ seems legitimate enough, but $x = 8$ requires explanation. If the Martian number system developed in a manner similar to ours, how many fingers did the Martians have?

Exercise 4.3. If $Anne_{\text{base } 8} - Anne_{\text{base } 5} = Anne_{\text{base } 7}$, then what digits do the letters A, n, and e represent?

4.3.2 Unsolved Problems

> Why is it that we entertain the belief that for every purpose odd numbers are the most effectual? — Pliny the Elder
> 23–79 A.D.
> *Natural History*, Book xxviii, sec. 23.

> The god delights in odd numbers.
> (*Numero deus impare gaudet.*) — Virgil
> 70–19 B.C.
> *Eclogue* VIII.75

Pierre de Fermat (1601–1665) wrote the following claim in the margin of a book by Diophantus and added that the margin was too small to contain the proof.

Theorem (Fermat's Last Theorem)**.** *If n is an integer greater than 2, then there are no positive integers x, y, and z such that $x^n + y^n = z^n$.*

For more than three centuries mathematicians tried to prove this claim, and recently Wiles and Taylor succeeded in completing a proof.[1] The claim, though curious in its own right, doesn't seem to have any use other than being pretty (excuse enough). Actually the following mathematics was developed in the attempts to prove Fermat's Last Theorem.

- Noetherian Rings
- Elliptic Curves
- Projective Plane
- Cyclotomic Extensions
- Modular forms
- Shimura and Taniyama-Weil Conjectures

One of our resident number theorists, Doug Hensley, who loves problems, was asked for some unsolved problems that he particularly likes and that are easy to state. The following is his reply.

Unsolved Problem 4.1. If the second difference of a sequence (a, b, c, d, e) of squares of positive integers in ascending order is $(2, 2, 2)$, does it follow that there exists an n so that $a = n^2$, $b = (n+1)^2$, $c = (n+2)^2$, $d = (n+3)^2$, $e = (n+4)^2$?

(The difference of a sequence in ascending order (a, b, c, d, e) is the sequence $(b-a, c-b, d-c, e-d)$. The difference of the difference is the second difference: $(c-2b+a, d-2c+b, e-2d+c)$. An example of such a sequence of squares is $(4, 9, 16, 25, 36)$.)

The betting is that the answer is "yes," and if so it would have interesting consequences for Diophantine equations and formal logic.

Unsolved Problem 4.2. Let $\pi(x)$ denote the number of primes from 2 to x, counting 2, and counting x if it is prime. Do there exist positive integers x and y (both larger than 2 to avoid trivial counterexamples) so that $\pi(x+y) > \pi(x) + \pi(y)$?

---

[1] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, *Annals of Mathematics (2)*, **141** (1995), number 3, 443–551; Andrew Wiles and Richard Taylor, Ring-theoretic properties of certain Hecke algebras, *Annals of Mathematics (2)*, **141** (1995), number 3, 553–572.

Again, the betting is that the answer is "yes," but the prospects of hitting upon x and y in a random search are slim. The first example probably involves very large x or y.

> Round numbers are always false. Samuel Johnson
> 1709–1784
> Boswell's *Life of Johnson*, vol. iii, p. 226 (30 March 1778)

Here are some books of unsolved problems; one of your readings is taken from the second one.

- *Unsolved Problems in Number Theory*, by Richard K. Guy, Problem Books in Mathematics, Volume 1, Springer-Verlag, 1981.
- *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Victor Klee and Stan Wagon, Dolciani Mathematical Expositions, No. 11, Mathematical Association of America, 1991.

4.3.3 Fermat's Little Theorem and Euler's Generalization

> Knowledge is more than equivalent to force. Samuel Johnson
> 1709–1784
> *The History of Rasselas, Prince of Abissinia*, Chapter 13

Definition. We say $a \equiv b \pmod{n}$ if and only if $b - a$ is divisible by n. For example, $27 \equiv 13 \pmod{7}$.

Exercise 4.4. Prove that congruence $\pmod{n}$ is an equivalence relation on the integers.

Definition. The set of equivalence classes $\pmod{n}$ is denoted by $\mathbf{Z}_n$.

Exercise 4.5. Prove that addition and multiplication are well defined in $\mathbf{Z}_n$. What are the units (elements with multiplicative inverses) in $\mathbf{Z}_n$?

> But what minutes! Count them by sensation, and not by calendars, and each moment is a day, and the race a life.
> Benjamin Disraeli, Earl Beaconsfield
> (1805–1881)
> *Sybil*, Book i, Chapter ii

Exercise 4.6 (The perpetual calendar)**.** Derive a formula that gives the day of the week of any day of any year in the Gregorian calendar. (The calendar in current use is called the Gregorian calendar because Pope Gregory set it up in 1582.) Care must be used in dealing with historical dates because different countries adopted the Gregorian calendar at different times. Britain and its colonies did not adopt the Gregorian Calendar until 1752. We were not the last to convert: Greece did not change over until 1923.

Proceed as follows. For days of the week, work modulo 7: Sunday = 0, Monday = 1, ..., Saturday = 6. For months, work modulo 12; since the extra day in leap year is in February, it is convenient to start in March: March = 1, April = 2, ..., February = 12. Thus, January and February are viewed as part of the previous year. For example, February 1984 is the 12th month of 1983 in this system. Use the following notation.

- W is the day of the week $(0, 1, 2, 3, 4, 5, 6)$.
- k is the day of the month $(1, 2, \ldots, 31)$.
- m is the month $(1, \ldots, 12)$.
- C is the century.
- Y is the particular year of the century $(0, 1, \ldots, 99)$.
- $N = 100C + Y$ is the year (for example, $1996 = N = 100C + Y$ where $C = 19$ and $Y = 96$).
- d_N is the day of the week of March 1 in year N.

The year Y is a leap year if $Y \neq 0$ and Y is divisible by 4 (notice that Y is divisible by 4 if and only if N is divisible by 4), or if $Y = 0$ and N is divisible by 400. For example, the years 1996 and 2000 are leap years, but the year 1900 is not a leap year.

1. Find d_N. Since $d_N \equiv d_{N-1} + \epsilon \pmod 7$, where ϵ equals 2 in a leap year and 1 otherwise, you can find d_N by counting leap years from some reference date (say 1600). In 1995, March 1 was a Wednesday.

2. Next find the first day of month m in year N. You can do this by finding a function $f(m)$ that matches the shift in the day of the week from

March to month m. Hint: What is the average shift? You can express the function f by using the function $\lfloor x \rfloor$ that represents the greatest integer less than or equal to x.

3. Adjust for the kth day of the month and gather the final formula for $W \equiv d_N + f(m) + k - 1 \pmod 7$.

Theorem (Fermat's Little Theorem). *Suppose a is a positive integer, and p is a prime number that does not divide a. Then $a^{p-1} \equiv 1 \pmod p$.*

Soft is the Strain when Zephyr gently blows,
And the smooth Stream in smoother Numbers flows;
But when loud Surges lash the sounding Shore,
The hoarse, rough Verse shou'd like the Torrent roar.

Alexander Pope
(1688–1744)
An Essay on Criticism, Part II

Exercise 4.7. Use induction to prove Fermat's Little Theorem.

Fermat's Little Theorem is quite useful in computing $\pmod n$. Here is an example $\bmod 7$:

$$\begin{aligned}
(12)^{53} &= ((12)^6)^8 \cdot (12)^5 \\
&\equiv 1^8 \cdot 5^5 && \pmod 7 \\
&= (25)^2 \cdot 5 \\
&\equiv 4^2 \cdot 5 && \pmod 7 \\
&\equiv 10 && \pmod 7 \\
&\equiv 3 && \pmod 7.
\end{aligned}$$

However, to use Fermat's Little Theorem one must have a prime modulus, a luxury that does not always arise. Euler noticed that $p - 1$ is the number of units in $\mathbf{Z}_p$ when p is prime, so he made the following definition.

Definition (Euler's ϕ Function). When n is a positive integer, $\phi(n)$ is the number of integers between 1 and n (inclusive) that are relatively prime to n.

For example, $\phi(12) = 4$ because the four numbers 1, 5, 7, 11 are relatively prime to 12.

Exercise 4.8. Find a formula for $\phi(n)$ as follows.

1. Find $\phi(p^r)$ when p is a prime.
2. Prove that $\phi(st) = \phi(s)\phi(t)$ when s and t are relatively prime. (You may want to start with the case that s and t are primes.)

Exercise 4.9. Compute $\phi(54)$ by applying the result of the previous exercise.

Theorem (Euler's generalization of Fermat's little theorem)**.** *If x and $n > 1$ are positive integers that are relatively prime, then $x^{\phi(n)} \equiv 1 \pmod{n}$.*

Exercise 4.10. Compute $25^{86} \pmod{21}$ by applying the previous theorem.

Exercise 4.11. Use induction to prove Euler's generalization of Fermat's little theorem.

4.3.4 Chinese Remainder Theorem

And wisely tell what hour o' the day
The clock does strike, by algebra.

Samuel Butler
(1612–1680)
Hudibras, Part I, Canto i, line 125

Suppose we want to solve the pair of congruences $x \equiv 4 \pmod{7}$ and $x \equiv 14 \pmod{30}$ for x. (This could be asking to find a day of the week and a time of the month in terms of the entire year.) Is there a solution? What is a good way to find it? The ancient Chinese worked out a method that is still computationally viable.

Theorem (Chinese Remainder Theorem)**.** *Every system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned}$$

where the m_i are pairwise relatively prime, has a solution. Furthermore, every two solutions are congruent $\bmod M$, where $M = m_1 m_2 \ldots m_k$.

Exercise 4.12. Prove the Chinese Remainder Theorem constructively as follows.

1. If $M_i = M/m_i$, then what is $\gcd(M_i, m_i)$?

2. Find a way to determine c_i so that $c_i M_i \equiv 1 \pmod{m_i}$.

3. Use the a_i, c_i, and M_i to get a formula for a solution x_0.

4. Show that if $x_1 \equiv a_i \pmod{m_i}$ for all i, then $x_1 \equiv x_0 \pmod{M}$.

Exercise 4.13. Use the Chinese Remainder Theorem to solve the following pair of congruences for x.

$$\begin{aligned} x &\equiv 4 \pmod{7} \\ x &\equiv 14 \pmod{30} \end{aligned}$$

4.3.5 Exact Solutions to Systems of Equations

Now noisy, noxious numbers notice nought,
Of outward obstacles o'ercoming ought;
Poor patriots perish, persecution's pest!
Quite quiet Quakers "Quarter, quarter" quest;
Reason returns, religion, right, redounds,
Suwarrow stop such sanguinary sounds!

Alliteration, or the Siege of Belgrade: a Rondeau

In this age of computers, round-off errors can be a major problem. Consequently, it is to our advantage to solve systems of equations using integer arithmetic. A method for doing this was in the reading.

Exercise 4.14. Solve the following system of equations, first by picking a large enough prime and using the procedure of the reading, and then by picking a large enough composite of small primes and using the procedure of the reading and the Chinese Remainder Theorem.

$$\begin{aligned} 5x_1 - 3x_2 &= 3 \\ 4x_1 - x_2 &= 6 \end{aligned}$$

4.4 Problems

> For words are wise men's counters; they do but reckon by them: but they are the money of fools.
>
> Thomas Hobbes
> (1588–1679)
> *Leviathan*, Part I, Chapter IV

Problem 4.1. So that we may start with a common vocabulary, please review the following concepts that are often used in number theory.

- a divides b or $a \mid b$ (for integers a and b)
- prime number
- relatively prime
- gcd or greatest common divisor
- lcm or least common multiple
- division algorithm
- Euclidean algorithm
- linear combination

Number theory has intrigued many people, non-mathematicians and mathematicians alike. Problems in number theory come in many varieties at various levels of complexities. The following are some fun ones for you to solve. (Have fun. That is an order!)

4.4.1 Cryptoanalysis

Problem 4.2. The dep ression was no joke, but this joke came out of the depression. The different letters represent different digits. Find them.

$$\begin{array}{ccccc} USA & + & FDR & = & NRA \\ USA & + & NRA & = & TAX \end{array}$$

Problem 4.3. Our good friend and eminent numerologist, Professor Euclide Paracelso Umbugio, has been busily engaged testing on his calculator the $81 \cdot 10^9$ possible solutions to the problem of reconstructing the following exact long division problem in which digits indiscriminately were each replaced by x.

Deflate the Professor! That is, reduce the possibilities to $(81 \cdot 10^9)^0$.

$$
\begin{array}{ccccccccccc}
 & & & & & & x & x & 8 & x & x \\
\cline{4-11}
x & x & x & \multicolumn{1}{|c}{x} & x & x & x & x & x & x & x \\
 & & & & x & x & x & & & & \\
\cline{4-7}
 & & & & & x & x & x & x & & \\
 & & & & & & x & x & x & & \\
\cline{6-9}
 & & & & & & & x & x & x & x \\
 & & & & & & & x & x & x & x \\
\cline{8-11}
\end{array}
$$

(This problem is at least half a century old, but the original source is unknown. The problem appeared, for example, as problem E 1111 in the *American Mathematical Monthly* in 1954.)

Problem 4.4. Each letter represents a distinct digit in the decimal scale. Identify the digits.

$$7 \cdot (FRYHAM) = 6 \cdot (HAMFRY)$$

Problem 4.5. Each letter represents a distinct digit in the decimal scale. Identify the digits.[2]

$$(NAUGHT)^3 = (ZERO)^4$$

Problem 4.6. After making an ordinary arithmetic multiplication, a student replaced every even digit with E and every odd digit with O. The result is shown below. What was the multiplication?

$$
\begin{array}{cccc}
 & \mathrm{O} & \mathrm{E} & \mathrm{E} \\
 & & \mathrm{E} & \mathrm{E} \\
\hline
\mathrm{E} & \mathrm{O} & \mathrm{E} & \mathrm{E} \\
\mathrm{E} & \mathrm{O} & \mathrm{E} & \\
\hline
\mathrm{O} & \mathrm{O} & \mathrm{E} & \mathrm{E}
\end{array}
$$

[2] Alan Wayne, *Journal of Recreational Mathematics* **12** (1980), 288.

4.4.2 Other types of number puzzles

Problem 4.7. On April 1, 1946, the *Erewhon Daily Howler* carried the following item: "The famous astrologer and numerologist of Guayazuela, the Professor Euclide Paracelso Bombasto Umbugio, predicts the end of the world for the year 2141. His prediction is based on profound mathematical and historical investigations. Professor Umbugio computed the value of the formula

$$1492^n - 1770^n - 1863^n + 2141^n$$

for $n = 0, 1, 2, 3$, and so on, up to 1945, and found that all the numbers which he obtained in many months of laborious computation are divisible by 1946. Now, the numbers 1492, 1770, and 1863 represent memorable dates: the Discovery of the New World, the Boston Massacre, and the Gettysburg Address. What important date may 2141 be? That of the end of the world, obviously."

Deflate the professor! Obtain his result with little computation.

Problem 4.8. Not all large numbers are hard to factor. Find all the prime factors of $1,000,027$ by hand, without much work.

> This is the third time; I hope good luck lies in odd numbers. Away I go. They say there is divinity in odd numbers, either in nativity, chance, or death. William Shakespeare
> *The Merry Wives of Windsor*, Act V, Scene i

> What I tell you three times is true. Lewis Carroll
> *The Hunting of the Snark: an Agony in Eight Fits*

Problem 4.9. If p_1 and p_2 are consecutive odd primes (that is, $p_2 - p_1 = 2$), then $p_1 + p_2$ is even, and so can be written in the form $2q$. Show that q is composite.

Problem 4.10. Does there exist a positive integer whose prime factors include at most the primes 2, 3, 5, 7, and which ends in the digits 11? If so, find the smallest such positive integer; if not, show why none exists.

Problem 4.11. In which bases b are $35_{\text{base } b}$ and $58_{\text{base } b}$ relatively prime?

Problem 4.12. Show that an integer in an odd base system is odd in the base 10 system if and only if it has an odd number of odd digits. (For example, $111_{\text{base } 3}$ is $9 + 3 + 1 = 13$ in base 10 and is odd.)

The above puzzles were taken from

- *150 Puzzles in Crypt-Arithmetic*, by Maxey Brooke, 2nd rev. ed., Dover, New York, 1969.
- *Mathematical Quickies*, by Charles W. Trigg, Dover, New York, 1985.
- *The Wohascum County Problem Book*, by George T. Gelbert, Mark I. Krusemeyer, and Loren C. Larson, Dolciani Mathematical Expositions, No. 14, Mathematical Association of America, 1993.

Problem 4.13 (Fractals with Moduli)**.** For the first 10 lines of Pascal's Triangle, replace the odd numbers by black squares and the even numbers by white squares. Conjecture a formula for which rows are all black. See if you can prove your formula.

Problem 4.14 (Perpetual Calendar)**.** 1. Is the probability that Christmas falls on a Wednesday equal to 1/7? Prove or disprove.

2. True or False: The 13th of the month falls on Friday more often than any other day. How might you go about justifying your answer? If the method is long or tedious, just give a method.

Problem 4.15. Use Fermat's Little Theorem and modular arithmetic to compute the following by hand (not computer).

1. $(3100)^{76} \pmod{17}$. Give an answer between 0 and 16.
2. $(200)^{37} \pmod{21}$. Give an answer between 0 and 20.
3. Prove that $n^{33} - n$ is divisible by 15 for every positive integer n.

Problem 4.16. Use the Chinese Remainder Theorem and both the techniques (taking M prime or composite) from the reading "Exact Solutions to Systems of Equations" to solve the following system.

$$\begin{aligned} 3x_1 + x_2 &= 1 \\ 2x_1 + 3x_2 &= 2 \end{aligned}$$

Priestley was the first (unless it was Beccaria) who taught my lips to pronounce this sacred truth, that the greatest happiness of the greatest number is the foundation of morals and legislation.

Jeremy Bentham
(1748–1832)
The Commonplace Book (*Works*, volume x, page 142)

That action is best, which procures the greatest happiness for the greatest numbers.

Francis Hutcheson
(1694–1746)
Treatise II. *Concerning Moral Good and Evil*, section 3, line 8

Chapter 5

Codes

Mastering the lawless science of our law,—
That codeless myriad of precedent,
That wilderness of single instances.

Alfred, Lord Tennyson
(1809–1892)
Aylmer's Field

5.1 Goals

1. Learn some cryptography, especially what RSA codes are and how to use them.

2. Learn about error-correcting codes and their uses.

3. Gain an appreciation of the usefulness of some mathematics that was originally studied for its beauty, not its utility.

5.2 Reading

Such graves as his are pilgrim shrines,
Shrines to no code or creed confined,—
The Delphian vales, the Palestines,
The Meccas of the mind.

Fitz-Greene Halleck
(1790–1867)
Burns

1. Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, third edition, Addison-Wesley, 1992, 234–245.

2. Joseph Gallian, "Math on Money," *Math Horizons*, Mathematical Association of America, November, 1995, 10–11.

3. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* **21** (1978), 120–126. Available as LaTeX source and as PostScript on Rivest's home page at `http://theory.lcs.mit.edu/~rivest/publications.html`.

4. Sue Geller, An Introduction to Error-Correcting Codes, 1997.

5. Daniel Pedoe, *The Gentle Art of Mathematics*, Macmillan, 1959 (Collier, 1963; Dover, 1973), pages 18–21 (excerpt on Nim).

5.3 Classroom Discussion

5.3.1 Cryptography

> When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.
>
> Anonymous

In the reading, you learned about Caesar ciphers and shift transformations. A product cipher is simply the composition of two (or more) ciphers.

Exercise 5.1.

1. Find the product cipher obtained by using the transformation $C_1 \equiv 5P + 13 \pmod{26}$ followed by the transformation $C_2 \equiv 17P + 3 \pmod{26}$. (Rosen, exercise 15 on page 243)

2. Find the product cipher obtained by using the transformation $C_1 \equiv aP + b \pmod{26}$ followed by the transformation $C_2 \equiv cP + d \pmod{26}$, where $\gcd(a, 26) = \gcd(c, 26) = 1$. (Rosen, exercise 16 on page 243)

Instead of enciphering each letter of a plaintext message in the same way, we can vary how we encipher letters. For example, a *Vigenère* cipher operates in the following way. A sequence of letters $\ell_1, \ell_2, \ldots, \ell_n$, with numerical equivalents $k_1, k_2, \ldots, k_n$, serves as the key. Plaintext messages are split into blocks of length n. To encipher a plaintext block of letters with numerical equivalents $p_1, \ldots, p_n$ to obtain a ciphertext block of letters with numerical equivalents $c_1, \ldots, c_n$, we use a sequence of shift ciphers with $c_i \equiv p_i + k_i \pmod{26}$ for each i.

Exercise 5.2. (Rosen, exercises 17 and 18, page 243.) Using a Vigenère cipher with key `SECRET` and setting `A` $= 0$,

1. encipher the message `DO NOT OPEN THIS ENVELOPE`;
2. decipher the message `WBRCSL AZGJMG KMFV`.

5.3.2 RSA Code

Exercise 5.3. Given that $n = 65$ and $d = 11$ in an RSA code, find e.

Exercise 5.4. Does RSA encryption guarantee that the message is obscured? Suppose that $n = 15$, and the block size is 2. How many of the allowable code blocks are encoded to themselves when $e = 3$? when $e = 5$? That is, how many X are there such that $0 \le X \le 14$ and $X^e \equiv X \pmod{n}$ when $e = 3$? when $e = 5$?

Exercise 5.5. Use the square and multiply method to decode the message 28717160 when $n = 77$ and $d = 13$. (For the letter/number correspondence, set `A` $= 1$.)

Exercise 5.6. The Evil Empire thinks it is clever. Their cryptographers tell the world to send them messages in an RSA code with $n = 10573$ and $e = 2531$ and claim that this is a secure method. They know that education in Goodguyland has deteriorated, so that people know theorems such as the Fundamental Theorem of Arithmetic, but have forgotten how to factor numbers as large as n. A clever agent from Goodguyland steals the information (bribery is suspected) that $\phi(n) = 10368$. How can the Spooks of Goodguyland now decode all the messages that the Evil Empire receives?

5.3.3 Error-Correcting Codes

Truth crushed to earth shall rise again,—
The eternal years of God are hers;
But Error, wounded, writhes with pain,
And dies among his worshippers.

William Cullen Bryant
(1794–1878)
The Battle-Field

Exercise 5.7. Prove that the distance function on code words is a metric; that is, the distance function satisfies the following three properties.

1. $d(u, v) = 0$ if and only if $u = v$.
2. $d(u, v) = d(v, u)$.
3. $d(u, w) \leq d(u, v) + d(v, w)$.

Exercise 5.8. Prove that the minimum distance between two code words in a code C is d if and only if C can correct $\lfloor (d-1)/2 \rfloor$ or fewer errors via maximum-likelihood decoding.

Exercise 5.9. Let C be the binary code whose generator matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

1. Find a parity check matrix for C.
2. Determine the syndromes for C.
3. Construct the standard array for C.
4. Make a syndrome and coset leader table.
5. Use the table you constructed to decode 101111 and 111111.
6. Calculate the probability of decoding correctly assuming that the probability of correct transmission of a bit is $p = 0.9$. What is the probability of receiving a message correctly if no coding is used?

Exercise 5.10. Construct a standard array for the ternary Hamming $(4, 2, 3)$ code. (Here $q = 3$ and $r = 2$.)

5.3.4 Nim

The game of Nim can be solved by using number theory or by using an area of mathematics called game theory. We are going to discuss the game of Nim as a bridge between the two areas. Nim is a two-person game that can be played with any small objects, such as matches, tokens, poker chips, m&m's,

chocolate chips. We will assume the use of matches. To start the game, some piles of matches (it doesn't matter how many piles, but three is typical), each with an arbitrary number of matches, are placed on a flat surface. Each player in turn can take as many matches as desired, but at least one, from any one pile. The person who takes the last match wins. (In an alternate version of the game, the person who takes the last match loses.)

For example, suppose there are 2, 7, 6 matches in the initial piles. If Player A chooses to take three matches from the second pile, then there are 2, 4, 6 matches in the piles. If Player B takes all 6 matches of the third pile (leaving 2, 4, 0 matches in the piles), then Player A should take two matches from the second pile (leaving 2, 2, 0). If Player B takes both matches from one pile, Player A can take both matches from the other pile and win. If Player B takes one match from a pile, then Player A should take one match from the other pile so that, whatever pile Player B chooses, Player A takes the last match and wins.

Exercise 5.11. Devise a winning strategy for Nim in each of its versions. You might want to try a few games first.

5.4 Problems

Errors, like straws, upon the surface flow;
He who would search for pearls must dive below. John Dryden (1631–1701)
All for Love. Prologue

Problem 5.1. An affine transformation $C \equiv aP+b \pmod{26}$ was used to encipher the message `PJXFJ SWJNX JMRTJ FVSUJ OOJWF OVAJR WHEOF JRWJO DJFFZ BJF`. Use frequencies of letters to determine a and b and to recover the plaintext.

Problem 5.2. Another type of cipher or cryptosystem is a replacement cipher: let τ be a permutation of the alphabet, and apply τ to each letter of the message. Frequency analysis is useful for breaking this type of code, just as it was in the shift cipher. Decode the following, which was encoded using a replacement cipher.

```
MIZVN  KXXHA  XRRTK  NXYEX  QIZVI
IZXWM  NXYGT  JWVHC  YTOXX  QNHTI
JYTWV  NMHUR  XOYLN  ZTJTE  XYAZX
RWMHU  XEMRK  LIJYT  WNWVR  REXPV
IMTHN  OTHIM  HLVRR  GYXCX   VIXQ
        ---   NVWLX  RBTZH   NTH
```

Problem 5.3. Pick n, d, and e to use in your own public key cryptosystem, and encrypt a message. Turn in the answer in two parts: first give the public information and the encrypted message, and then give your decryption key and the original message.

Problem 5.4. If the probability of a digit being received correctly is 0.9, what is the probability of having a correct message after decoding the send-it-three-times code with three information digits? How does this compare with the probability of receiving a three-digit message correctly without any coding?

Problem 5.5. Find eight binary vectors of length 6 such that $d(u, v) \geq 3$ for every pair (u, v) of the vectors.

Problem 5.6. Is it possible to find nine binary vectors of length 6 such that $d(u, v) \geq 3$ for every pair (u, v) of the vectors?

Problem 5.7. Give generator and parity check matrices for the binary code consisting of all even weight vectors of length 8.

Problem 5.8. If C is an (n, k, d) code with $n > 1$, prove that any vector of weight $\lfloor (d-1)/2 \rfloor$ or less is a unique coset leader.

Problem 5.9. Show that if d is the minimum weight of a code C, this weight d is even, and $t = \lfloor (d-1)/2 \rfloor$, then there are two vectors of weight $t+1$ in some coset of C.

Problem 5.10. A generator matrix $G = (I\ A)$ for the ternary $(12, 6)$ Golay code has

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Show that this code has minimum weight 6.

Problem 5.11. Let C be a perfect binary code with minimum weight 7. Show that $n = 7$ or $n = 23$.

Chapter 6

Constructibility

It 's wiser being good than bad;
It 's safer being meek than fierce;
It 's fitter being sane than mad.
My own hope is, a sun will pierce
The thickest cloud earth ever stretched;
That after Last returns the First,
Though a wide compass round be fetched;
That what began best can't end worst,
Nor what God blessed once prove accurst.

Robert Browning
(1812–1890)
Apparent Failure, vii

6.1 Goals

The measure of a man's life is the well spending of it, and not the length.

Plutarch
(circa 46–circa 120 A.D.)
Consolation to Apollonius

1. Understand what the Greeks meant by a number being constructible.
2. Understand what the Greeks meant by a figure being constructible.
3. Learn the algebra of polynomial rings.
4. Learn about extension fields.

5. Be able to determine whether or not a given real number is constructible.

6.2 Reading

1. Sue Geller, Algebra for Constructibility, 1998.
2. Sue Geller, Factoring Polynomials, 1997.

6.3 Classroom Discussion

6.3.1 Classical Constructions

> There 's no art to find the mind's construction in the face.
>
> William Shakespeare
> *Macbeth*, Act I, scene 4

The ancient Greeks knew about rulers, but only the kind that govern a country. They did not have rulers for measurement, nor even an idea of standardized measurement—nor did the rest of the world. In fact, one of the "standard" units of measurement, the cubit, was the length of the ruler's (e.g., king's) right arm from the elbow to the end of the middle finger. Another standard measure was the "foot" which was the length of the ruler's right foot. So when the ruler changed, so did the length of the cubit and the foot. It was even worse when the ruler was a growing child! Think about what it meant to the economy to have a changing unit of length.

But the Greeks still wanted to create lengths and figures in a repeatable way. They did have a straight-edge with which to draw lines and a compass with which to draw circles. Their compasses would not stay open like ours do, so they couldn't just put the points at the ends of a line segment and copy that segment elsewhere, but they did have a procedure to produce a reliable copy. For our purposes, we will use the modern compass that can easily copy a line segment.

> A narrow compass! and yet there
> Dwelt all that 's good, and all that 's fair;
> Give me but what this riband bound,
> Take all the rest the sun goes round.
>
> Edmund Waller
> (1605–1687)
> *On a Girdle*

What the Greek mathematicians did was to start with a given unit of length and to work from there. Their idea was that a number ℓ (a length) is *constructible* if, starting with a given unit length, one can construct a line segment of length $|\ell|$ units in a finite number of steps using only a straight-edge and a compass. By putting such line segments together (again with straight-edge and compass), they could make various geometric figures. For example, they could construct an equilateral triangle, a square, a regular pentagon, a regular hexagon, an angle bisector, a perpendicular bisector, a perpendicular from a point to a line, a line through a given point parallel to a given line, and, of course, a circle. However, they could not figure out how to construct a regular heptagon (a seven-sided figure), how to trisect every angle, or how to construct a square with the same area as a given circle.

According to legend, the oracle at Delos told the Athenians that a plague would end if they constructed a new altar to Apollo in the shape of a cube, but with double the volume of the existing one. However, they found no way to "double a cube" using straight-edge and compass constructions. The story recorded by Eratosthenes, as it comes to us through Theon of Smyrna, shows that public relations is an old art. When Plato was consulted, he declared the meaning of the oracle to be not that Apollo required a new altar, but that the Greeks needed to pay more attention to mathematics.

> Double, double toil and trouble;
> Fire burn, and cauldron bubble.
>
> William Shakespeare
> *Macbeth*, Act iv, scene 1

The straight-edge and compass constructions at which the Greeks failed were worked on for over two millennia until Gauss, Wantzel, Lindemann, and others showed in the 1800s that these constructions are impossible. In this chapter, you too will show the non-constructibility of the classical Greek objects. We start by looking at what lengths *can* be constructed.

Exercise 6.1. Suppose that α and β are constructible numbers. Show that $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, α/β (if $\beta \neq 0$), and $\sqrt{\alpha}$ (if $\alpha > 0$) are constructible.

Recall that a *field* is a set that is closed under two binary operations, called addition and multiplication, such that both operations are commutative and associative, both have identities, the distributive laws hold, every element has an additive inverse, and every non-zero element has a multiplicative inverse. In Exercise 6.1 you proved that the set of constructible numbers is a subfield of the real numbers that is closed under taking square roots. The constructible numbers are sometimes called the "surds", although in keeping with the cognate word "absurd", a surd is strictly speaking an irrational number.

> Yet what are all such gaieties to me
> Whose thoughts are full of indices and surds? Lewis Carroll
> *Phantasmagoria*

We can build the surds one step at a time. If F is a subset of K, and both F and K are fields under the same operations, then we say that F is a *subfield* of K and that K is an *extension field* of F.

Exercise 6.2. Let $\mathbf{Q}[\sqrt{2}\,] = \{a + b\sqrt{2} \,:\, a, b \in \mathbf{Q}\}$. Show that this set is a subfield of the field of real numbers.

We can continue to build the surds by finding an extension field of $\mathbf{Q}[\sqrt{2}\,]$ that is also contained in the surds. Precisely how we do this will have to wait for later.

Now we have a list of procedures for constructing new surds from old ones. Is this list complete, or are there other ways to obtain constructible numbers?

For any subfield F of the real numbers we can think of the plane of F as the set of points in the real plane that have both coordinates in F. Thus a line in F has an equation $ax+by+c = 0$, where a, b, and c are elements of F. Likewise, a circle in F has an equation of the form $x^2+y^2+ax+by+c = 0$, where a, b, and c are elements of F. Since all our straight-edge and compass constructions are done with lines and circles, all numbers that can be constructed from numbers in F can be obtained from a sequence of intersections of lines and circles in F. To prove the converse of Exercise 6.1, you must show that intersections of two lines, a line and a circle, and two circles can be obtained using only field operations and extraction of square roots.

> Though pleased to see the dolphins play,
> I mind my compass and my way. Matthew Green
> (1696–1737)
> *The Spleen*

Exercise 6.3. Show that the surds consist precisely of those real numbers that can be obtained from the rational numbers by applying field operations and taking square roots in some order a finite number of times.

In order to double a cube, we need to be able to construct $\sqrt[3]{2}$, which doesn't look like it can be done by a sequence of the operations of addition, subtraction, multiplication, division, and extraction of square roots; but how do you know that it can't? To prove the impossibility, we need to take a side path into the area of algebra called field extensions.

6.3.2 Polynomials and Field Extensions

> Consider the lilies of the field, how they grow; they toil not, neither do they spin. *Matthew* 6:28

We start with some material on polynomial rings as defined in the reading.

Exercise 6.4. Prove the following theorem and corollaries from the reading.

Theorem (Division Algorithm)**.** *Let $f, g \in F[x]$, where F is a field and $g \neq 0$ (or F is a ring and g is monic). Then there exist unique polynomials $q, r \in F[x]$ such that $f = qg + r$, where either $r = 0$ or $\deg(r) < \deg(g)$.*

Corollary 1 (Remainder Theorem)**.** *Let R be a ring, $a \in R$, and $f \in R[x]$. Then there exists a polynomial $q \in R[x]$ such that $f(x) = (x - a)q(x) + f(a)$.*

Corollary 2 (Factor Theorem)**.** *The number a is a root of the polynomial f (that is, $f(a) = 0$) if and only if the first-degree polynomial $x - a$ is a factor of f.*

Corollary 3. *A polynomial of degree n with coefficients in a field F (or in $\mathbf{Z}$) has at most n roots in F (or in $\mathbf{Z}$).*

> For out of the old fieldes, as men saithe,
> Cometh al this new corne fro yere to yere;
> And out of old bookes, in good faithe,
> Cometh al this new science that men lere. Geoffrey Chaucer (1328–1400)
> *The Assembly of Fowles*, line 22

Exercise 6.5. Use the first isomorphism theorem and the evaluation homomorphism to show that $\mathbf{C} \cong \mathbf{R}[x]/(x^2 + 1)$.

Exercise 6.6. Prove the following result.

Theorem. *Suppose that F is a subfield of K, and α is an element of K that is algebraic over F. If m is the minimal polynomial of α over F, then $F[\alpha] \cong F[x]/(m)$.*

Exercise 6.7. Use the preceding theorem to prove the following corollary.

Corollary 4. *If $f \in F[x]$ is irreducible, then there is an extension field of F that contains a root of f.*

Exercise 6.8. Prove that if $F \subseteq E \subseteq K$ is a tower of finite field extensions, then $[K : F] = [K : E]\,[E : F]$. (Hint: Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis for E over F, and let $\{\beta_1, \ldots, \beta_n\}$ be a basis for K over E. Can you construct a basis for K over F?)

6.3.3 Constructibility

> If you choose to represent the various parts in life by holes upon a table, of different shapes,—some circular, some triangular, some square, some oblong,—and the persons acting these parts by bits of wood of similar shapes, we shall generally find that the triangular person has got into the square hole, the oblong into the triangular, and a square person has squeezed himself into the round hole. The officer and the office, the doer and the thing done, seldom fit so exactly that we can say they were almost made for each other.
>
> Sydney Smith
> (1769–1845)
> *Sketches of Moral Philosophy*

Now that we have the algebra machinery at hand, we can prove a theorem that will allow us to test when a number is constructible.

Theorem. *Let $\alpha \in \mathbf{R}$. Then α is constructible $\Longrightarrow$ $[\mathbf{Q}[\alpha] : \mathbf{Q}] = 2^n$ for some non-negative integer n. Equivalently, α is constructible $\Longrightarrow$ $\deg(\mathrm{irr}(\alpha, \mathbf{Q})) = 2^n$, where $irr(\alpha, \mathbf{Q})$ is the minimal polynomial of α over $\mathbf{Q}$.*

Actually the implication in the above theorem is an equivalence (if and only if), but we need only the direction stated above and the proof of the other direction uses material we have not studied.

Exercise 6.9. Prove the above theorem.

Now it is easy to tell if a number is constructible. For example, consider the case of doubling a cube. We want to know if $\sqrt[3]{2}$ is constructible. We know that $\sqrt[3]{2}$ is a root of $x^3 - 2$, and the other two roots are complex numbers. Since none of the roots is rational, $x^3 - 2$ is irreducible over $\mathbf{Q}$. Therefore $[\mathbf{Q}[\sqrt[3]{2}] : \mathbf{Q}] = 3$, which is not a power of 2. Thus $\sqrt[3]{2}$ is not constructible, and so we cannot double a cube using only straight-edge and compass.

Exercise 6.10. Show that a square with the same area as a circle of unit radius is not constructible with straight-edge and compass.

In the next exercise you will see what angles are constructible by showing that an angle θ is constructible if and only if $\cos\theta$ is constructible. The question then arises of how to find a minimal polynomial for $\cos\theta$. A common way to do this is to choose a positive integer n for which we know that $\cos n\theta$ is constructible, and to relate $\cos\theta$ to $\cos n\theta$ by De Moivre's Theorem. Since $\cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n$, we have in particular that $\cos n\theta = \mathrm{Re}((\cos\theta + i\sin\theta)^n)$.

For example, the binomial expansion implies that $\cos 3\theta = \mathrm{Re}((\cos\theta + i\sin\theta)^3) = \cos^3\theta - 3\cos\theta\sin^2\theta = \cos^3\theta - 3\cos\theta(1-\cos^2\theta) = 4\cos^3\theta - 3\cos\theta$. If $\theta = 10°$, then $\cos 3\theta = \cos 30° = \sqrt{3}/2$, so $\cos 10°$ satisfies the polynomial equation $\sqrt{3}/2 = 4x^3 - 3x$. Since $\sqrt{3}/2$ is not a rational number, we do not yet have a candidate for a minimal polynomial for $\cos 10°$ over $\mathbf{Q}$. However, squaring both sides shows that $\cos 10°$ satisfies the polynomial equation $3/4 = 16x^6 - 24x^4 + 9x^2$. (Alternatively, one could directly express $\cos 6\theta$ in terms of $\cos\theta$.) An equivalent equation is $0 = 64x^6 - 96x^4 + 36x^2 - 3$, and since $64x^6 - 96x^4 + 36x^2 - 3$ is irreducible by Eisenstein's criterion, it follows that $\cos 10°$ is not constructible.

Exercise 6.11.

1. Show that the following are equivalent: the length $\cos\theta$ is constructible, the length $\sin\theta$ is constructible, the angle θ is constructible.

2. Show that there is at least one angle that cannot be trisected using straight-edge and compass.

3. Show that a regular pentagon is constructible using straight-edge and compass.

6.4 Problems

In arguing too, the parson own'd his skill,
For e'en though vanquish'd he could argue still;
While words of learned length and thundering sound
Amaz'd the gazing rustics rang'd around;
And still they gaz'd, and still the wonder grew
That one small head could carry all he knew. Oliver Goldsmith
(1728–1774)
The Deserted Village

Problem 6.1. Use the theorems from the handout on factoring to factor the following polynomials over the rationals. Then factor them over the complex numbers.

1. $x^4 - 9x^3 - 8x + 72$
2. $12x^5 + 80x^4 + 79x^3 - 135x^2 - 158x - 40$
3. $x^4 - x^3 - x^2 - 5x - 30$
4. $x^5 + x^4 + x^3 + x^2 + x + 1$
5. $20x^6 + 28x^5 + 23x^4 - 35x^3 - 55x^2 + 7x + 12$

Problem 6.2. Use Eisenstein's Irreducibility Criterion to prove that $2x^{17} - 18x^{12} + 24x^9 + 243x^6 - 30x^3 - 6$ is irreducible over $\mathbf{Q}$.

Problem 6.3. Let $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

1. Show that when p is odd, the polynomial f_p has no linear factors over the rational numbers.
2. Use Eisenstein's Irreducibility Criterion and a change of variables (say $x \to y + 1$) to prove that f_5 is irreducible over the rational numbers.
3. Use Eisenstein's Irreducibility Criterion to prove that for every prime number p, the polynomial f_p is irreducible over the rational numbers. Hint: $x^p - 1 = (x - 1)f_p(x)$.

Problem 6.4. Show that a regular 9-gon is not constructible using straightedge and compass.

Problem 6.5. Show that a regular heptagon (7-gon) is not constructible using straight-edge and compass.

Problem 6.6. Show that a regular 10-gon is constructible using straight-edge and compass.

Problem 6.7. Show that a regular 20-gon is constructible using straight-edge and compass.

Problem 6.8. Show that a regular 30-gon is constructible using straight-edge and compass.

Problem 6.9. Show that an angle of $72°$ is constructible using straight-edge and compass.

Problem 6.10. Show that a regular 15-gon is constructible using straight-edge and compass.

Problem 6.11. Conjecture and prove what you can about the values of n for which a regular n-gon is constructible using straight-edge and compass. (For example, if a regular n-gon is constructible, is a regular $2n$-gon, a regular $n/2$-gon (for n even), a regular $3n$-gon?)

Chapter 7

Game Theory

The game is up. William Shakespeare
Cymbeline, Act iii, scene 2

7.1 Goals

1. Learn the basic principles of the mathematical theory of games.
2. Be able to apply the principles of game theory to analyze both abstract games and real-life situations.
3. Realize that mathematics does not prescribe a best "solution" for all games.

7.2 Reading

1. Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993, Part I, pages 3–61.
2. John G. Kemeny and J. Laurie Snell, "Game-theoretic solution of baccarat," *American Mathematical Monthly* **64** (1957), 465–469.

7.3 Classroom Discussion

A clear fire, a clean hearth, and the rigour of the game.
Charles Lamb

(1775–1834)
Mrs. Battle's Opinions on Whist

7.3.1 Warm up

The reading introduced the following concepts from the mathematical theory of games.

- two-person game
- zero-sum game
- perfect information

Exercise 7.1. List some familiar games. To which of them do the above terms apply?

Exercise 7.2. The minimax theorem of John von Neumann says that every $m \times n$ matrix game has a solution.

1. What does this theorem say about the games you listed in the previous exercise?
2. Does this mean that some of these games are uninteresting to play?

Exercise 7.3. Review the definitions of the following concepts.

- dominance
- saddle point
- mixed strategy
- value of a game

7.3.2 Examples of games

Whose game was empires and whose stakes were thrones,
Whose table earth, whose dice were human bones. Lord Byron
(1788–1824)
Age of Bronze, Stanza 3

Exercise 7.4. Solve the following 4×5 matrix game.[1]

	A	B	C	D	E
A	1	1	1	2	2
B	2	1	1	1	2
C	2	2	1	1	1
D	2	2	2	1	0

Exercise 7.5. In the **Monty Hall game**, the host of a game show offers the contestant the choice of three doors, two of which conceal goats, and one of which conceals a new automobile. After the contestant chooses a door, the host does not open it, but instead opens one of the other doors, displaying a goat. The contestant now is offered the choice either of taking whatever is behind the originally chosen door, or of switching and taking whatever is behind the third door. Should the contestant switch or not, or does it matter?

7.3.3 Generalizations

In a zero-sum game, it suffices to write the payoffs to the row player, since the payoffs to the column player are the negatives of the payoffs to the row player. In a non-zero-sum game, it is necessary to write the payoffs to both players. Here is an example of a 3×3 non-zero-sum two-person game.[2]

	A	B	C
A	$(0, 1)$	$(0, 1)$	$(2, 4)$
B	$(5, 1)$	$(4, 2)$	$(1, 0)$
C	$(4, 3)$	$(1, 4)$	$(1, 0)$

For instance, if both players use pure strategy A, the payoffs are 0 to the row player and 1 to the column player. Since both players want to maximize their payoffs, this strategy would not be optimal for either player.

Exercise 7.6. Find what you think is a reasonable solution to the above game. You may not find the solution satisfactory in all respects, since non-zero-sum games admit puzzling phenomena such as the prisoner's dilemma.

[1] Problem 2, page 11, from Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993.

[2] Problem 4, page 72, from Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993.

As there are three of us come on purpose for the game, you won't be so cantankerous as to spoil the party by sitting out.

Richard Brinsley Sheridan
(1751–1816)
The Rivals, Act v, scene 3

Exercise 7.7. 1. What would be a reasonable strategy for playing the three-person zero-sum game shown in Figure 7.1?[3]

2. If two players could form a coalition to play in concert against the third player, which two players would most likely team up?

7.4 Problems

Our hopes, like towering falcons, aim
At objects in an airy height;
The little pleasure of the game
Is from afar to view the flight.

Matthew Prior
(1664–1721)
To the Hon. Charles Montague

Problem 7.1. Solve the following 4×3 matrix game.[4]

	A	B	C
A	5	2	1
B	4	1	3
C	3	4	3
D	1	6	2

Problem 7.2. Rose holds a double-faced playing card made by gluing the ♠A back-to-back with the ♡8. Colin has a similar card made by gluing the ♢2 back-to-back with the ♣7.

Rose and Colin play a game in which they simultaneously display one side or the other of their cards. Rose wins if the colors match; Colin wins otherwise. In either case, the payoff to the winner is the face value of the winner's card. (Here the value of an ace is 1.)

[3]Example taken from Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993, page 127.

[4]Problem 5b, page 22, from Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993.

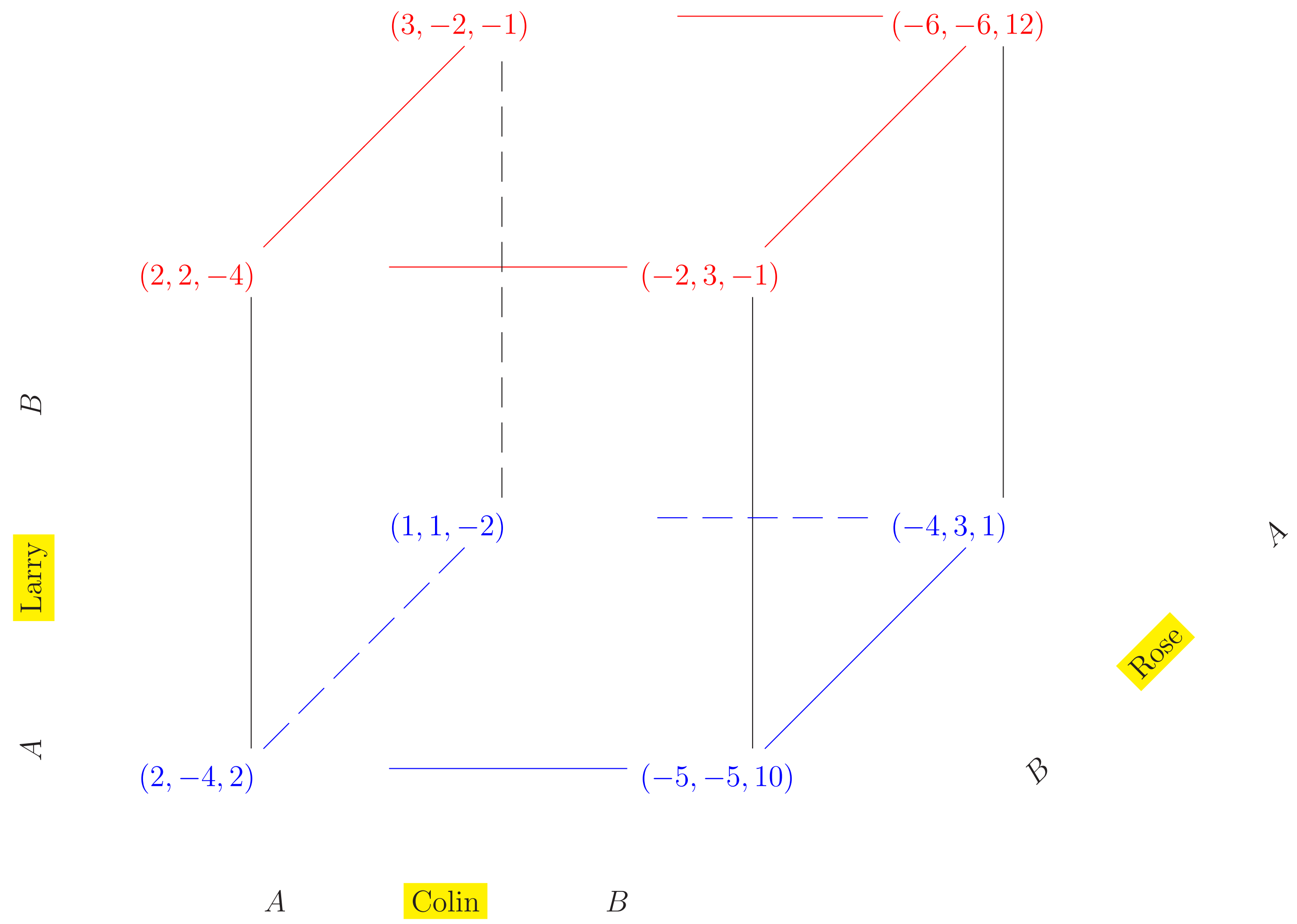


Figure 7.1: A three-person game

1. Does $1 + 8 = 2 + 7$ mean that the game is fair?

2. Solve the game: find optimal strategies for both players and determine the value of the game.

Problem 7.3. Solve the following 4×4 matrix game.[5]

	A	B	C	D
A	1	2	2	2
B	2	1	2	2
C	2	2	1	2
D	2	2	2	0

7.5 Additional Literature

1. Leonard Gillman, The car and the goats, *American Mathematical Monthly* **99** (1992), number 1, 3–7.

2. R. R. Kadesch, *Problem Solving Across the Disciplines*, Prentice-Hall, 1997, chapter IV.

[5]Problem 8, page 22, from Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993.

Chapter 8

Set Theory and Foundations

8.1 Goals

1. Understand the notions of axiomatic systems, consistency, and independence.
2. Be aware that mathematics is open-ended, even at the most basic level.
3. Understand the fundamental theorems of Cantor and Gödel about set theory.

8.2 Reading

1. Stanisław Lem, "The extraordinary hotel, or the thousand and first journey of Ion the quiet", in *Stories about Sets* by N. Ya. Vilenkin, Academic Press, 1968.
2. Robert Gray, Georg Cantor and transcendental numbers, *American Mathematical Monthly* **101** (1994), no. 9, 819–832.

8.3 Classroom Discussion

8.3.1 The axiomatic method

A formal approach to mathematics consists in specifying some undefined terms and some axioms. Theorems in a formal axiomatic system are statements about the undefined terms that can be deduced logically from the axioms.

The axiomatic method is especially associated with the name of David Hilbert, who viewed mathematics as a particularly elaborate game, like chess, with no intrinsic meaning: "Mathematics is a game played according to certain simple rules with meaningless marks on paper." His *Grundlagen der Geometrie* presented an axiomatic development of Euclidean geometry.

A *model* for a formal axiomatic system is a concrete realization of the undefined terms that satisfies all the axioms. An axiomatic system is *consistent* if it admits at least one model. In a consistent system, an axiom is *independent* of the other axioms if it is false in some model that satisfies the remaining axioms.

Exercise 8.1. Consider the following formal axiomatic system.

Undefined terms ag, kow, trad

Axiom 1 Every ag kows at least two trads.

Axiom 2 There is at least one trad that every ag kows.

Axiom 3 For each trad, at least one ag kows it.

Axiom 4 The set of trads is non-empty.

1. Construct a model showing that this axiomatic system is consistent.

2. Is each axiom independent of the other axioms?

Exercise 8.2. Prove that there are at least two trads.

8.3.2 Peano's axioms

Giuseppe Peano formalized arithmetic as an axiomatic system. He showed how the basic principles of arithmetic, such as the commutative, associative, and distributive laws, can be derived as theorems from a small set of fundamental principles. Peano's five axioms for the natural numbers are the following.[1]

[1]Peano's original work is a booklet *Arithmetices principia nova methodo exposita*, Turin, Bocca, 1889. For an English translation, see "The principles of arithmetic, presented by a new method" in *Selected Works of Giuseppe Peano*, translated and edited by Hubert C. Kennedy, University of Toronto Press, 1973, pages 101–134.

Peano 1 There is a natural number denoted by 1.

Peano 2 Every natural number a has a successor, a natural number denoted by a'.

Peano 3 If a and b are natural numbers, then $a = b$ if and only if $a' = b'$.

Peano 4 The natural number 1 is not a successor: for every natural number a, we have $a' \neq 1$.

Peano 5 Axiom of Induction. Let S be a set of natural numbers. If $1 \in S$, and if for every natural number a, the condition $a \in S$ implies that $a' \in S$, then S is the set of all natural numbers.

Exercise 8.3. Using only Peano's axioms, prove that no natural number is its own successor, and every natural number other than 1 is a successor.

Using the induction axiom, Peano defined addition of natural numbers by the following properties.

- $a + 1 = a'$ for every natural number a;
- $a + b' = (a + b)'$ for all natural numbers a and b.

Exercise 8.4. Prove the associative law of addition: $(a + b) + c = a + (b + c)$ for all natural numbers a, b, and c.

8.3.3 Cantor's theorems

Georg Cantor was the first one to understand the notion of *cardinality* of infinite sets. Two sets have the same cardinality if they can be put into one-to-one-correspondence with each other. (According to the Schroeder-Bernstein theorem, two sets have the same cardinality if each can be put into one-to-one correspondence with a subset of the other.)

Cantor showed in particular that there is no one-to-one correspondence between the rational numbers and the real numbers.

Theorem (Cantor)**.** *No sequence of real numbers exhausts an interval.*

Cantor's first proof is based on the proposition that a sequence of nested closed intervals has a nonvoid intersection. Then, Cantor says, the first two elements of the sequence determine an interval. The next two elements of the sequence that are in the first interval determine a second interval, and so on. The intersection of the nested intervals contains a number that is not in the sequence.

Cantor's second proof is his famous diagonal argument. Write the numbers of the sequence as a list of decimals. Read down the diagonal, changing each digit to a different one. If done with a little care, this procedure creates a number that is not in the list.

Exercise 8.5. Enumerate the rational numbers in the interval $(0, 1)$ as $1/2$, $1/3$, $2/3$, $1/4$, $3/4$, $1/5$, $2/5$, $3/5$, $4/5$, $\dots$. Construct the first few digits of an irrational number:

1. by Cantor's nested set procedure;
2. by Cantor's diagonal procedure.

Cantor's power set theorem says that the power set $P(S)$ (the set of all subsets of S) has larger cardinality than the set S itself. That is, $P(S)$ cannot be put into one-to-one correspondence with S, but S can be put into one-to-one correspondence with a subset of $P(S)$.

Exercise 8.6. Show that the power set of the positive integers has the same cardinality as the set of real numbers.

8.3.4 The continuum hypothesis

Cantor's continuum hypothesis is the statement that every infinite set of real numbers can be put into one-to-one correspondence with either the integers or the whole set of real numbers. In other words, there is no set of cardinality strictly between the cardinality of the integers and the cardinality of the real numbers. Cantor was able to prove neither the continuum hypothesis nor the *generalized continuum hypothesis*: For every set S, there is no set of cardinality between the cardinality of S and the cardinality of the power set of S.

It turns out that there is a good reason for Cantor's failure.

Theorem (Kurt Gödel (1940))**.** *Both the continuum hypothesis and the generalized continuum hypothesis are* consistent *with the usual axioms of set theory.*

Theorem (Paul Cohen (1963))**.** *Both the continuum hypothesis and the generalized continuum hypothesis are* independent *of the usual axioms of set theory.*

Exercise 8.7. What do the preceding two theorems say about the existence of certain models for set theory?

8.3.5 Gödel's incompleteness theorems

Hilbert's program of axiomatizing all of mathematics failed, and for a good reason. In 1931, Kurt Gödel showed that any interesting formal axiomatic system must contain undecidable propositions: statements that cannot be either proved or disproved within the system.

Theorem (Gödel's first incompleteness theorem)**.** *Any axiomatic system that is consistent and that contains elementary logic and arithmetic must contain undecidable propositions.*

Exercise 8.8. Does Gödel's theorem mean that it is pointless to study mathematics?

Gödel's proof is based on formalizing the liar paradox. ("This sentence is false.") Namely, Gödel assigns to each symbol an integer. A statement or formula is a string of symbols, so each statement within a formal system gets a number assigned to it; similarly, each proof within the system has an assigned *Gödel number.* Essentially, Gödel uses a diagonal argument to show the existence of a number n that is assigned to the statement: "Sentence number n is not provable in the system." This statement is *true*, but neither it nor its negative can be proved within the formal axiomatic system.

Exercise 8.9. Why?

Theorem (Gödel's second incompleteness theorem)**.** *A consistent axiomatic system that contains elementary logic and arithmetic cannot prove its own consistency.*

Indeed, if the system is consistent, then *we* know that it cannot prove the above undecidable proposition n (which asserts its own unprovability). If the system can prove its own consistency, then *it* can prove that it cannot prove proposition n. But this is just what proposition n states, that it is unprovable; so the system has proved proposition n after all. Contradiction.

For nothing worthy proving can be proven,
Nor yet disproven: wherefore thou be wise,
Cleave ever to the sunnier side of doubt. Alfred, Lord Tennyson
(1809–1892)
The Ancient Sage

8.4 Problems

Problem 8.1. Formulate a proposition that is undecidable in the axiomatic system of Exercise 8.1. How do you know that the proposition cannot be proved and cannot be disproved?

Problem 8.2. Use Peano's axioms to prove the validity of the commutative law $a + b = b + a$ for all natural numbers a and b.

Problem 8.3. Formulate a definition of multiplication of natural numbers based on Peano's axioms and use it to prove the distributive law $(a + b) \times c = (a \times c) + (b \times c)$.

8.5 Additional Literature

1. Donald M. Davis, *The Nature and Power of Mathematics*, Princeton University Press, 1993, section 2.1.

2. William Dunham, *Journey Through Genius*, Wiley, 1990, Chapters 11–12.

3. Howard Eves, *Great Moments in Mathematics (After 1650)*, Mathematical Association of America, 1981, sections 37–41.

4. Edmund Landau, *Foundations of Analysis: The Arithmetic of Whole, Rational, Irrational and Complex Numbers*, translated from the German by F. Steinhardt, third edition, Chelsea, New York, 1966.

5. Rudy Rucker, *Infinity and the Mind*, Birkhäuser, 1982.

Chapter 9

Limits

9.1 Goals

1. Renew your acquaintance with the notion of a limit.
2. Be able to apply your knowledge to new situations.

9.2 Reading

1. Edward B. Burger and Thomas Struppeck, Does $\sum_{n=0}^{\infty} \frac{1}{n!}$ really converge? Infinite series and p-adic analysis, *American Mathematical Monthly* **103** (1996), number 7, 565–577.

9.3 Classroom Discussion

> Human life was once like a zero-sum game. Humankind lived near its ecological limit and tribe fought tribe for living space. Where pastures, farmland, and hunting grounds were concerned, more for one group meant less for another. Because one's gain roughly equaled the other's loss, net benefits summed to zero. Still, people who cooperated on other matters prospered, and so our ancestors learned not just to grab, but to cooperate and build.
>
> K. Eric Drexler, *Engines of Creation*

The notion of a *limit* is a fundamental concept in the realm of continuous mathematics (calculus and analysis). According to the Humpty Dumpty principle,[1] the correspondence between concepts and words is not a one-to-one correspondence; the word "limit" has more than one mathematical meaning. For example, the expression $\lim_{a\to 0}\int_a^1 x^{-1/2}\,dx$ might be expressed in words as "the *limit* of the integral as the lower *limit* tends to zero."

In ordinary discourse, the word "limit" most often conveys the idea of a boundary or a restriction. Here are some examples of this usage.

- A pun is not bound by the laws which limit nicer wit. Charles Lamb
  Last Essays of Elia
- There is a limit to a mother's patience. Sir Arthur Conan Doyle
  Sussex Vampire
- Human thought has no limit. Victor Hugo
  Les Misérables
- For stony limits cannot hold love out. William Shakespeare
  Romeo and Juliet, II. ii. 67

This is the sense in which mathematicians use the word "limit" in the phrase "limit of integration."

However, we shall be dealing with the notion of "limit" as a value to which one approaches arbitrarily closely. This second notion is not disjoint from the first one: it may happen that a limiting value is also an extreme point.

> Here at the quiet limit of the world. Alfred, Lord Tennyson
> *Tithonus*, l. 7

9.3.1 Intuitive limits

> To define is to limit. Oscar Wilde
> *Picture of Dorian Gray*

The sequence of rational numbers 1/2, 2/3, 3/4, 4/5, ... evidently approaches the limit 1. Indeed, the nth term of the sequence equals $n/(n+1)$, or equivalently $1-(n+1)^{-1}$, so we can be sure that the terms are within, say, 10^{-k} of 1 when $n > 10^k$.

[1] "When I use a word," Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean—neither more nor less." *Through the Looking-Glass*

It is often said that the sequence $\{n/(n+1)\}_{n=1}^{\infty}$ has limit 1 because the terms get "closer and closer" to 1. This is good intuition, but suspiciously imprecise.

Exercise 9.1. Aren't the terms of the sequence $\{n/(n+1)\}_{n=1}^{\infty}$ also getting "closer and closer" to π?

> "Oh, don't you see, Marilla? There must be a limit to the mistakes one person can make, and when I get to the end of them, then I'll be through with them. That's a very comforting thought."
>
> L. M. Montgomery
> *Anne of Green Gables*

Exercise 9.2. In what sense do the numbers $n^{-1}\cos(\pi n/2)$ get "closer and closer" to 0 as the integer n increases?

The repeating decimal 0.171717... implicitly defines a limit: namely, the sum of the infinite series

$$\frac{1}{10} + \frac{7}{100} + \frac{1}{1000} + \frac{7}{10000} + \cdots .$$

It is evident, even without computation, that the limit exists. Indeed, each partial sum is certainly less than 1, and the sequence of partial sums is monotonically increasing, so we can invoke the fundamental property of the real numbers that a bounded increasing sequence converges (in fact, converges to its least upper bound). We say that this repeating decimal equals 17/99 because the value of the limit is 17/99.

Exercise 9.3. 1. Verify the value of the repeating decimal 0.171717....

2. Suppose that 0.171717... is reinterpreted as an expansion in base 8. What would its value be, expressed as an ordinary rational number?

3. How would you answer the question: "Does it ever get there?"

Understanding the definition of the limit concept does not necessarily mean being able to compute numerical values of limits. For example, the verification that

$$\lim_{n\to\infty} \frac{n^n e^{-n}\sqrt{2\pi n}}{n!} = 1$$

is sufficiently subtle that the equality bears the name *Stirling's formula.* The formula is indeed a beautiful one, as it ties together properties of the natural numbers (represented by the factorial function) with the special numbers e and π.

Exercise 9.4. Show that $\displaystyle\lim_{n\to\infty}\sum_{k=1}^{n}\frac{n}{n^2+k^2}=\frac{\pi}{4}$.

The von Koch fractal snowflake curve is defined by an iterative process, starting from an equilateral triangle with sides of length 1. At each stage of the construction, every straight line segment is subdivided into three equal parts, an outward-pointing equilateral triangle is erected on the middle piece, and that middle segment is deleted. The first four stages of the construction are shown in Figure 9.1.

Exercise 9.5.

1. In what sense does the snowflake construction converge to a limiting curve?
2. What is the area enclosed by the limiting curve?
3. What is the perimeter of the limiting curve?

> It is therefore evident that, ascend as high as we may, we cannot, literally speaking, arrive at a limit beyond which no atmosphere is to be found. It must exist, I argued; although it may exist in a state of infinite rarefaction. Edgar Allan Poe
> *Hans Phaall*

9.3.2 Continued fractions

> I will then limit my assertion to pure mathematics, the very conception of which implies that it consists of knowledge altogether non-empirical and a priori. Immanuel Kant
> *Critique of Pure Reason*

The most familiar way to represent real numbers is via decimal expansions, which (as observed above) are limits of sums. For many purposes, it is advantageous instead to represent real numbers as limits of quotients.

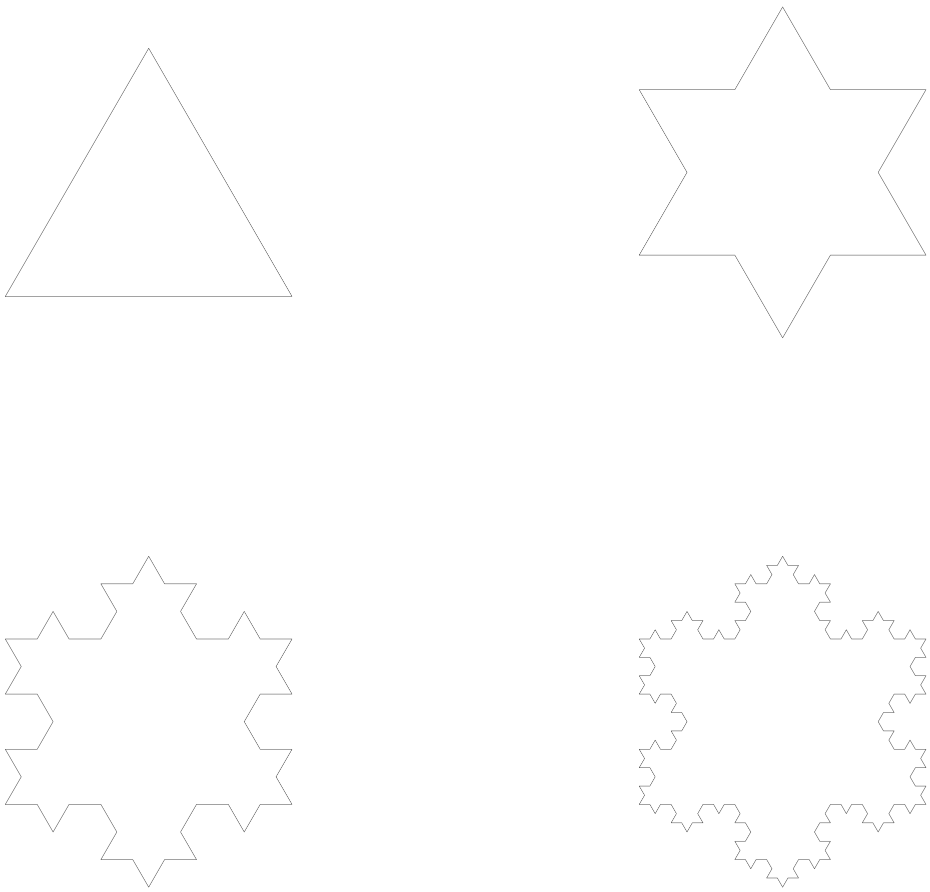


Figure 9.1: Four stages in the construction of the von Koch snowflake

For example, consider the rational number 17/99, which we saw above has the repeating decimal expansion 0.171717... (implicitly involving a limiting operation). We could alternatively express the same rational number as follows:

$$\frac{17}{99} = \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2}}}}}.$$

Exercise 9.6. Verify the preceding equality.

For typographical simplicity, it will be convenient to abbreviate the above *continued fraction* as $[0, 5, 1, 4, 1, 2]$, the initial 0 indicating that there is no integer part. The numbers appearing in the denominators are closely related to the Euclidean algorithm. Recall that to find the greatest common divisor of 99 and 17, you would iteratively apply the division algorithm as follows.

$$\begin{aligned} 99 &= 5 \cdot 17 + 14 \\ 17 &= 1 \cdot 14 + 3 \\ 14 &= 4 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

The penultimate line shows that $\gcd(99, 17) = 1$. Now the first line shows that

$$\frac{99}{17} = 5 + \frac{14}{17}, \text{ so } \frac{17}{99} = \cfrac{1}{5 + \cfrac{14}{17}}.$$

The second line in the Euclidean algorithm shows that

$$\frac{17}{14} = 1 + \frac{3}{14}, \text{ so } \frac{17}{99} = \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{3}{14}}}.$$

The third line in the Euclidean algorithm shows that

$$\frac{14}{3} = 4 + \frac{2}{3}, \text{ so } \frac{17}{99} = \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{2}{3}}}}.$$

The fourth line in the Euclidean algorithm shows that

$$\frac{3}{2} = 1 + \frac{1}{2}, \text{ so } \frac{17}{99} = \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2}}}}}.$$

Thus the numbers in the continued fraction expansion $[0, 5, 1, 4, 1, 2]$ of $17/99$ are just the quotients obtained by applying the Euclidean algorithm to the numbers 99 and 17.

Exercise 9.7. Show that $99/17 = [5, 1, 4, 1, 2]$.

Exercise 9.8. Find a continued fraction expansion for the negative number $-17/99 = -1 + 82/99$.

Exercise 9.9. Evidently, the above procedure makes it possible to represent every rational number as a continued fraction $[a_1, a_2, \ldots, a_n]$, where the a_j are integers, all positive except perhaps the first one. Is the representation unique?

What are we to make of an unending continued fraction? Consider, for example

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}.$$

Some truncated versions of this fraction are

$$1+\frac{1}{2}=1.5,$$

$$1+\cfrac{1}{2+\cfrac{1}{2}}=1.4,$$

$$1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}=1.416\bar{6}.$$

It would be reasonable to assign to the unending continued fraction the value of the limit of the truncated fractions, if the limit exists.

Exercise 9.10. Show that the limit exists in the above example, and find its value, as follows.

1. Assuming that the limit exists, determine what its value must be.
2. More generally, assuming that the even-order truncations have a limit, determine what its value must be; similarly for the odd-order truncations.
3. Show that the even-order truncations form a monotonic sequence; similarly for the odd-order truncations.
4. Use the fundamental property of the real numbers that a bounded monotonic sequence converges.

Continued fractions play a minor role in one of the most romantic stories in the history of mathematics. In 1913, Srinivasa Ramanujan, a poor Indian clerk who had flunked out of college, wrote down some mathematical formulas that he had discovered and sent them to the famous G. H. Hardy in England. One of these formulas was a closed-form expression for a certain continued fraction:

$$\cfrac{1}{1+\cfrac{e^{-2\pi}}{1+\cfrac{e^{-4\pi}}{1+\cfrac{e^{-6\pi}}{1+\cdots}}}}=\left(\sqrt{\frac{5+\sqrt{5}}{2}}-\frac{\sqrt{5}+1}{2}\right)e^{2\pi/5}.$$

Hardy, wondering what to make of this communication from an unknown Indian, tried to prove Ramanujan's formulas, with mixed success. Of this continued fraction and two related ones, Hardy later said[2] that they

> 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 brought Ramanujan to England to work with him. Tragically, Ramanujan's health failed in 1917, and he died three years later.

Exercise 9.11. If x has the continued fraction expansion $[a_1, a_2, \ldots]$, let $s_n(x)$ and $t_n(x)$ denote the numerator and denominator of the nth approximant $[a_1, \ldots, a_n]$ (written as a fraction in lowest terms with positive denominator). Guess recursive formulas for $s_n(x)$ and $t_n(x)$, and prove your formulas by induction.

9.3.3 The p-adic numbers

> 'Yes, I have a pair of eyes,' replied Sam, 'and that's just it. If they wos a pair o' patent double million magnifyin' gas microscopes of hextra power, p'raps I might be able to see through a flight o' stairs and a deal door; but bein' only eyes, you see my wision's limited.'
>
> Charles Dickens
>
> *Pickwick Papers*, ch. 34

In order to talk about limits, we need to be able to say when two quantities are close to each other. Formally, we need a distance function or *metric*. Recall the following defining properties of a metric d.

1. $d(x, y) \geq 0$ for all x and y (with equality if and only if $x = y$).

2. Symmetry: $d(x, y) = d(y, x)$ for all x and y.

[2]Lecture delivered at the Harvard Tercentenary Conference of Arts and Sciences on August 31, 1936, published as The Indian mathematician Ramanujan, *American Mathematical Monthly* **44** (1937), 137–155, and reprinted in Hardy's book *Ramanujan*, Cambridge University Press, 1940.

3. Triangle inequality: $d(x, y) \leq d(x, z) + d(z, y)$ for all x, y, and z.

So far we have been dealing only with the usual metric on the real numbers: $d(x, y) = |x - y|$. It is useful to isolate the properties of the absolute value function that enable us to define a metric in this way. These properties are the following.

1. $|x| \geq 0$ (with equality if and only if $x = 0$).

2. $|x \cdot y| = |x| \cdot |y|$ for all x and y.

3. Triangle inequality: $|x + y| \leq |x| + |y|$ for all x and y.

A function with these properties is often called a *norm* in the context of vector spaces and a *valuation* in the context of fields.

Exercise 9.12. Show that the three properties of a metric d given by $d(x, y) = |x - y|$ are consequences of the three properties of an absolute value.

A standard example of a nonstandard metric is the *discrete metric* defined by $d(x, y) = 1$ if $x \neq y$.

Exercise 9.13. 1. Verify that the discrete metric on the real numbers does satisfy the three properties of a metric.

2. What valuation on the real numbers induces the discrete metric?

3. What are the convergent sequences of real numbers in the discrete metric?

It is worthwhile to keep in mind that the familiar real numbers are actually a quite abstract notion. On a calculator or a computer, you will see only rational numbers. There is no explicit way to display a non-terminating, non-repeating decimal in numerical form without resorting to a limiting operation.[3] We normally exhibit irrational real numbers as limits of convergent sequences of rational numbers.

If we change the metric on the rational numbers, then we may have a different set of convergent sequences, and their limits will define a new number system. This process of generating new numbers by taking limits of convergent sequences is known as *completion*.[4]

---

[3]You might be able to display an irrational number *geometrically*: $\sqrt{2}$ is the length of the diagonal of a unit square.

[4]More precisely, the elements of the completion are equivalence classes of convergent sequences, two sequences being equivalent if their difference tends to zero.

Exercise 9.14. Completing the rational numbers when they are equipped with the discrete metric is uninteresting. Why?

We can create an interesting new number system by using a non-trivial, non-standard valuation on the rational numbers. For example, we can define a valuation $|\cdot|_2$ (which we might call the dyadic valuation) on the rational numbers in the following way. A non-zero rational number r can be factored as a product of primes (some powers being negative). Extract from the product the power of 2, say 2^k, and define $|r|_2$ to be the *reciprocal* $1/2^k$. For example, $|4|_2 = 1/4$, $|5|_2 = 1$, $|6|_2 = 1/2$, $|25/96|_2 = 32$.

Exercise 9.15. Verify that $|\cdot|_2$ is a valuation on the rational numbers. Moreover, $|\cdot|_2$ satisfies the *strong triangle inequality*: $|x+y|_2 \leq \max(|x|_2, |y|_2)$.

Exercise 9.16. When does equality hold in the strong triangle inequality? That is, for which rational numbers x and y is $|x+y|_2 = \max(|x|_2, |y|_2)$?

The rational numbers with the dyadic valuation appear strange at first sight. For example, they fail the axiom of Archimedes[5] that if a positive quantity is added to itself a sufficient number of times, its value becomes bigger than any specified value.

Exercise 9.17. If n is an integer, then $|n|_2 \leq 1$.

Convergence with respect to the dyadic valuation $|\cdot|_2$ is dramatically different from convergence with respect to the ordinary absolute value. For example, consider the infinite series

$$1 + 2 + 4 + 8 + 16 + \cdots + 2^n + \cdots .$$

This series converges dyadically! Indeed, the difference between the nth partial sum and the $(n+k)$th partial sum has dyadic absolute value no more than $1/2^n$, which tends to zero as n increases without bound.

Exercise 9.18. The series $1 + 2 + 4 + 8 + \cdots + 2^n + \cdots$ converges dyadically to an integer: which integer?

---

[5] This is the Greek philosopher of "Eureka" fame. As related by Plutarch in his biography of Marcellus, Archimedes was killed by a Roman soldier during the sack of Syracuse in 212 B.C. For a modern retelling of this legend by Karel Čapek (inventor of the word "robot"), see "The Death of Archimedes" in his *Apocryphal Stories*, Penguin Books, 1975, pages 38–41.

On the other hand, the series

$$1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}+\cdots$$

diverges dyadically since $|1/2^n|_2 = 2^n$. Indeed, a series of the form $\sum_{j=-\infty}^{\infty} a_j 2^j$, where each a_j is either 0 or 1, converges dyadically if and only if there are only a finite number of non-zero coefficients a_j with negative indices. Such series may converge to rational numbers, but in general they converge to elements of the dyadic completion of the rational numbers.

Exercise 9.19. 1. Find the dyadic expansion of the current year.

2. Find the dyadic expansion of 2/3.

A non-Archimedean valuation $|\cdot|_p$ can be defined similarly for every prime number p. For example, $|17/99|_3 = 9$ and $|100/33|_5 = 1/25$. The *p-adic numbers* are the completion of the rational numbers with respect to $|\cdot|_p$. Thus a p-adic number can be represented as a series

$$\frac{a_{-k}}{p^k}+\cdots+\frac{a_{-1}}{p}+a_0+a_1p+a_2p^2+\cdots$$

where each coefficient a_j is an integer between 0 and $(p-1)$ inclusive.

Exercise 9.20. The quotient

$$\frac{1\cdot 3^0+1\cdot 3^1+1\cdot 3^2+1\cdot 3^3+1\cdot 3^4+1\cdot 3^5+\cdots}{1\cdot 3^0+2\cdot 3^1+1\cdot 3^2+2\cdot 3^3+1\cdot 3^4+2\cdot 3^5+\cdots}$$

of 3-adic expansions can itself be expressed as a 3-adic expansion. Use long division to find this expansion.

> Evidently, therefore, 'limit' has as many senses as 'beginning', and yet more; for the beginning is a limit, but not every limit is a beginning.
>
> Aristotle
> *Metaphysics*

9.4 Problems

> For the rest of it, the last and greatest art is to limit and isolate oneself.[6]
>
> Goethe
>
> *Conversations with Eckermann*

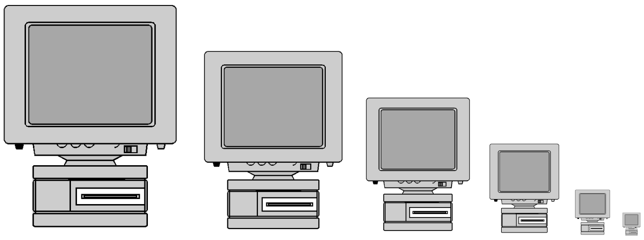
Problem 9.1. What can you say about the limiting behavior of the sequence of numbers $\sin n$ as n runs through the natural numbers? Does it matter if the argument is measured in degrees or in radians?

Problem 9.2. For which values of x larger than 1 does the sequence x^x, x^{x^x}, $x^{x^{x^x}}$, ... converge to a (finite) limit?

Problem 9.3. Consider the iterative construction shown in Figure 9.2. The first stage shows an isosceles right triangle whose hypotenuse is a horizontal line segment of length 1. (The other two sides each have length $1/\sqrt{2}$, so the two slanted sides together have length $\sqrt{2}$.) At each subsequent stage, every isosceles right triangle is replaced by two isosceles right triangles whose sides have half the length. Consequently, the total length of the slanted sides at each stage is always $\sqrt{2}$. Since the seesaw curves approach the horizontal line of length 1 as their limit, we deduce that $\sqrt{2} = 1$. What went wrong?

Figure 9.2: $\sqrt{2} = 1$

Problem 9.4 (The limits of computers[7])**.**



[6] Im übrigen ist es zuletzt die größte Kunst, sich zu beschränken und zu isolieren.

[7] This problem was suggested by a note of Allen J. Schwenk: "Introduction to limits, or why can't we just trust the table?", *College Mathematics Journal* **28** (1997), number 1, 51.

Beginning calculus students often think that their instructors' discussions of limits are pedantic, for it seems perfectly obvious from numerical evidence what the value of a limit like $\lim_{x\to 0}(\sin x^{2/5})/x^{2/5}$ must be (see Table 9.1).

x	± 0.1	± 0.01	± 0.001	± 0.0001	± 0.00001
$(\sin x^{2/5})/x^{2/5}$	0.97379	0.99584	0.99934	0.99989	0.99998

Table 9.1: A table of values for $(\sin x^{2/5})/x^{2/5}$

1. Using a calculator or computer, make a similar table of values for the function f defined for $x \neq 0$ by
$$f(x) = \cos\left(\frac{1}{x} \cdot \tan^{-1}\left(\frac{1}{x}\right)\right).$$
What does this table suggest for the value of $\lim_{x\to 0} f(x)$?

2. Make analogous tables of values of $f(x)$ when $x = 0.3, 0.03, 0.003, \ldots$; when $x = 0.6, 0.06, 0.006, \ldots$; and when $x = 0.9, 0.09, 0.009, \ldots$. What do these tables suggest for the value of $\lim_{x\to 0} f(x)$?

3. Make sense out of the numbers that the computer generated.

4. What is the true value of $\lim_{x\to 0} f(x)$?

Problem 9.5. In the reading handouts is "Chapter 47, Bentley's theorems," a "proof" done by a group of entering freshman in a special enrichment program the summer before they started. They purportedly prove that $\pi = 47$. Did they? If not, where did their argument go wrong? (Find ALL errors.)

Problem 9.6. Circumscribe an equilateral triangle around a unit circle; then circumscribe a circle around the triangle and a square around the new circle; then circumscribe a circle around the square and a regular pentagon around the new circle; and so on. See Figure 9.3. Edward Kasner and James Newman state[8] that the construction converges to a limit circle whose radius is about 12. They are wrong. What really happens in the limit?

[8] *Mathematics and the Imagination*, Simon and Schuster, 1940, page 312.

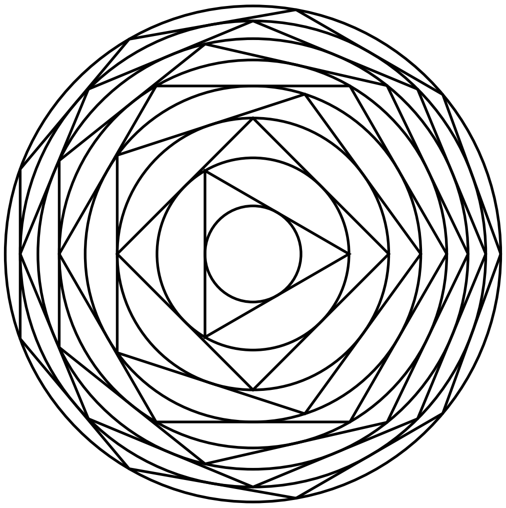


Figure 9.3: What happens in the limit?

Problem 9.7. 1. By considering Riemann sums, show that the limit

$$\lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\int_{1}^{n}\frac{1}{t}\,dt\right)$$

exists. This limit, usually denoted by the Greek letter γ, is known as Euler's constant. The numerical value of γ is about 0.577, but nobody knows if γ is a rational number or an irrational number.

2. By using the preceding part twice, show that

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\frac{1}{7}-\frac{1}{8}+\dots=\log 2.$$

This series is often called the alternating harmonic series.

3. Rearrange the preceding conditionally convergent series so that each positive term is followed by the next four negative terms. Show that the rearranged series converges to zero:

$$1-\frac{1}{2}-\frac{1}{4}-\frac{1}{6}-\frac{1}{8}+\frac{1}{3}-\frac{1}{10}-\frac{1}{12}-\frac{1}{14}-\frac{1}{16}+\frac{1}{5}-\dots=0.$$

Problem 9.8. Find the continued fraction expansion of $\sqrt{3}$.

Problem 9.9. Prove that *every* unending continued fraction $[a_1, a_2, \dots]$ converges, whatever the values of the positive integers a_j. (This amounts to showing that the limit of the even-order truncations equals the limit of the odd-order truncations.)

Problem 9.10. Show that if x is an eventually periodic continued fraction (that is, $x = [a_1, a_2, \dots, a_n, \overline{b_1, \dots, b_k}\,]$, where the bar denotes a repeating block), then x is a quadratic surd: an irrational number that is the root of a quadratic equation with integral coefficients. (The converse is also true, but harder to prove.)

Problem 9.11. Show that if $|\cdot|$ is a valuation that satisfies the strong triangle inequality, then every triangle is isosceles with respect to $|\cdot|$. In other words, for all x and y, at least two of the numbers $|x|$, $|y|$, and $|x - y|$ are equal.

Consequently, the strong triangle inequality might equally well be called the *isosceles triangle inequality*.

Problem 9.12. Show that -1 is not a 3-adic square, but -1 is a 5-adic square.

Problem 9.13. Does every rational number have a p-adic expansion whose coefficients are eventually periodic?

9.5 Additional Literature

1. Claude Brezinski, *History of Continued Fractions and Padé Approximants*, Springer, 1991.

2. A. Ya. Khinchin, *Continued Fractions*, University of Chicago Press, 1964.

3. Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, second edition, Springer, 1984.

4. Kurt Mahler, *Introduction to p-adic Numbers and Their Functions*, Cambridge University Press, 1973.

5. C. D. Olds, *Continued Fractions*, Random House, 1963.

6. W. H. Schikhof, *Ultrametric Calculus*, Cambridge University Press, 1984.

Chapter 10

Functions

10.1 Goals

1. Solidify your understanding of functions, especially transcendental functions: the different ways in which they arose and their various definitions.

2. Learn some of the history and applications of special functions.

10.2 Reading

1. Zeev Barel, "A mnemonic for e," *Mathematics Magazine* **68** (1995), number 4, 253.

2. Wayne Barrett, "It had to be e", *Mathematics Magazine* **68** (1995), number 1, 15.

3. Chapter 47, "bentley's theorems", Pomona group (provided by one of the original members of the group).

4. B. C. Carlson, *Special Functions of Applied Mathematics*, Academic Press, 1977, pages 1–6.

5. John Fauvel, "Revisiting the history of logarithms," *Learn from the Masters*, Frank Swetz et al., eds., Mathematical Association of America, 1995, pages 39–48.

6. Victor J. Katz, "Napier's logarithms adapted for today's classroom," *Learn from the Masters*, Frank Swetz et al., eds., Mathematical Association of America, 1995, pages 49–55.

7. David Shelupsky, "Limitless integrals and a new definition of the logarithm," *Mathematics Magazine*, **68** (1995), number 4, 294–295.

8. Victor J. Katz, "Ideas of calculus in Islam and India," *Mathematics Magazine* **68** (1995), number 3, 163–174.

9. Jacques Redway Hammond, *Concise Spherical Trigonometry*, Houghton Mifflin Co., (1943), pages 29–37 and 98–101.

10.3 Classroom Discussion

10.3.1 The function concept

Still glides the Stream, and shall for ever glide;
The Form remains, the Function never dies.

William Wordsworth
The River Duddon, xxxiv

Gottfried Wilhelm Leibniz[1] introduced the term "function," but historically, there was considerable uncertainty about its meaning. The uncertainty persists today among undergraduate students who wonder if a piecewise-defined function is really one function or two.

Exercise 10.1. What is a function? Is it a formula? a rule? a set? all of the above? none of the above? Formulate a definition of "function" that satisfies you.

Exercise 10.2. Make up a strange function that illustrates a subtlety of your definition.

> Our federal income tax law defines the tax y to be paid in terms of the income x; it does so in a clumsy enough way by pasting several linear functions together, each valid in another interval or bracket of income. An archeologist who, five thousand years from

[1] Co-inventor with Newton of the calculus, Leibniz lived 1646–1716.

now, shall unearth some of our income tax returns together with relics of engineering works and mathematical books, will probably date them a couple of centuries earlier, certainly before Galileo and Vieta. Hermann Weyl, 1940

10.3.2 Transcendental functions

In their nomination to office, they will not appoint to the exercise of authority as to a pitiful job, but as to a holy function.
Edmund Burke
Reflections on the Revolution in France, Vol. III

The simplest functions that come to mind are polynomials. Just as the rational numbers are defined to be ratios of integers, the rational functions are defined to be ratios of polynomials. For example, the function f defined by $f(x) = (x^2 - 1)/(x^2 + 1)$ is a rational function.

The algebraic numbers are the numbers that satisfy polynomial equations with integral coefficients. Similarly, the algebraic functions are the functions that satisfy polynomial equations with polynomial coefficients. That is, a function f is algebraic if there are polynomials $p_0, p_1, \ldots, p_n$ such that the function

$$p_n(x)f(x)^n + p_{n-1}(x)f(x)^{n-1} + \cdots + p_1(x)f(x) + p_0(x)$$

is identically zero.

Exercise 10.3. The function $\sqrt{\dfrac{x^2-1}{x^2+1}}$ is algebraic. What polynomial equation does it satisfy?

Functions that are not algebraic are called *transcendental.* Some examples of transcendental functions are the trigonometric functions, the logarithm function, and the exponential function.

Exercise 10.4. By considering growth rates as $x \to \infty$, show that the exponential function e^x is transcendental.

How can one define a transcendental function, given that it does not satisfy any algebraic equation? There are several common ways to define such functions:

- geometrically;
- via power series;
- as solutions of differential equations;
- as solutions of functional equations.

For example, the trigonometric functions may be defined as lengths (see Figure 10.1). The exponential function 2^x may be defined as the unique continuous

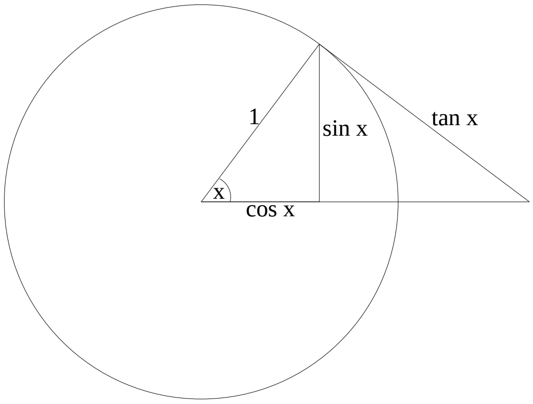


Figure 10.1: Geometric definition of the trigonometric functions

solution of the functional equation $f(x+y) = f(x)f(y)$ satisfying $f(1) = 2$.

Exercise 10.5 (Trigonometric functions)**.**

1. Of the six trigonometric functions, how many need to be defined before all six are determined through functional relationships?
2. What power series expansions are there for trigonometric functions?
3. What differential equations do the trigonometric functions satisfy?
4. In calculus class, you viewed the sine and cosine functions as the "basic" trigonometric functions. Was there a good reason for this, or could you just as well have viewed the tangent and cosecant (for example) as the "basic" functions?

5. Show that the geometric definition of the trigonometric functions agrees with the power series and differential equation definitions.

Exercise 10.6 (e^x and $\log x$)**.** 1. What power series expansions are there for the exponential and logarithm functions?

2. What differential equations do the exponential and logarithm functions satisfy?

3. What functional equations characterize the exponential and logarithm functions?

4. What geometric characterizations are there for these functions?

But love, first learned in a lady's eyes,
Lives not alone immured in the brain;
But, with the motion of all elements,
Courses as swift as thought in every power,
And gives to every power a double power,
Above their functions and their offices. William Shakespeare
Love's Labour's Lost, IV. iii. 327–332

The identity $\cos^2 t + \sin^2 t = 1$ shows that the trigonometric functions are connected with the unit circle $x^2 + y^2 = 1$. The hyperbola $x^2 - y^2 = 1$ is connected with the hyperbolic functions $\cosh t = \frac{1}{2}(e^t + e^{-t})$ and $\sinh t = \frac{1}{2}(e^t - e^{-t})$. Vincenzo Riccati studied the hyperbolic functions in the middle of the eighteenth century. Subsequently, these functions were popularized and given their modern names by Johann Heinrich Lambert (a modest man who is supposed to have replied "All" to Frederick the Great's inquiry of which science he knew best[2]).

Exercise 10.7 (Hyperbolic functions)**.** 1. Draw a diagram analogous to Figure 10.1, and identify $\cosh t$, $\sinh t$, and $\tanh t$ as lengths of certain line segments related to the graph of the hyperbola $x^2 - y^2 = 1$.

2. Find the area bounded by the hyperbola, the x-axis, and the line joining the origin to the point $(\cosh t, \sinh t)$. Compare with the area of a sector of a unit circle with central angle t.

[2]Carl B. Boyer, *A History of Mathematics*, Princeton University Press, 1985, page 504.

10.3.3 Mercator's map and rhumb lines

> The one function TV news performs very well is that when there is no news we give it to you with the same emphasis as if there were.
> attributed to David Brinkley

Since antiquity, it has been important to know where on Earth you are, how to get somewhere else, and how to draw illustrative maps of regions of the Earth's surface. To a first approximation, the surface of the Earth is a sphere, and a location on this two-dimensional surface can be specified by two coordinates, most commonly by two angles.

In geography, the two coordinates are *latitude*, which is the angle of elevation above the plane of the equator, and *longitude*, which is the *azimuthal* angle, that is, the polar angle measured in the plane of the equator. Circles where the latitude is constant are *parallels* of latitude, and circles where the longitude is constant are *meridians*. Normally latitude ranges from $0°$ to $90°$, with an additional designation of North (for angles of elevation above the equator) and South (for angles below the equator). Longitude ranges from $0°$ to $180°$, either East or West of the zero meridian or *prime meridian* that passes through Greenwich, England.

Mathematicians ordinarily use the angle complementary to the latitude, the *co-latitude*, which is measured down from the North Pole instead of up from the equator. Unfortunately, there is no standard convention for the designation of the spherical angles. At one time, mathematics textbooks denoted the azimuthal angle by ϕ and the co-latitude by θ, and this is still the most common convention in physics books, but most college mathematics texts have now switched to using ϕ for the co-latitude and θ for the azimuthal angle.[3]

A standard unit for measuring distance on the surface of the Earth is the *nautical mile*, which is the length of one minute of arc (1/60th of a degree) along a great circle. This works out to be about 1,852 meters or 6,076 feet (compared to the *statute mile* of 5,280 feet).

Since the equatorial radius and the polar radius of the Earth differ by about 1 part in 300, there is some ambiguity about the precise value of the nautical mile. The U.S. nautical mile was 1853.25 meters or 6080 feet, but this has been replaced by the standard international nautical mile of 1852 meters.[4]

---

[3] The notation is now a hopeless muddle that will be resolved only when the topic of spherical coordinates goes out of fashion in the undergraduate curriculum.

[4] See `http://physics.nist.gov/cuu/Units/outside.html`.

The meter itself was originally intended to be 10^{-7} times the distance from the Equator to the North Pole along a meridian through Paris. Due to its rotation, the Earth would not be a perfect sphere even if its surface were devoid of geographical irregularities such as mountains and valleys, and the first standard meter was slightly short because of a miscalculation. The Earth is not a satisfactory standard for very precise measurements, so for many years, the standard meter was defined by a platinum-iridium bar in Paris. Currently, the meter is defined to be $1/299,792,458$ times the distance that light travels in one second in a vacuum.[5] The National Institute of Standards and Technology provides definitive information about the International System of Units (abbreviated SI from the French *Système International d'Unites*).[6]

Exercise 10.8. Suppose that a Martian nautical mile is defined to be the length of one minute of arc along a great circle on the surface of Mars, and a Martian meter is defined to be 10^{-7} times the distance from the equator of Mars to a pole. How many Martian meters are there in a Martian nautical mile?

In steering a ship at sea, it is most convenient to follow a fixed compass bearing, in other words, a course that makes a fixed angle with each meridian of longitude. Such a course is a *rhumb line*[7] or *loxodrome*.[8] It is important to know how to choose the course to navigate between two locations of prescribed latitude and longitude, and how to determine the loxodromic distance between two points.

Exercise 10.9. It is easy to determine the loxodromic distance (in nautical miles) between two points on the globe if you know the difference in latitudes and the angle that the loxodromic path between them makes with the meridians. Find a formula.

Drawing a planar map of the spherical surface of the Earth is problematical: there is no way to do it without distorting either distances, areas, or shapes. There are various techniques in use for projecting the round Earth

[5] See `http://physics.nist.gov/cuu/Units/meter.html`.

[6] See the online references at `http://physics.nist.gov/cuu/Units/bibliography.html`.

[7] The word "rhumb" comes from the same Greek root that gives us "rhombus".

[8] The "loxo" is a Greek root meaning "oblique" or "slanting", and the "drome" is a Greek root referring to running, as in "hippodrome".

onto a flat map. A glance at a modern atlas reveals a multitude of methods, with names such as azimuthal equal-area projection, azimuthal equidistant polar projection, bipolar oblique conic conformal projection, Bonne projection, Briesemeister elliptical equal-area projection, conic projection, conic equal-area projection, cylindrical projection, cylindrical equal-area projection, Lambert azimuthal equal-area projection, Lambert conformal conic projection, Mercator projection, oblique conic conformal projection, oblique cylindrical projection, polar projection, polyconic projection, and sinusoidal projection.

The most famous method for drawing a flat map of the Earth is the Mercator projection, named for the Flemish surveyor Gerhard Kremer.[9] In the Mercator map, the meridians of longitude appear as evenly spaced vertical straight lines. The parallels of latitude appear as horizontal straight lines, but not evenly spaced: the Mercator map badly distorts distances in the Arctic and in the Antarctic.

The Mercator map is constructed to be *conformal*, meaning that locally it preserves shapes (angles), even though it distorts distances. What is needed for a map to be conformal is that near every point, the distance distortion is the same in all directions.

Exercise 10.10 (The Mercator projection)**.**

1. On the globe, meridians converge at the poles, but on Mercator's map, the meridians are spread apart to be parallel lines. To achieve this effect, how should you choose the length magnification factor along a parallel at latitude x?

2. Conformality demands that the length magnification be the same in the direction of a meridian as in the direction of a parallel. Integrate and use trigonometric identities to show that a point at positive latitude x radians has distance from the equator on Mercator's map equal to

$$\ln \tan\left(\frac{\pi}{4} + \frac{x}{2}\right),$$

where the unit of length is the radius of the globe on which the map is based. (This quantity is also $\operatorname{gd}^{-1}(x)$, where gd is the Gudermannian function of Problem 10.6 below.)

[9] Kremer's Latinized name was Mercator. He lived 1512–1594 and should not be confused with Nicolaus Mercator, who was born in Denmark and lived 1620–1687. This second Mercator is the one who found an infinite series expansion for the logarithm function.

On Mercator's map, the meridians are parallel straight lines, so loxodromic curves are also straight lines. Mercator's map makes it straightforward to determine the proper course heading for a rhumb line between two specified points.

Exercise 10.11. Find the loxodromic distance between Miami Beach, Florida ($25^\circ\, 47'\, 25''$ N, $80^\circ\, 7'\, 49''$ W) and Lisbon, Portugal ($38^\circ\, 42'\, 0''$ N, $9^\circ\, 5'\, 0''$ W).

> My thought, whose murder yet is but fantastical,
> Shakes so my single state of man that function
> Is smother'd in surmise, and nothing is
> But what is not.
>
> William Shakespeare
> *Macbeth*, I. iii. 139–142

10.4 Problems

> Form follows function—that has been misunderstood. Form and function should be one, joined in a spiritual union.
>
> Frank Lloyd Wright

Problem 10.1. The following is purportedly a proof of Taylor's Theorem of order two with remainder.

We want to show that

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \frac{f^{(3)}(c)}{3!}(x-a)^3$$

for some point c between a and x. Start with the mean-value theorem applied to the function f'': namely, $f''(x) = f''(a) + f^{(3)}(c)(x-a)$ for some c. Take the antiderivative of this formula with an appropriate integration constant to get

$$f'(x) = f'(a) + f''(a)(x-a) + f^{(3)}(c)\frac{(x-a)^2}{2}.$$

Now repeat the antiderivative process to get

$$f(x) = f(a) + f'(a)(x-a) + f''(a)\frac{(x-a)^2}{2} + f^{(3)}(c)\frac{(x-a)^3}{3!}.$$

Find all the errors in this alleged proof, and construct appropriate counterexamples to show that the errors you identified are indeed errors.

Problem 10.2. Show that the Maclaurin series expansions of $\tan x$ and $\sec x$ have coefficients that are all non-negative rational numbers.

Problem 10.3. Robinson Crusoe, shipwrecked on a desert island, wants to compute the product $48,480,962 \times 258,819,045$. He has salvaged a table of values of the cosine function (Table 10.1). How can he evaluate this product (to nine significant figures) without much work?

Problem 10.4.

1. Show that the geometric, infinite series, and differential equation definitions for the logarithm function are equivalent.
2. Show that the infinite series and differential equation definitions for the exponential function are equivalent.

Problem 10.5.

1. Show that the logarithm function is transcendental.
2. Show that the trigonometric functions are transcendental.

Problem 10.6 (The Gudermannian)**.** The trigonometric functions are related to the hyperbolic functions via $\cos(ix) = \cosh(x)$, where $i = \sqrt{-1}$. Christoph Gudermann[10] discovered that it is possible to relate the trigonometric functions and the hyperbolic functions without employing complex numbers. The Gudermannian function $\operatorname{gd}(x)$ is defined implicitly via $\sinh x = \tan \operatorname{gd}$, with $-\pi/2 < \operatorname{gd} < \pi/2$.

1. Express each of the six hyperbolic functions of x in terms of the six trigonometric functions of gd.
2. Show that $\tanh(x/2) = \tan(\operatorname{gd}/2)$.
3. Find the derivative $d\operatorname{gd}/dx$.
4. Show that $\operatorname{gd}(x) = 2\tan^{-1}(e^x) - \pi/2$.
5. Show that $x = \ln\tan\left(\dfrac{\pi}{4} + \dfrac{\operatorname{gd}(x)}{2}\right)$. This quantity appeared in Exercise 10.10.

Problem 10.7. Calculate the shortest distance on the globe (great circle route) between Miami Beach, Florida and Lisbon, Portugal.

Problem 10.8. Historical Challenge: Why was Gudermann interested in the Gudermannian function?

[10]Gudermann lived 1798–1852 and is mainly remembered as a teacher of the great Karl Weierstrass.

x	$\cos(x^\circ)$	x	$\cos(x^\circ)$	x	$\cos(x^\circ)$
1	0.9998476952	31	0.8571673007	61	0.4848096202
2	0.9993908270	32	0.8480480962	62	0.4694715628
3	0.9986295348	33	0.8386705679	63	0.4539904997
4	0.9975640503	34	0.8290375726	64	0.4383711468
5	0.9961946981	35	0.8191520443	65	0.4226182617
6	0.9945218954	36	0.8090169944	66	0.4067366431
7	0.9925461516	37	0.7986355100	67	0.3907311285
8	0.9902680687	38	0.7880107536	68	0.3746065934
9	0.9876883406	39	0.7771459615	69	0.3583679495
10	0.9848077530	40	0.7660444431	70	0.3420201433
11	0.9816271834	41	0.7547095802	71	0.3255681545
12	0.9781476007	42	0.7431448255	72	0.3090169944
13	0.9743700648	43	0.7313537016	73	0.2923717047
14	0.9702957263	44	0.7193398003	74	0.2756373558
15	0.9659258263	45	0.7071067812	75	0.2588190451
16	0.9612616959	46	0.6946583705	76	0.2419218956
17	0.9563047560	47	0.6819983601	77	0.2249510543
18	0.9510565163	48	0.6691306064	78	0.2079116908
19	0.9455185756	49	0.6560590290	79	0.1908089954
20	0.9396926208	50	0.6427876097	80	0.1736481777
21	0.9335804265	51	0.6293203910	81	0.1564344650
22	0.9271838546	52	0.6156614753	82	0.1391731010
23	0.9205048535	53	0.6018150232	83	0.1218693434
24	0.9135454576	54	0.5877852523	84	0.1045284633
25	0.9063077870	55	0.5735764364	85	0.0871557427
26	0.8987940463	56	0.5591929035	86	0.0697564737
27	0.8910065242	57	0.5446390350	87	0.0523359562
28	0.8829475929	58	0.5299192642	88	0.0348994967
29	0.8746197071	59	0.5150380749	89	0.0174524064
30	0.8660254038	60	0.5000000000		

Table 10.1: Values of the cosine function

10.5 Additional Literature

1. Man-Keung Siu, "Concept of function—its history and teaching," *Learn from the Masters*, Frank Swetz et al., eds., Mathematical Association of America, 1995, pages 105–121.

2. John Nord and Edward Miller, "Mercator's rhumb lines: A multivariable application of arc length," *The College Mathematics Journal* **27** (1996), number 5, 384–387.

3. I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, fifth edition, edited by Alan Jeffrey, Academic Press, 1994; Library of Congress call number QA55 .G6613 1994. Information about the Gudermannian, for example, is on pages 51–52.

Chapter 11

Plane geometry

Geometry is the art of correct reasoning on incorrect figures.

G. Polya
How To Solve It

11.1 Goals

1. Renew and deepen your acquaintance with linear, quadratic, and cubic equations and their geometric significance.
2. Appreciate the interplay between analytic and algebraic geometry.
3. Learn about non-Euclidean geometries.

11.2 Classroom Discussion

11.2.1 Algebraic geometry

There is no royal road to geometry. Euclid
(to Ptolemy I)

You are familiar with two ways to describe a curve in the two-dimensional plane: you can specify the curve either geometrically, or by a formula. For example, a circle is the locus of points at fixed distance from a specified center point (geometric definition), or the set of points with coordinates (x, y) satisfying an equation of the form $(x-a)^2+(y-b)^2 = r^2$ (analytic definition).

The idea of connecting the two descriptions is due to René Descartes,[1] for whom Cartesian coordinates are named. The interplay between the geometry of curves and their analytic descriptions is the subject of *analytic geometry*. In the case that the formulas are given by polynomial equations, the subject is *algebraic geometry*.

The simplest plane curve is a straight line, which is given by a polynomial equation of first degree: $Ax + By + C = 0$.

> Caesar said to me 'Darest thou, Cassius, now
> Leap in with me into this angry flood,
> And swim to yonder point?'
>
> William Shakespeare
> *Julius Caesar*, I ii

Exercise 11.1. Since a line is uniquely determined by *two* points in the plane, and each point has *two* coordinates, why are there *three* parameters A, B, and C in the general equation of a line?

> Everything an Indian does is in a circle, and that is because the poser of the world always works in circles, and everything tries to be round.
>
> Black Elk

The most familiar way to parametrize the unit circle $x^2+y^2 = 1$ is by using trigonometric functions: $x = \cos t$ and $y = \sin t$. However, it may seem a bit odd to parametrize an algebraic curve with transcendental functions. There is a way to parametrize the circle with rational functions, indeed, with quotients of polynomials of degrees 1 and 2.

Exercise 11.2. Taking as the parameter t the negative of the slope of the line joining $(0, 1)$ to a point on the circle $x^2 + y^2 = 1$, derive the parametrization

$$x = \frac{2t}{1+t^2} \qquad \text{and} \qquad y = \frac{1-t^2}{1+t^2}.$$

The rational parametrization of the circle has interesting applications. For example, you are familiar with Pythagorean triples such as $(3, 4, 5)$ and $(5, 12, 13)$, which correspond to the equalities $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. There are infinitely many essentially distinct such triples, and it is possible to describe all of them.

[1] Lived 1596–1650.

Exercise 11.3. Use the rational parametrization of the circle to find all triples (a, b, c) of positive integers such that $a^2 + b^2 = c^2$.

The recent proof of Fermat's last theorem[2] confirmed that when n is an integer larger than 2, there are no positive integers a, b, and c such that $a^n + b^n = c^n$. Evidently, one cannot expect in general to find a rational parametrization of a plane curve given by a polynomial equation of degree larger than 2.

A topic that is falling out of fashion in the second-semester calculus course is a substitution that converts the integral of a rational function of $\cos x$ and $\sin x$ into the integral of a rational function of a new variable t. If this substitution is presented at all, it is given as a magical formula without motivation. In fact, the substitution is nothing more than the rational parametrization of the circle.

> Take a circle, caress it, and it will turn vicious.[3] Eugène Ionesco
> *The Bald Soprano*

Exercise 11.4. Convert the integral $\displaystyle\int \frac{dx}{1+\cos x}$ into the integral of a rational function of t by using the rational parametrization of the circle. Evaluate the integral, and reconstitute your answer as a function of x. Can you reconcile your result with the answer $\tan(x/2)$ that Maple gives?

The most general polynomial equation of degree two in variables x and y has the form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Such an equation describes a *conic* curve, so called because the ellipse, hyperbola, and parabola can be obtained by slicing a cone with a plane at different angles. In degenerate cases, a conic can reduce to a line (for instance, $x = 0$), a pair of parallel lines (for instance, $x^2 - 1 = 0$), a pair of intersecting lines (for instance, $xy = 0$), a single point (for instance, $x^2 + y^2 = 0$), or the empty set (for instance, $x^2 + y^2 + 1 = 0$).

[2] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, *Annals of Mathematics (2)* **141** (1995), number 3, 443–551; Andrew Wiles and Richard Taylor, Ring-theoretic properties of certain Hecke algebras, *ibid.*, 553–572.

[3] *Prenez un cercle, caressez-le, il deviendra vicieux!* The meaning of *vicious circle* is the same in French as in English.

Exercise 11.5. Under what conditions on a, b, c, d, e, and f does the above equation describe an ellipse? a hyperbola? a parabola?

Two points determine a line. Three points determine a circle (Problem 11.1). Four points, however, do not determine a general conic curve.

> The billiard sharp whom any one catches,
> His doom's extremely hard—
> He's made to dwell—
> In a dungeon cell
> On a spot that's always barred.
> And there he plays extravagant matches
> In fitless finger-stalls
> On a cloth untrue
> With a twisted cue
> And elliptical billiard balls.
>
> W. S. Gilbert
> *The Mikado*

Exercise 11.6. Find two different ellipses passing through the four points $(1, 1)$, $(-1, 1)$, $(-1, -1)$, and $(1, -1)$.

On the other hand, six points will not lie on a conic unless the points are in special positions.

Exercise 11.7. Show that no conic contains the six points $(1, 1)$, $(-1, 1)$, $(-1, -1)$, $(1, -1)$, $(0, 0)$, and $(1, 0)$.

Five points in general position determine a conic, but in degenerate cases the conic may not be uniquely determined.

Exercise 11.8.

1. Show that if five points are specified in the plane, then there is at least one conic (possibly a degenerate one) passing through all five points.

2. Find two distinct (degenerate) conics passing through the five points $(0, 0)$, $(0, 1)$, $(1, 0)$, $(2, 0)$, $(3, 0)$.

A *cubic* curve is specified by a polynomial in x and y of degree 3. Such curves begin to have sufficient complexity that it becomes tedious to sketch their graphs by hand, but you can easily display pictures of such curves using a graphing calculator or computer (Problem 11.4).

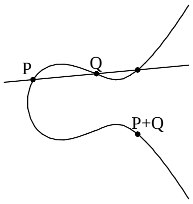


Figure 11.1: The cubic curve $4y^2 = (x+4)(x^2+1)$

Exercise 11.9. How many points would you expect to need to specify in order to determine a cubic curve?

Nondegenerate cubic curves have the remarkable property that their points carry a natural group structure. This is illustrated for the specific cubic $4y^2 = (x+4)(x^2+1)$ in Figure 11.1. The addition law is determined in the following way. If P and Q are points on the cubic, draw the line through them. It intersects the cubic at a third point. The reflection of this point with respect to the x-axis is defined to be the sum $P+Q$.

A group is supposed to have an identity element E with the property that $P+E=P$ for every P. There is no such point on the cubic, but we can supplement the cubic with an idealized point "at infinity" that will serve as the identity element if we agree that all vertical lines pass through the point at infinity.

Exercise 11.10. For the cubic $4y^2 = (x+4)(x^2+1)$ shown in Figure 11.1, use the group law to find the sum of the two points $(-4,0)$ and $(0,1)$.

> Till that Bellona's bridegroom, lapp'd in proof,
> Confronted him with self-comparisons,
> Point against point, rebellious arm 'gainst arm,
> Curbing his lavish spirit: and, to conclude,
> The victory fell on us.
>
> William Shakespeare
> *Macbeth*, I ii

Exercise 11.11. Verify that the addition law described above does provide the cubic curve with the structure of a commutative group.

1. The rule specifying the addition law needs to be modified for the case $P = Q$. How should $P + P$ be defined?

2. The rule needs to be modified when the line joining P and Q is tangent to the curve at P. How should $P + Q$ be defined in this case?

3. Check that the addition is commutative.

4. Check that the point at infinity does act as an identity element.

5. What is the additive inverse of a point P?

6. A group law is supposed to be associative. The (not so easy) verification of associativity is left for Problem 11.6.

11.2.2 Non-Euclidean geometry

> The eye is the first circle; the horizon which it forms is the second; and throughout nature this primary figure is repeated without end. It is the highest emblem in the cipher of the world. St. Augustine described the nature of God as a circle whose centre was everywhere, and its circumference nowhere. We are all our lifetime reading the copious sense of this first of forms. One moral we have already deduced, in considering the circular or compensatory character of every human action. Another analogy we shall now trace; that every action admits of being outdone. Our life is an apprenticeship to the truth, that around every circle another can be drawn; that there is no end in nature, but every end is a beginning; that there is always another dawn risen on mid-noon, and under every deep a lower deep opens. Ralph Waldo Emerson
>
> *Essays*, x. Circles

You probably saw in high school some basic notions from Euclidean geometry such as the principle of similar triangles and the construction of a perpendicular bisector of a line segment. The next exercise is a typical example of that kind of reasoning.

Exercise 11.12. 1. By considering a circle circumscribed around a triangle, show that the perpendicular bisectors of the three sides of a triangle meet at a common point.

2. By considering a circle inscribed in a triangle, show that the lines bisecting the three angles of a triangle meet at a common point.

3. By making a copy of a triangle four times as big as the original, show that the three altitudes of a triangle meet at a common point.

Euclid's *Elements* builds up the theory of ordinary planar geometry from a few basic assumptions and "common notions." Euclid's axioms are the following.

1. A straight line segment can be drawn from any point to any other point.
2. A straight line segment can be extended continuously to a straight line.
3. A circle can be drawn with any center and any radius.
4. All right angles are equal.
5. Parallel postulate: through a given point not on a given line can be drawn exactly one line parallel to the given line.

> As Lines so Loves Oblique may well
> Themselves in every Angle greet:
> But ours so truly Parallel,
> Though infinite can never meet.
>
> Andrew Marvell
> *The Definition of Love*

Euclid's fifth axiom—the parallel postulate—was a source of controversy for centuries. Many people tried to prove it from the other axioms, and some thought that they succeeded. In fact, however, the fifth axiom is independent of the others. In other words, it is possible to construct a geometric model that satisfies the first four axioms but not the fifth. One such model is hyperbolic geometry in the unit disk. Figure 11.2 shows a picture of some lines in the "Poincaré unit disk."

In the hyperbolic disk, "lines" are arcs of circles that are orthogonal to the boundary unit circle at both intersection points. Diameters of the unit circle also count as "lines." Notice in Figure 11.2 the two intersecting lines that are

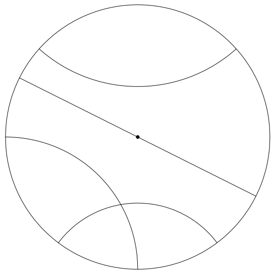


Figure 11.2: The Poincaré unit disk

disjoint from (that is, "parallel to") the other two lines. Thus Euclid's fifth axiom does not hold in the hyperbolic disk.

> What! will the line stretch out to the crack of doom?
>
> William Shakespeare
>
> *Macbeth*, IV i

Exercise 11.13. Verify Euclid's first axiom for the hyperbolic disk.

The distance between points in the hyperbolic disk is obtained by integrating $\dfrac{ds}{1-x^2-y^2}$ along the "line" joining the points. Distances become very large near the boundary of the disk. The boundary circle is not included as part of the hyperbolic disk. Indeed, the boundary is at infinite distance from any point of the disk, so Euclid's second axiom is satisfied. Angles are computed in the usual way: the angle of intersection of two curves is the angle between their tangent lines.

> For precept must be upon precept, precept upon precept; line upon line, line upon line; here a little, and there a little. *Isaiah*, 28:10

Exercise 11.14. Compute the sum of the angles of the hyperbolic triangle with vertices at $(0,0)$, $(0,1/2)$, and $(1/2,0)$. See Figure 11.3.

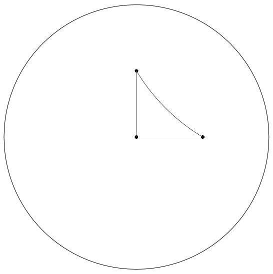


Figure 11.3: A hyperbolic triangle

> "If you were sensible of your own good, you would not wish to quit the sphere in which you have been brought up." Jane Austen
> *Pride and Prejudice*
> (Lady Catherine de Bourgh, to Elizabeth Bennet)

One can also put a "spherical geometry" on the plane by using stereographic projection (Problem 11.10). It is more convenient, however, to think of this geometry on the sphere itself. The "lines" are great circles on the sphere (circles whose radius is the same as the radius of the sphere). In spherical geometry, Euclid's fifth postulate fails not because there are too many parallel lines, but because there are none! In hyperbolic geometry, the angles of a triangle sum to less than 180°, while in spherical geometry, the angles of a triangle sum to more than 180°.

Exercise 11.15. Find a spherical triangle with three right angles.

> He has many friends, laymen and clerical.
> Old Foss is the name of his cat:
> His body is perfectly spherical,
> He weareth a runcible hat. Edward Lear
> *Nonsense Songs*

Exercise 11.16. A photographer for *National Geographic* sets out to capture a bear on film. She walks one mile due south from base camp, then one mile due east, takes a picture of a bear, turns due north, walks one mile and is back at camp. What color was the bear?

The wheel is come full circle; I am here. — William Shakespeare, *King Lear*, V iii

11.3 Problems

Let no one enter who does not know geometry.
inscription on Plato's door

Problem 11.1. Show that if three points in the plane are not all on the same line, then there is one and only one circle passing through them.

Problem 11.2. Show that if five points are specified in the plane, and if no four of the points are on the same line, then there is a *unique* conic (possibly degenerate) passing through the five points.

Problem 11.3. Suppose given an infinite sequence of points in the plane with the property that for every pair of points, the distance separating them is an integer. Prove that the points must all lie on a line.[4]
Hint: what sort of curve is the locus of points whose distances from two specified locations have a fixed difference?

Problem 11.4. Produce pictures (by computer, if you like) of the graphs of the three cubics defined by the equations $y^2 = x^3 + x^2 + 2x + 1$, $y^2 = x^3 + x^2$, and $y^2 = x^3 + x^2 - 2x - 1$. Observe that the three graphs look very different from each other.

Problem 11.5. Show that if two points P and Q on the cubic shown in Figure 11.1 have coordinates that are rational numbers, then the coordinates of the sum point $P + Q$ are again rational numbers.

Problem 11.6. Prove that the addition law for points on the cubic curve shown in Figure 11.1 is associative.

[4]In February 1958, this problem was posed as part of the eighteenth William Lowell Putnam mathematical competition. The result first appeared in a paper by Norman H. Anning and Paul Erdős, Integral distances, *Bulletin of the American Mathematical Society* **51** (1945), 598–600. According to legend, a follow-up paper giving a simpler solution was ghost-written for Erdős by the reviewer Irving Kaplansky, and the review of that paper was ghost-written for Kaplansky by the editor of *Mathematical Reviews*. (See *Lion Hunting and Other Mathematical Pursuits*, edited by Gerald L. Alexanderson and Dale H. Mugler, Mathematical Association of America, 1995, pages 33–34.) However, a different story appeared in the *Mathematical Intelligencer* **14** (1992), number 1, 56–57.

Problem 11.7. Verify Euclid's third axiom for the hyperbolic disk.

Problem 11.8. Knowing how to compute length in the hyperbolic disk, how might you define area in the hyperbolic disk?

Problem 11.9. Show that the (hyperbolic) area of the hyperbolic triangle shown in Figure 11.3 equals $\frac{1}{2}\arctan(1/4)$.

Problem 11.10. The planar model of spherical geometry is obtained from the spherical model by *stereographic projection.* Imagine a sphere resting on the plane with its south pole at the origin[5] and a light source at the north pole. A point on the sphere casts a shadow on the plane. The "straight lines" in the plane are defined to be the shadows of great circles. Prove the remarkable fact that these "straight lines" in the plane are actually ordinary circles (unless the great circle passes through the poles, in which case its projection is an ordinary straight line).

Problem 11.11. Show that the area of a spherical triangle on a sphere of radius 1 is $\Delta - \pi$, where Δ is the sum of the angles (in radians) of the triangle.

11.4 Additional Literature

1. H. S. M. Coxeter, *Non-Euclidean Geometry*, University of Toronto Press, 1942. (QA 685 C7.8)

2. Arlan Ramsay and Robert D. Richtmyer, *Introduction to Hyperbolic Geometry*, Springer-Verlag, 1995. (QA 685 R18 1995)

3. Jeffrey R. Weeks, *The Shape of Space*, Marcel Dekker, 1985. (QA 612.2 W44 1985)

[5] An alternate version of stereographic projection places the center of the sphere at the origin.

Chapter 12

Beyond the real numbers

Hence, horrible shadow!
Unreal mockery, hence!

William Shakespeare
Macbeth, Act III, Scene iv

12.1 Goals

1. Learn some of the history, properties, and applications of the complex numbers.

2. Learn some of the history, properties, and applications of the quaternions.

3. Prove the Fundamental Theorem of Algebra and appreciate its beauty.

12.2 Reading

1. B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, 1985, pages 52–62, 94–102, and 177–186.

2. William Dunham, *Journey through Genius: The Great Theorems of Mathematics*, Wiley, 1990, Chapter 6: Cardano and the Solution of the Cubic, pages 133–154.

3. Uwe F. Mayer, "A Proof that Polynomials have Roots," The College Math Journal, **28**, (1997), number 1, page 58.

4. David Eugene Smith, *A source book in Mathematics*, Dover, 1959, "Gauss", pages 292–306.

12.3 Classroom Discussion

12.3.1 The complex numbers

Exercise 12.1 (Warm up)**.** A high school student says, "When I enter the number -1 on my calculator and push the square-root key, I get an error message. Therefore the equation $x^2 + 1 = 0$ has no solution." How would you respond?

What are the complex numbers? There are several ways to think about them. The most familiar description is that the complex numbers consist of all expressions $a + bi$, where a and b are ordinary real numbers, and the imaginary unit i has the property that $i^2 = -1$. Such expressions are added and multiplied by following the usual rules of "high school algebra", with the additional rule that all occurrences of i^2 should be replaced by -1. Consequently, it is easy to see that the operations of addition and multiplication of complex numbers satisfy the usual commutative, associative, and distributive laws.

> Friendship is only a reciprocal conciliation of interests, and an exchange of good offices; it is a species of commerce out of which self-love always expects to gain something.
>
> Francis, Duc de La Rochefoucauld
> (1613–1680)
> *Reflections, or Sentences and Moral Maxims*
> Maxim 83

Exercise 12.2. Show that if a and b are not both zero, then the reciprocal $\dfrac{1}{a + bi}$ of a complex number is again a complex number: it can be rewritten in the form $A + Bi$ for suitable real numbers A and B.

In more abstract language, we can say that the complex numbers are a *field*, in fact, an extension of the field of real numbers.

Exercise 12.3. In the field of complex numbers, what is the additive identity? the multiplicative identity?

An alternative definition of the complex numbers—first made explicit by the nineteenth-century Irish mathematician William Rowan Hamilton—is the set of all ordered pairs (a, b) of real numbers subject to the addition law $(a, b)+(c, d) = (a+c, b+d)$ and the multiplication law $(a, b)\cdot(c, d) = (ac-bd, ad+bc)$.

Exercise 12.4. In what sense is this definition the same as the usual one?

The identification of a complex number $a+bi$ with a vector (a, b) means that the complex numbers can be viewed geometrically as points in the ordinary Euclidean plane. Consequently, a complex number $a + bi$ has an associated length $\sqrt{a^2 + b^2}$, called its *modulus* and often written $|a+bi|$, and an associated angle $\arctan b/a$, called its *argument* and often written $\arg(a + bi)$. (Just like the angle in polar coordinates, the argument of a complex number is determined only up to integral multiples of 2π.)

The truth is always the strongest argument. Sophocles 496–406 B.C.

Exercise 12.5. Find the modulus and the argument of the following complex numbers: 1; i; $1 + i$; $-2/(1 + \sqrt{3}\, i)$; $i/(-2 - 2i)$.

Exercise 12.6. What familiar geometric object is the set of complex numbers z with the property that $|z - i| = 4$?

Exercise 12.7. The *triangle inequality* says that $|z + w| \leq |z| + |w|$ for all complex numbers z and w. Prove the triangle inequality, and interpret it geometrically by representing complex numbers as vectors in the plane.

The complex numbers can also be represented as the set of all 2×2 matrices $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$, where a and b are real numbers, the addition and multiplication operations being the usual ones for matrices.

Exercise 12.8.

1. In what sense is this definition the same as the previous ones?
2. Matrix multiplication is a basic example of a noncommutative operation. However, multiplication of complex numbers is a commutative operation. Explain why there is not a conflict with your preceding answer.

One motivation for introducing the complex numbers is to force the "unsolvable" quadratic equation $x^2 + 1 = 0$ to have a solution. This idea can be used to give the complex numbers an algebraic definition. Namely, define an equivalence relation on the set of polynomials with real coefficients by declaring polynomials p and q to be equivalent if and only if there exists a polynomial r (which could be a constant, or even 0) such that $p(x) - q(x) = (x^2 + 1)r(x)$ for all x.

Exercise 12.9. Verify that this is an equivalence relation.

Now define the complex numbers to be the set of all equivalence classes. The operations of addition and multiplication are inherited from the corresponding operations on polynomials. (In the notation of abstract algebra, this definition says that the complex numbers are the quotient ring $\mathbf{R}[x]/(x^2+1)$.)

Exercise 12.10. Confirm that this definition makes sense and is compatible with the other definitions of the complex numbers. Which equivalence class corresponds to the complex number i?

We know what i^2 means (namely, $i \times i$, or -1), but what might 2^i mean? We are free to give this symbol whatever meaning seems reasonably consistent with the notion of exponentiation of real numbers. One way to characterize the usual real exponential function is that e^{kx} is the unique solution of the differential equation $f'(x) = kf(x)$ satisfying the initial condition $f(0) = 1$. If there is going to be a reasonable generalization of the exponential function to complex numbers, we would expect e^{ix} to be a function whose derivative is ie^{ix} and whose second derivative is $-e^{ix}$. On the other hand, we know that two linearly independent solutions of the differential equation $g''(x) = -g(x)$ are $\cos(x)$ and $\sin(x)$. Consequently, we expect there to be (complex) constants c_1 and c_2 such that $e^{ix} = c_1 \cos(x) + c_2 \sin(x)$.

Exercise 12.11. Assuming that the complex exponential function suggested by the preceding heuristic argument does exist, deduce Euler's formula

$$e^{ix} = \cos(x) + i \sin(x).$$

Exercise 12.12. Observing that $2 = e^{\log 2}$, express 2^i in the form $a+bi$, where a and b are real numbers.

Specializing Euler's formula to $x = \pi$ gives a formula regarded by many as one of the most beautiful in mathematics:

$$e^{i\pi} = -1.$$

Here we see in one formula the base of the natural logarithms, the imaginary unit, and the ratio of the circumference of a circle to its diameter.

Exercise 12.13. Use Euler's formula to show that every nonzero complex number can be written in the form $re^{i\theta}$, where r equals the modulus and θ equals the argument.

Exercise 12.14.

1. Write $(1+i)^{99}$ in the form $a + bi$, where a and b are real numbers.
2. The complex number $1 - \sqrt{3}\,i$ has two square roots. Find them.

The real logarithm function is often defined as the inverse of the real exponential function: namely, $e^{\log x} = x$ and $\log e^x = x$ for every real number x. This definition makes sense because the real exponential function is strictly increasing and hence one-to-one. The complex exponential function, however, is very far from being one-to-one: every point of its image has infinitely many pre-images.

Exercise 12.15. Show that the complex exponential function $z \mapsto e^z$ is periodic with period $2\pi i$.

To define a complex logarithm function as an inverse of the complex exponential function, we need to restrict the domain of the exponential function to a set on which the function is one-to-one. Different choices of domain lead to different *branches* of the logarithm function. In view of the periodicity of the complex exponential function, the most natural restricted domain is a horizontal strip of height 2π in the complex plane. The *principal branch* of the logarithm corresponds to taking this strip to be centered on the real axis, so that the imaginary part of z lies between $-\pi$ and π.

> Those green-robed senators of mighty woods,
> Tall oaks, branch-charmed by the earnest stars,
> Dream, and so dream all night without a stir.
>
> John Keats
> 1795–1821
> *Hyperion*, Book I

Exercise 12.16. Determine the principal value of i^i. What are the other possible values of i^i (corresponding to different branches of the logarithm)?

12.3.2 The solution of cubic and quartic equations

> The shortest path between two truths in the real domain passes through the complex domain.
>
> Jacques Hadamard
> 1865–1963
> (attributed)

It is a remarkable phenomenon that complex numbers arise naturally in problems about real numbers. This phenomenon was first observed in the Renaissance, when solving cubic and quartic equations was a hot research topic. It turns out that there are formulas for the solutions of cubic and quartic equations, but the formulas may involve complex numbers even when the solutions turn out to be real numbers.

Exercise 12.17. It is not obvious how to simplify complicated expressions involving roots. For example, how does $\sqrt[4]{97+\sqrt{9408}}$ simplify? If you are stuck, look at the answer in the footnote for a clue.[1]

The key to solving a cubic equation is to use some trickery to reduce the problem to solving an associated quadratic equation. A first step is to eliminate the quadratic term in a cubic equation.

Exercise 12.18. Show how to choose d so that the change of variable $x = y-d$ transforms the general cubic equation $y^3+Ay^2+By+C = 0$ to the "reduced" cubic equation $x^3 - 3ax - 2b = 0$.

The formula due to Tartaglia and Cardano is that a solution of the reduced cubic equation $x^3 - 3ax - 2b = 0$ is given by

$$x = \sqrt[3]{b+\sqrt{b^2-a^3}} + \sqrt[3]{b-\sqrt{b^2-a^3}}. \tag{12.1}$$

> The insane root
> That takes the reason prisoner.
>
> William Shakespeare
> *Macbeth*, Act I, Scene iii

Exercise 12.19. Verify that formula (12.1) gives a correct real-valued solution of the reduced cubic equation $x^3 - 3x - 2 = 0$.

---

[1] It equals $2+\sqrt{3}$.

One way to derive the formula is to introduce two auxiliary variables u and v such that $u+v=x$. Substituting into the cubic equation and simplifying gives $u^3+v^3-2b+(u+v)(3uv-3a)=0$, which will certainly be true if u and v satisfy the simultaneous equations

$$\begin{aligned} u^3+v^3 &= 2b \\ uv &= a. \end{aligned}$$

Exercise 12.20. Solve the simultaneous equations by eliminating v and solving a quadratic equation for u^3. Deduce formula (12.1).

Exercise 12.21. Use (12.1) to find the three real solutions of the cubic equation $x^3-6x-4=0$. Observe that although (12.1) initially produces answers involving complex numbers, simplification leads to real answers.

Just as one can solve a cubic equation by reducing it to an associated quadratic equation, one can solve a quartic equation by reducing it to an associated cubic equation. A first step is to eliminate the cubic term in a quartic equation.

Exercise 12.22. Show how to choose d so that the change of variable $x=y-d$ transforms the general quartic equation $y^4+Ay^3+By^2+Cy+D=0$ to the reduced quartic equation $x^4+ax^2+bx+c=0$.

François Viète had the following idea for solving a reduced quartic equation $x^4+ax^2+bx+c=0$: introduce a second variable z and add $2x^2z+z^2$ to both sides of the equation to create a perfect square on the left-hand side. This manipulation yields the new equation

$$(x^2+z)^2=(2z-a)x^2-bx+z^2-c. \tag{12.2}$$

The right-hand side will also be a perfect square if z is chosen appropriately.

> Read not my blemishes in the world's report;
> I have not kept my square, but that to come
> Shall all be done by the rule. William Shakespeare
> *Antony and Cleopatra*, Act II, Scene iii

Exercise 12.23. Show that the condition for the right-hand side of equation (12.2) to be a perfect square is a certain cubic equation in z.

Since we already know how to solve a cubic equation, we can determine a suitable value for z. Then by taking square roots in (12.2), we get a quadratic equation for x, which we can solve too.

Exercise 12.24. Solve $x^4 - 2x^2 - 16x + 1 = 0$.
Hint: the associated cubic equation has an integer solution that is easier to find *without* using formula (12.1).

12.3.3 The fundamental theorem of algebra

In the previous section, you derived formula (12.1) for solving a cubic equation. The procedure for solving a quartic equation can also be codified into a formula, but the formula is too complicated to be of practical use. It is a surprising theorem of Niels Abel[2] that there is no general formula for writing down the solution of every fifth degree polynomial equation in terms of radicals. A characterization of when a polynomial equation is solvable by radicals was found by Évariste Galois, a political revolutionary who was arrested for threatening the life of king Louis Philippe.[3]

> A radical is a man with both feet firmly planted in the air.
> Franklin D. Roosevelt
> (1882–1945)

Of course, to say that the general quintic equation cannot be solved by radicals is not to say that every quintic equation is unsolvable. There actually is a formula for solving those quintics that can be solved by a formula.[4] For example, the quintic equation $x^5 + 15x + 12 = 0$ has a unique real root.

Exercise 12.25. Why?

---

[2]A Norwegian mathematician, Abel lived 1802–1829. He died tragically young, a victim of tuberculosis.

[3]In his short life (1811–1832), Galois made revolutionary contributions to algebra, but he failed to express himself in a way that his contemporaries could understand. He introduced the word "group" in its modern algebraic sense. Galois died in a duel—the circumstances of which are still under dispute by historians—before reaching his twenty-first birthday.

[4]Although this statement sounds tautological, it has nontrivial content! See D. S. Dummit, Solving solvable quintics, *Mathematics of Computation* **57** (1991), 387–401, from which the example is taken.

The real root of this quintic equation is given by the following expression involving square roots and fifth roots:

$$-\frac{1}{5}\Bigg(\sqrt[5]{1875+525\sqrt{10}}+\sqrt[5]{1875-525\sqrt{10}} \\ +\sqrt[5]{-5625+1800\sqrt{10}}-\sqrt[5]{5625+1800\sqrt{10}}\Bigg)$$

(where the real fifth root is taken in each term).

Evidently, the problem of explicitly finding roots of polynomial equations is a difficult one. It is therefore useful to have an existence theorem.

According to the fundamental theorem of algebra, every polynomial equation with real or complex coefficients does have a solution in the complex numbers (unless, of course, the polynomial is a constant). Thus, not only does the equation $x^2+1=0$ have a solution in the complex numbers, but so do the equations $x^{28}+37x^{14}+92x^6+13=0$ and $x^4+(2+3i)x^2+(9-2i)=0$. In other words, the complex numbers form an algebraically closed field.

There are many proofs of the fundamental theorem of algebra. The goal of this section is to work through a short one based on ideas from advanced calculus. The following exercise says that if we are looking for a point in the complex plane where a polynomial is equal to zero, then we should look close to home.

Exercise 12.26. If p is a nonconstant polynomial, then $\lim_{|z|\to\infty}|p(z)|=\infty$. Here $|z|\to\infty$ means that z escapes from every disk centered at the origin.

Exercise 12.27. Deduce that since a continuous, real-valued function on a closed, bounded subset of the plane attains a minimum on the set, there is a point a in the plane such that $|p(a)|\le|p(z)|$ for every complex number z.

Evidently our candidate for a solution to the equation $p(z)=0$ should be the point $z=a$ where $|p(z)|$ attains a minimum. To confirm that this candidate works, we need to analyze the local behavior of the polynomial p near a. There exist a positive integer k, a nonzero complex number b, and a polynomial q such that

$$p(z)=p(a)+b(z-a)^k+(z-a)^{k+1}q(z)$$

for all z.

Exercise 12.28. Why can the polynomial p be represented in this way?

Suppose, seeking a contradiction, that $p(a) \neq 0$. Let θ denote the difference between the argument of $p(a)$ and the argument of b.

> Nor knowest thou what argument
> Thy life to thy neighbor's creed has lent.
> All are needed by each one;
> Nothing is fair or good alone.
>
> Ralph Waldo Emerson (1803–1882)
> *Each and All*

Exercise 12.29. Show that if ϵ is a sufficiently small positive real number, then $|p(a + \epsilon e^{i(\theta-\pi)/k})| < |p(a)|$.

Since $|p(z)|$ was supposed to have a global minimum at $z = a$, we have a contradiction. This shows that $p(a)$ must be zero after all, and so the fundamental theorem of algebra is proved.

12.3.4 Reflections and rotations

> But with the morning cool reflection came.
>
> Sir Walter Scott (1771–1832)
> *Chronicles of the Canongate*, Chapter iv

Complex numbers provide a convenient notation to describe transformations of the Euclidean plane. For example, taking the complex conjugate (that is, transforming $x+iy$ into $\overline{x+iy} = x-iy$) corresponds to reflection with respect to the x-axis. From the representation of a complex number in the form $re^{i\theta}$, it follows that multiplication by $e^{i\varphi}$ corresponds to rotation by the angle φ in the positive (counterclockwise) direction. If $w = a+bi$ is a fixed complex number, then the transformation $z \mapsto z+w$ is a translation of the plane a units to the right and b units vertically.

Exercise 12.30. Using the notation of complex numbers, write a formula describing reflection with respect to a line making an angle φ with the x-axis.

Suppose we view the complex plane as a sheet of newspaper spread out on a desk. We can transform the plane into itself by sliding the paper around on the desk. Evidently the set of all sliding motions forms a group. An element of this group can be viewed as the composition of some finite sequence of translations and rotations. If we admit the possibility of picking the sheet of paper up and flipping it over, then we obtain a larger group of rigid motions: namely, the group of isometries (distance-preserving transformations) of the plane. It is remarkable that every sliding motion can be obtained as the composition of just two reflections, and every isometry can be obtained as the composition of three reflections.

To see this, pick any two points p and q in the plane. Denote their images under an isometric transformation T by Tp and Tq. A reflection across the perpendicular bisector of the line segment joining p and Tp maps p to Tp and q to some new point q'. Because both T and reflection preserve distances, the line segment joining Tp to Tq has the same length as the line segment joining Tp to q'. Consequently, the perpendicular bisector of the line segment joining Tq and q' is also the angle bisector of the angle determined by Tq, Tp, and q'. A reflection across this perpendicular bisector therefore takes q' to Tq while keeping Tp fixed. Now consider any third point r in the domain plane. A distance-preserving transformation that takes p to Tp and q to Tq can take r to one of only two locations, since there are only two triangles congruent to the triangle pqr and having Tp and Tq as vertices; moreover, the two possible locations for the image of r are reflections of each other across the line through Tp and Tq. Therefore T is the composition of either two or three reflections.

Exercise 12.31. Show that if a rigid motion of the plane is the composition of two reflections, then it preserves the sense of angles, while if it is the composition of three reflections, then it reverses the sense of angles.

> Remembrance and reflection how allied!
> What thin partitions sense from thought divide!
>
> Alexander Pope
> (1688–1744)
> *Essay on Man*, Epistle i, line 225

A rotation is a rigid motion, and so every rotation can be realized as the composition of two reflections. It is illuminating to see which two reflections generate a rotation by angle θ. A rotation by angle θ about the origin is described by $z \mapsto e^{i\theta}z$. By rewriting $e^{i\theta}z$ as $\overline{e^{-i\theta/2}\bar{z}e^{i\theta/2}}$, we find from Exercise 12.30 that the rotation is the composition of reflections in two lines making an angle of $\theta/2$ with each other.

Exercise 12.32. Show that a rotation by angle θ about an axis in three-dimensional space can be realized as the composition of two reflections in planes whose line of intersection is the rotation axis and whose normal lines make an angle of $\theta/2$ with each other.

12.3.5 Quaternions

The complex numbers arise from the real numbers by adjoining a quantity i with the property that $i^2 = -1$. It is natural to consider the possibility of extending the complex numbers by adjoining another quantity j to form objects of the form $a + bi + cj$. However, there is no reasonable way to make such an extension.

Exercise 12.33. Show that there is no consistent way to define multiplication on objects of the form $a + bi + cj$, where a, b, and c are real numbers, if all of the following properties are to hold:

- closure under multiplication;
- the usual associative and distributive laws;
- $i^2 = -1$;
- $a + bi + cj = 0$ if and only if a, b, and c are all 0.

A famous story from the history of mathematics relates that William Rowan Hamilton spent years looking for a way to multiply and divide triples of real numbers. He failed, because no such operation exists. One of his attempts was what we now call the cross product. Recall that the cross product of two vectors in three-dimensional space is a vector perpendicular to both and with length equal to the product of the lengths of the two vectors times the sine of the angle between them.

> A man I am, cross'd with adversity. William Shakespeare
> *The Two Gentlemen of Verona*, Act iv, Scene 1

Exercise 12.34. Three-dimensional vectors equipped with the usual addition and with the cross product fail to form a field. Which properties of a field are lacking?

Each cursed his fate that thus their project crossed;
How hard their lot who neither won nor lost!

Richard Graves
(1715–1804)
The Festoon

Reportedly, a game in the Hamilton household was for the children to ask at mealtimes, "Papa, have you found a way to divide triples?" In response, Hamilton would say in lugubrious tones, "No, I can only multiply them."

The story continues that on the morning of Monday, October 16, 1843, Hamilton had a flash of insight while strolling with his wife along the Royal Canal: he suddenly realized that the problem of multiplying and dividing vectors could be solved in *four*-dimensional space. He was so taken with his discovery that he carved it into the stones of Brougham Bridge, an action that historians seem to consider romantic, although nowadays it would bring a fine for defacing public property. Hamilton had discovered the *quaternions*: the set of objects $a+bi+cj+dk$, where a, b, c, and d are real numbers, multiplied according to the usual rules of high school algebra, but with the additional rules that $i^2 = j^2 = k^2 = ijk = -1$. One of the revolutionary aspects of Hamilton's work was the noncommutativity of the multiplication law.

Exercise 12.35. Show that the rules $i^2 = j^2 = k^2 = ijk = -1$ imply the properties $ij = k = -ji$, $jk = i = -kj$, and $ki = j = -ik$.

In analogy with the complex numbers, quaternions have a conjugation operation. If $Q = a+bi+cj+dk$, where a, b, c, and d are real numbers, then $\bar{Q}$ is defined to be $a-bi-cj-dk$. It is easy to see that $Q\bar{Q} = a^2+b^2+c^2+d^2$, so $\sqrt{Q\bar{Q}}$ is the *length* of Q. According to the next exercise, the operations of conjugation and multiplication interact with a twist.

Exercise 12.36. Show that if Q_1 and Q_2 are quaternions, then $\bar{Q}_1\bar{Q}_2 = \overline{Q_2Q_1}$.

Exercise 12.37. Show that if a, b, c, and d are not all zero, then the reciprocal $\dfrac{1}{a+bi+cj+dk}$ of a quaternion is again a quaternion: it can be written in the form $A+Bi+Cj+Dk$ for suitable real numbers A, B, C, and D.

You are probably familiar with the idea of representing vectors in three-dimensional space as linear combinations of orthogonal basis vectors i, j, and k. This idea comes directly from Hamilton's work. He viewed a quaternion $a+bi+cj+dk$ as consisting of a scalar part a and a "pure quaternion" part $bi+cj+dk$, which he termed a "vector". Thus, quaternions can be used as a tool for the analysis of three-dimensional vectors.

Exercise 12.38. Show that if V and W are pure quaternions, then

$$VW = -V \cdot W + V \times W. \tag{12.3}$$

The multiplication on the left-hand side is quaternionic multiplication, while the multiplication operations on the right-hand side are the scalar product ("dot product") and vector product ("cross product") of the associated vectors.

An interesting application of quaternions is to describe motions of three-dimensional space. For example, suppose V is a fixed unit vector, and consider the transformation that sends a variable vector W into VWV. According to the preceding exercise,

$$\begin{aligned} VWV &= -(V \cdot W)V + (V \times W)V \\ &= -(V \cdot W)V - (V \times W) \cdot V + (V \times W) \times V \\ &= -(V \cdot W)V + (V \times W) \times V, \end{aligned} \tag{12.4}$$

the last step following because the vector $V \times W$ is orthogonal to the vector V. In particular, the quaternionic product VWV of vectors (pure quaternions) is again a pure quaternion. We can now investigate how the transformed vector VWV compares to W.

Exercise 12.39. Show that if the vector W is orthogonal to the unit vector V, then $VWV = W$.

On the other hand, (12.4) implies that $VVV = -V$. Since every vector can be decomposed into the sum of a vector orthogonal to V and a vector parallel to V, it follows that the transformation $W \mapsto VWV$ is reflection in the plane perpendicular to the unit vector V.

According to Exercise 12.32, the composition of reflections in two different planes making an angle $\theta/2$ is a rotation of angle θ about the line of intersection of the planes. If vectors V_1 and V_2 are unit vectors orthogonal to the planes, then the operation corresponding to the composition of reflections is $W \mapsto V_2V_1WV_1V_2$. By (12.3), we can write $V_2V_1 = -\cos(\theta/2) - V\sin(\theta/2)$, where V is a unit vector in the direction of the rotation axis. In summary, if Q denotes the quaternion $\cos(\theta/2) + V\sin(\theta/2)$, where V is a unit vector, then the transformation $W \mapsto QW\bar{Q}$ represents rotation of a vector W by angle θ about the direction of the vector V.

Quaternionic multiplication gives an easy way to compute the composition of rotations. Namely, we multiply the quaternions that represent the two rotations, and the product is a quaternion representing the composite rotation.

Exercise 12.40. Rotate space by $\pi/2$ radians about the z-axis, then by π radians about the y-axis, and then by $\pi/2$ radians about the x-axis. The composite motion is a rotation by what angle about what axis?

12.4 Literature

- H. S. M. Coxeter, Quaternions and reflections, *American Mathematical Monthly* **53** (1946), 136–146.
- Semyon Grigorevich Gindikin, *Tales of Physicists and Mathematicians*, Birkhäuser, 1988, *Ars Magna*, pages 1–24.
- Sir William Rowan Hamilton, *Elements of Quaternions*, London, Longmans, 1866; third edition reprinted by Chelsea, 1969.
- Tristan Needham, *Visual Complex Analysis*, Oxford University Press, 1997.
- Joseph Rotman, *Journey into Mathematics: An Introduction to Proofs*, Prentice Hall, 1998, Cubics and Quartics, pages 183–203.
- V. S. Varadarajan, *Algebra in Ancient and Modern Times*, American Mathematical Society, 1998.

12.5 Problems

Problem 12.1. Explain the fallacy:

$$-1 = i \times i = \sqrt{-1} \times \sqrt{-1} = \sqrt{(-1)(-1)} = \sqrt{1} = 1.$$

Problem 12.2. Verify that Euler's formula $e^{ix} = \cos(x) + i\sin(x)$ is compatible with the usual power series expansions for the trigonometric and exponential functions.

Problem 12.3. Use Euler's formula to derive

1. the addition formula $\cos(\theta + \varphi) = (\cos\theta)(\cos\varphi) - (\sin\theta)(\sin\varphi)$;
2. the identity $\cos 3\theta = \cos^3\theta - 3(\cos\theta)(\sin^2\theta)$.

Problem 12.4.

1. Find all complex numbers z such that $e^z = 2$.
2. Find all complex numbers z such that $e^z = i$.
3. Find all complex numbers z such that $e^z = 0$.

Problem 12.5. François Viète solved the reduced cubic equation $x^3 - 3ax - 2b = 0$ by making the change of variable $x = w + aw^{-1}$. Show how this method leads to the solution formula (12.1).

Problem 12.6. In the solution formula (12.1) for the reduced cubic equation, there are two different cube roots. Since a cube root has three complex values, why does the formula not produce $3 \times 3 = 9$ different solutions of a cubic equation?

Problem 12.7. Find all four solutions of the equation[5]

$$(x-3)^4 + (x-7)^4 = 24832.$$

Problem 12.8. Find all four solutions of the equation[6]

$$x^4 - 4x = 1.$$

Problem 12.9. Show that quaternions may be represented as 2×2 matrices $\left(\begin{smallmatrix} a+di & -c+bi \\ c+bi & a-di \end{smallmatrix}\right)$ of *complex* numbers.

[5] *Mathematics Student Journal* **28** (1981/4), 3.

[6] Murray Klamkin, *Mathematics Student Journal* **28** (1980/3), 2.

Chapter 13

Projects

13.1 Paradoxes

Research one of the following paradoxes, write a paper about it, and make a presentation in class about it.

You are expected to do more than simply research the topic in the library and on the Internet and report your findings. You should include some original contribution of your own. For example, you might present illustrative examples and your opinion (with explanatory reasons) about a solution of the paradox.

Of course your paper should be computer printed, preferably by LaTeX, the de facto standard for mathematical typesetting.

Please consult your instructor if you have any questions.

Banach-Tarski paradox A ball the size of a pea can be cut into finitely many pieces that can be reassembled into a ball the size of the sun.

Braess's paradox Adding capacity to a network can make it less efficient.

Carl Hempel's paradox of the ravens Every black raven that Edgar Allan Poe observes gives him more confidence in the truth of the statement: "All ravens are black." The contrapositive statement "Everything that is not black is not a raven" is equivalent. Therefore a purple cow is also a confirming instance of the proposition that all ravens are black.

Jacoby's paradox in backgammon Sometimes it can become advantageous for a player to double when the opponent's position improves.

Newcomb's problem Box A has \$1,000 in it; box B has \$1,000,000 or \$0. You may take either box B alone, or you may take both boxes. Box B is empty if and only if a Being with superior predictive powers has guessed that you will take both boxes. What should you do?

The exchange paradox You are offered a choice of one of two identical boxes, and you are given the information that one of the boxes contains twice as much money as the other one. You open your choice and observe how much money it contains. Now you are offered the chance to switch and take the other box. Should you switch?

Argument 1: By symmetry, it makes no difference whether or not you switch. If one box contains Y dollars and the other contains $2Y$ dollars, half the time you will gain Y by switching, and half the time you will lose Y by switching. Your expected gain by switching is zero.

Argument 2: Suppose your box contains X dollars. If you switch, half the time you will end up with $2X$ (a gain of X), and half the time you will end up with $X/2$ (a loss of $X/2$). Your expected gain by switching is therefore $(X - X/2)/2 = X/4$, so you should always switch.

Petersburg paradox A fair coin is flipped repeatedly until heads comes up. If heads comes up for the first time at toss n, you win 2^n dollars. What is a fair price to play the game?

Prisoner's dilemma In a competitive situation where all parties act rationally, they may arrive at an outcome that is inferior for all of them. Compare "the tragedy of the commons."

Surprise examination paradox There will be a surprise examination one day next week. If the examination has not been given by Thursday, then you deduce that it will be on Friday, so it will not be a surprise. Hence the examination cannot be on Friday. By induction, it cannot be on any of the preceding days either.

Nelson Goodman's grue-bleen paradox The adjective "grue" applies to all objects examined prior to the resolution of the Riemann hypothesis just in case they are green and to all other objects just in case they are blue. Confirming instances of the statement "All emeralds are green" are also confirming instances of the statement "All emeralds are grue". Color blindness is not an allowable resolution of the paradox!

> ... like a rudd yellan gruebleen orangeman in his violet indigonation ...
>
> James Joyce
> *Finnegans Wake*
> page 23

The content effect in the Wason selection task Although the following two problems are logically equivalent, the second one is significantly easier to solve. Why?

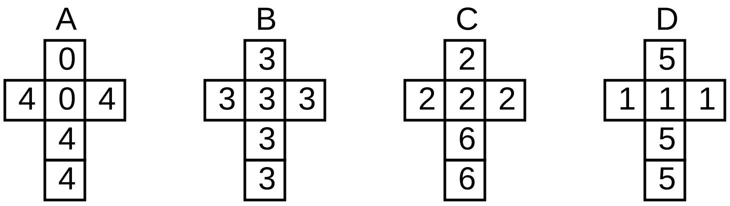
1. Each card has an integer written on one side and a letter written on the other side. To determine the truth or falsity of the statement "If there is a vowel on one side, then there is an even number on the other side", which cards *must* you turn over?

5	8	A	F

2. In a bar, there is a card in front of each customer with the customer's age written on one side and the name of the customer's drink written on the other side. To determine if all customers are drinking legally, which cards *must* you turn over?

25	16	Beer	Coke

The Efron dice Consider the following four "unfolded" dice with sides labelled as indicated.



If two of these dice are rolled in competition with each other, then A beats B two times out of three, B beats C two times out of three, C beats D two times out of three, and D beats A two times out of three.

Zeno's paradoxes These are the grandparents of all paradoxes. One of them says that this class will never end: before the end of class, half the remaining time must elapse; then half the time still remaining must elapse; then half . . . ; and there are infinitely many halves.

> "Was that a paradox?" asked Mr. Erskine. "I did not think so. Perhaps it was. Well, the way of paradoxes is the way of truth. To test Reality we must see it on the tight-rope. When the Verities become acrobats, we can judge them." Oscar Wilde
>
> *The Picture of Dorian Gray*

13.2 Special Functions

Research one of the following special functions, write a paper about it, and prepare a lesson about it that you will present in class. Your lesson should include homework (and solutions).

- Bessel functions
- elliptic functions/integrals
- Gamma function
- Hermite polynomials/functions
- hypergeometric functions
- Laguerre polynomials/functions
- Legendre polynomials/functions
- Riemann zeta function
- Weierstrass $\wp$ function
- Lambert's W function defined by $W(z)e^{W(z)} = z$
- other (please get the instructor's approval)

Some questions you might want to consider are:

- How is the function defined?
- When was it first defined?
- Who first defined it?
- What question or event motivated the inventor to think about this function?
- What other uses does this function have?
- What are some examples that illustrate the importance or application of this function?

These questions are to get you started. You should be creative and not simply do a literature search.

After you write your paper and the instructor reads and returns it, you will teach the rest of the class about your special function using group exercise techniques. You are also responsible for preparing a homework set for the other students to work to solidify their knowledge of your special function.

Appendix A

Sources for projects

In case the students are unable to find satisfactory sources for the projects, the instructor may need to provide hints. Here are some entry points to the literature.

Newcomb's problem One source, with references, is Chapters 13–14 of Martin Gardner's book *Knotted Doughnuts and Other Mathematical Entertainments* (W. H. Freeman, New York, 1986). Chapter 13 is Gardner's original *Scientific American* column, and Chapter 14 is Robert Nozick's follow-up guest column. A bibliography follows Chapter 14.

The exchange paradox A source for references for the exchange paradox is "Elusive optimality in the box paradox" by Nelson M. Blachman and D. Marc Kilgour, *Mathematics Magazine* **74** (2001), no. 3, 171–181.

Surprise examination paradox A source for references about the surprise examination paradox is Chapter 1 of Martin Gardner's book *The Unexpected Hanging* (Simon and Schuster, New York, 1969). Chapter 1, pages 11–23, is titled "The paradox of the unexpected hanging". In the bibliography at the end of the book, there are many additional references to the literature on this paradox.

Another source is T. Chow, "The surprise examination or unexpected hanging paradox", *American Mathematical Monthly* **105** (1998), 41–51; the electronic version available at `http://www-math.mit.edu/~tchow/unexpected.ps.gz` contains an extensive bibliography that was omitted from the published version.

The Efron dice Sources for references about the Efron dice are "Strategies for rolling the Efron dice" by Christopher M. Rump, *Mathematics Magazine* **74** (2001), no. 3, 212–216; "The paradox of nontransitive dice" by Richard P. Savage, Jr., *American Mathematical Monthly* **101** (1994), no. 5, 429–436. The problem has affinities with voting paradoxes.

Appendix B

Lesson Plans

B.1 Fall 1996

Class 1

Plan

Spend about 10 minutes on housekeeping, 80 minutes on logical paradoxes and logical formalism, 10 minutes break, and 80 minutes on induction exercises.

Reality

We spent the whole class on the formalism of logic. The students were comfortable filling out a straightforward truth table, but they had some trouble in translating word problems into mathematical formalism. They were not confident about translating an implication "$A \Rightarrow B$" into a statement using "only if" or "is necessary for."

We held over induction for the second class.

Class 2

Plan

Spend 20 minutes answering questions, 60 minutes on induction, 10 minutes break, 80 minutes on probability, 10 minutes wrap-up.

Reality

We spent half the class working on negating statements containing quantifiers. The students understood the principle perfectly well, and they had no trouble with mathematical statements formulated in symbols with $\exists$ and $\forall$, but working with English sentences was difficult for them. They had to learn that "but" is equivalent to "and" and "any" means "every" (usually).

We spent the second half of the class on induction. The students were confident about routine induction problems. It was not obvious to them where the flaw was in the proof that all horses are the same color.

Class 3

Plan

Spend 40 minutes answering questions on the homework and having the groups work another induction problem. Spend 60 minutes on probability. After a 10 minute break, spend 60 minutes beginning graph theory. The concluding 10 minutes is for wrap-up, assigning homework and reading, etc.

Reality

The induction problem with cases took half the time; the remainder of the time was spent on finite probability. Most of the students were familiar with counting arguments and worked through the exercises on probability with some facility.

Class 4

Plan

Spend 60 minutes discussing previous homework, answering questions, and/or having students present their own solutions. There were three common errors that students made in the previous homework:

- They had trouble negating "there exists a unique x."
- They incorrectly claimed that $n \mid p^n$ implies $n \mid p$ (in trying to prove that $\sqrt[n]{n}$ is irrational when $n > 1$).

- They missed the point in the induction proof that every set of positive integers has a least element: it is not sufficient to prove the statement for finite sets.

There will likely be questions from the new homework on the induction with cases, on the inverse weighted coin problem, and on Eddington's problem.

(This discussion could easily go to 90 minutes.)

Spend 30 minutes introducing graph theory and having the students determine Eulerian paths for examples. After a break, have the students try to discover Fleury's algorithm for constructing Eulerian paths.

If there is a lot of time left, have the students work on determining which maps are two-colorable. Otherwise, have them start on the homework during class.

Reality

Surprisingly, questions took less than an hour. Finding Eulerian paths went smoothly until the students tried to find an algorithm for constructing an Eulerian path in a complete graph on a large odd number of vertices.

After a break, the students tried to find a general algorithm to show the sufficiency of Euler's criterion. Even with hints, they failed. Completing the problem was left for homework.

Class 5

Plan

Spend 45 minutes answering questions on the homework (in particular, on the secretary problem). Have the students work on the two-color problem for 45 minutes. After a 10 minute break, spend 30 minutes on examples and basic results about Hamiltonian graphs. For the remaining 50 minutes, the students will try to prove Dirac's theorem.

Reality

The students quickly decided that two-colorable maps are the ones whose underlying graphs are Eulerian, but they did not succeed in finding a convincing algorithm to color a map. They realized that the problem is simple locally, but they could not make the jump to patch local colorings together to make a global coloring.

Finally, we cut off the discussion and went on to examples of Hamiltonian graphs, which they could do. We left Dirac's theorem as a homework exercise. (The students can look Dirac's theorem up in books if they have trouble with it.)

Class 6

Plan

Answer questions for 20 minutes. Give a quiz individually and in groups (35 minutes). Count vertices, edges, and faces of planar graphs (15 minutes).

Have the students work on Euler's formula for 20 minutes. Then each group will present its induction proof of Euler's formula (20 minutes).

After a 10 minute break, work on consequences of Euler's formula. If there is time left, the students can finish up by finding the duals of the Platonic graphs and their chromatic numbers.

Reality

The student presentations took much longer than anticipated. There were gaps in the proofs that the students had trouble filling.

We skipped the exercise on consequences of Euler's formula. (This material is in the assigned reading anyway.) We covered dual graphs, but did not have time to determine chromatic numbers of the Platonic graphs.

Class 7

Plan

Answer questions for 20 minutes. Have one group determine the number of colors needed to color the faces of the Platonic graphs, and the other group the number of colors for the vertices (15 min). Have each group present the results and check for consistency (10 min). Then have the groups prove the 6-color theorem (40 min).

After a 10 minute break, start number theory by having the groups prove the Fundamental Theorem of Arithmetic (30 min). Discuss algebraic and transcendental numbers (5 min). Have the groups do the warm-up exercises on the number of fingers that Martians have and on base n arithmetic (30 min). Discuss unsolved problems (15 min). Have the groups prove that congruence mod n is an equivalence relation (10 min).

Reality

The discussion of homework took 45 minutes. The coloring of the Platonic graphs took 20 minutes, but errors were found during the discussion that took another 25 minutes to fix (total time on coloring the Platonic graphs was 45 minutes).

After a 10 minute break, the students spent 60 minutes on the 6-color and 5-color problems. One group got the 6-color problem quickly. The other group took longer on the 6-color problem, but solved the 5-color problem faster.

The last 30 minutes were spent on proving the Fundamental Theorem of Arithmetic. Both groups quickly got the existence proof by induction. They then figured out that they needed to use divisibility to prove uniqueness, but they did not finish proving that if $p \mid ab$ for p a prime, then $p \mid a$ or $p \mid b$. They were told to finish the proof for homework.

Class 8

Plan

Discuss homework for 20 minutes. Discuss algebraic and transcendental numbers (5 minutes). Have the groups do the warm-up exercises on the number of fingers that Martians have and on base n arithmetic (30 min). Discuss unsolved problems (15 min). Have the groups prove that congruence $\mod n$ is an equivalence relation (10 min).

After a 10 minute break, have the groups prove that addition and multiplication are well-defined in $\mathbf{Z}_n$ and find the units in $\mathbf{Z}_n$ (20 min). Have the groups construct a perpetual calendar (60 min). Discuss Fermat's Little Theorem and how to use it (10 min).

Reality

There was no discussion of homework. The students said they knew about algebraic and transcendental numbers (5 minutes). The groups did the warm-up exercises on the number of fingers that Martians have and on base n arithmetic (35 min). We discussed unsolved problems (15 min). The groups proved that congruence mod n is an equivalence relation, that addition and multiplication are well-defined in $\mathbf{Z}_n$, and they found the units in $\mathbf{Z}_n$ (35 min).

After a 10 minute break the groups constructed a perpetual calendar (85 min).

Class 9

Plan

Discuss homework 30 minutes (expect discussion on the perpetual calendar problem). Discuss Fermat's Little Theorem and how to use it (15 min). Have the groups find and prove the formula for $\phi(n)$ and use it to compute $\phi(54)$ (50 min).

After a 10 minute break, discuss Euler's generalization of Fermat's Little Theorem and have the groups use it computationally (15 min). Have the groups prove the Chinese Remainder Theorem constructively and then apply it to a specific computation (60 min). If time is still left, start on exact solutions to systems of equations.

Reality

The discussion of homework took 20 minutes. We discussed Fermat's Little Theorem and its use (5 min). The groups found and tried to prove the formula for $\phi(n)$, but they got hung up on the proof that if s and t are relatively prime, then $\phi(st) = \phi(s)\phi(t)$. They could do it for distinct primes. We completed the proof together with one of the students giving an outline that we helped them make exact (80 min).

After a 10 minute break, the groups proved and used the Chinese Remainder Theorem not only on the exercise in the notes, but also on

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 6 \pmod{9} \\ x &\equiv 9 \pmod{25} \end{aligned}$$

(60 min). The last 10 minutes they started on a proof of Euler's generalization of Fermat's Little Theorem using Fermat's Little Theorem and the Chinese Remainder Theorem. They were told to complete the proof for homework.

Class 10

Plan

Discuss homework (20 min). Discuss the reading on exact solutions to systems of equations and have them solve a system using the two variants in the reading (45 min). Have them figure out why the procedure works (25 min).

After a 10 minute break, go on to cryptography. Have them solve two problems on product ciphers (40 minutes) and two on Vigenère ciphers (40 min). If time remains, discuss the idea of public key encryption systems and the problems inherent in them.

Reality

We discussed homework for 10 minutes, and the articles on transcendental numbers for 45 minutes. They solved a system of equations using the two variants in the reading (90 min).

After a 10 minute break, they were shown how to prove Fermat's Little Theorem by induction (5 minutes). They spent the remaining 20 minutes figuring out why the procedure for finding exact solutions works.

Class 11

Plan

Discuss homework (20 min). Have them solve two problems on product ciphers (40 minutes) and two on Vigenère ciphers (40 min). After a 10 minute break, have them work the four problems on RSA codes (70 min).

Reality

They solved the product ciphers problems (10 min) and then the two Vigenère ciphers (25 min). We discussed replacement ciphers, then reset the last class to Thursday, 12 December, 9:00–noon. We proceeded to discuss RSA codes. They found e given n and d (5 min), then did the security problem (20 min). We discussed the square and multiply method by doing an example with $e = 11$, $n = 65$, $M = \mathrm{O} = 15$ (the answer is 20) (15 min). They then did the decode problem (20 min).

After a 10 minute break, they did the problem on the Evil Empire (15 min), and then proved that the distance function is a metric, spending most of the time on the triangle inequality (35 min). We concluded by my showing them how to prove their conjecture on the Fractal Pascal's Triangle.

Class 12

Plan

Discuss homework 10 minutes. Do the remaining 3 problems on error correcting codes (80 min). After a 10 minute break, spend the rest of the time solving the problem of winning at Nim.

Reality

They solved the problem of distance and error-correcting properties (15 min) and worked a long example on the standard array (70 min). After a 10 minute break, we spent the rest of the class on Nim. One group did the greedy game (take the last m&m), and the other group did the dieter's game (leave the last m&m).

Class 13

Plan

Review the fundamental concepts of game theory, work a matrix game, the Monty Hall problem, and a two-person non-zero-sum game.

Reality

The class went more or less according to plan.

Class 14

Plan

Spend the first half of the class working a three-person zero-sum game. After a break, do as much set theory as time permits. There is no homework on set theory, as the last class will be devoted to student presentations.

Reality

About 30 minutes was spent discussing previous homework. The three-person game took somewhat more than an hour. Working an example of an axiomatic system took most of the remaining time because the students had troubling deciding the truth or falsity of universal and existential statements quantified over the empty set.

Class 15

At the final class, the students gave oral presentations of their projects in lieu of a final examination.

B.2 Spring 1997

Class 1

Plan

Spend 75 minutes on intuitive limits, 10 minutes break, and the remaining time on continued fractions. If time permits, start on p-adic numbers.

Reality

Intuitive limits took up the whole class. It took the students quite a while to make an appropriate Riemann sum appear, and they spent over an hour on the snowflake problem without completely resolving it.

Class 2

Plan

Spend the first half on continued fractions and the second half on p-adic numbers.

Reality

Continued fractions took the whole class. The students needed some prompting to nail down the (almost) uniqueness of continued fraction expansions.

Class 3

Plan

Do the section on p-adic numbers. Start the unit on functions if there is time.

Reality

We almost finished the unit on p-adic numbers, the long division problem being left for homework.

Class 4

Plan

Start the unit on functions. If time permits, begin the application on Mercator's map.

Reality

We did not get to the application on Mercator's map.

There was some discussion of what a function is. A student suggested that Dirichlet's function, which equals 1 on the rationals and 0 on the irrationals, is not given by a "formula," so we spent a few minutes on $\lim_{m\to\infty} \lim_{n\to\infty} \cos(m!\,\pi x)^n$.

It took the students quite a while to prove that the exponential function is transcendental; they started by claiming it was "obvious," but the obvious reasons were not readily forthcoming.

It was interesting to note that the students did not all have at their fingertips the power series and differential equations for the sine and cosine, although the groups quickly got these by taking the union of their individual knowledge. On the other hand, it appeared that none of the students had a conscious memory of having seen the geometric proof that $\lim_{x\to 0} \dfrac{\sin x}{x} = 1$.

Class 5

Plan

Spend 30 minutes discussing previous homework. Spend 50 minutes on hyperbolic functions. After a 10 minute break, spend the remaining 90 minutes on the Mercator map.

If time permits, begin the chapter on plane geometry.

Reality

Surprisingly, the students had trouble finding an appropriate picture to go with the hyperbolic functions; or they were not confident that they had a valid picture after drawing it.

We ended up with less than an hour to spend on the Mercator map, and so did not finish it.

Class 6

Finishing the Mercator map took nearly two hours. We then started the geometry unit, leaving two of the exercises for homework.

Class 7

We spent the whole class on conics. The students did not have in their conscious memory that the discriminant tells the flavor of the conic section.

Class 8

Plan

Work on cubic curves for the first half of class; then go on to non-Euclidean geometry.

Class 9

We finished non-Euclidean geometry in the first half of class. In the second half, we discussed different definitions and realizations of the complex numbers, similarities and differences between the real numbers and the complex numbers, and a proof of the fundamental theorem of algebra.

Class 10

Two students presented their projects on functions: Bessel functions and elliptic functions.

Class 11

Two students presented their projects on functions: the Gamma function and the Riemann zeta function.

Class 12

Two students presented their projects on functions: Hermite polynomials and Legendre polynomials.

Class 13

For one hour of the class, the students attended a meeting of the Geometry, Analysis, and Topology seminar, where one of the instructors spoke on "The football player and the infinite series." For the remaining two hours of the class, one of the students presented a project on hypergeometric functions.

Class 14

The students worked on a handout on proving various theorems about factoring polynomials. Also, they completed the course evaluation forms.

B.3 Fall 1997

Class 1

Plan

Spend about 15 minutes on housekeeping, 80 minutes on logical paradoxes, 10 minutes break, and 80 minutes on logical formalisms. Start induction if time permits.

Reality

Spent 20 minutes on housekeeping, 80 minutes on logical paradoxes, 10 minutes on break, 30 minutes on formalism (truth tables, Alice, ...) and 40 minutes on negation. Assignment: Read #1,2,4,5. Do Alice #17-25, Negations #7-8, Problems 1.1-1.2. Also decide on which paradox to investigate.

Class 2

Plan

Spend 20 minutes answering questions, 70 minutes on induction, 10 minutes break, 20 minutes more on induction, then 50 minutes on probability, 10 minutes wrap-up.

Reality

Went over homework 10 minutes, induction the rest of the time but did not get to last exercise. Homework: Read Bottle Imp and Chance and Chanceability. Do Exercises 1.13 and Problems 1.3, 1.4.

Class 3

Plan

Spend 40 minutes going over mistakes on 1st homework (Alice #21, 24), answering questions on the homework and maybe having the groups work another induction problem. Spend 60 minutes on probability. After a 10 minute break, spend 60 minutes beginning graph theory. The concluding 10 minutes is for wrap-up, assigning homework and reading, etc.

Reality

Answered questions on homework for 45 min, then gave them

Prove by induction: for all $n \in \mathbf{Z}^+$

$$(\frac{2n-1}{e})^{\frac{2n-1}{2}} < 1 \cdot 3 \cdot 5 \cdot \cdots \cdot 2n-1 < (\frac{2n+1}{e})^{\frac{2n+1}{2}}$$

65 minutes were spent on probability (Ex. 2.5 was not done), 10 minute break, then 60 minutes on graph theory. Since they had not had reading on graph theory it was necessary to give them some basic definitions before they started working. They finished Ex. 3.2. Homework: Read 3.2 #1,2,3,9. Do Exercise 2.5, Problems 2.1, 2.2, 2.3, 3.1.

Class 4

Plan

Spend 45 minutes going over the pieces of 1.3, 1.4 that they missed and answering questions on the homework. It may well take longer than 45 minutes, especially with Eddington's problem and the secretary problem. Have the students work on the two-color problem for 45 minutes. After a 10 minute break, spend 30 minutes on examples and basic results about Hamiltonian graphs. For the remaining 50 minutes, the students will try to prove Dirac's theorem.

Reality

Going over homework took 70 minutes. They asked good questions such as why do we assume the statement A affirms ... in Eddington's question is true, and what about other strategies for the secretary's problem. 2-coloring a map took 60 minutes (with a 10 minute break put in after 20 minutes). They took the first 20 minutes to conclude that Eulerian was the condition. After break they quickly got 2-colorable implies Eulerian, but took a lot of time going down dead ends before getting Eulerian implies 2-colorable (I gave them a hint). Finding Hamiltonian circuits (ex. 3.4-3.6) took 10 minutes. The remaining 20 minutes were spent working on Dirac's Theorem. We finished with me answering questions on the hint to Dirac's Theorem and telling them to finish the exercise for homework. Homework: Read #4,5,6. Do Exercise 3.7, Problems 3.2-3.6.

Class 5

Plan

Answer questions for 40 minutes. Count vertices, edges, and faces of planar graphs (15 minutes). Have the students work on Euler's formula for 20 minutes. Then each group will present its induction proof of Euler's formula (30 minutes). After a 10 minute break, work on consequences of Euler's formula. If there is time left, the students can finish up by finding the duals of the Platonic graphs and their chromatic numbers.

Reality

Went over Dirac's theorem, $G \cong L(G) \iff G \cong C_n$, and the climber's dilemma when plateaus are added (they got this fast) - 30 min. 3.8 took 15 min. 3.9 took them 10 minutes to do (they remembered the induction on vertices from the reading) with needing 30 minutes for the presentation - discussed induction some more as to why one starts with the $k+1$st case and uses the info from the kth case rather than build up to $k+1$ form k. 7 minute break. The consequences of Euler's theorem (3.10 1-3) took a total of 78 minutes because they had trouble proving that $3f < 2e$. The last 10 minutes were spent discussing what a dual graph is, how to find it, and their finding the duals of the platonic solids. Homework: read #7,8; do problems 3.7-3.10.

Class 6

Plan

Answer questions for 30 minutes, including going over the proof of Turán's theorem (Problem 3.7). Have one group determine the number of colors needed to color the faces of the Platonic graphs, and the other group the number of colors for the vertices (20 min). Have each group present the results and check for consistency (20 min). Then have the groups prove the 6-color and 5-color theorems (60 min).

After a 10 minute break, start number theory by having the groups prove the Fundamental Theorem of Arithmetic (35 min). Discuss algebraic and transcendental numbers (5 min). If time permits, have the groups do the warm-up exercises on the number of fingers that Martians have and on base n arithmetic.

Reality

Went over Turán's theorem and answered questions for 30 minutes. Both groups colored both faces and vertices of Platonic graphs and did so correctly along with observing the dual properties - 30 minutes. One group got the 6 color theorem in 10 minutes, other in 25 (while first started 5 color theorem). After a 10 minute break they went back to the 5 color theorem for 50 minutes. I had to remind them about Kempe chains. I also showed them how to use the fact that K_5 is not planar in a proof that does not use Kempe chains.

They proved the Fundamental Theorem of Arithmetic (30 minute), quickly realizing that they needed the lemma that, if p is a prime and p divides ab then p divides a or p divides b. Both groups got the lemma after I suggested they look at Problem 4.1 to remind themselves about some number theory definitions. The last 5 minutes were spent discussing algebraic and transcendental numbers. Homework: Read 4.1-3. Do Problems 4.1-8.

Class 7

Plan

Discuss homework and readings for 20 minutes. Have the groups do the warm-up exercises on the number of fingers that Martians have and on base n arithmetic (30 min). Discuss unsolved problems (15 min). Have the groups prove that congruence $\mod n$ is an equivalence relation (10 min), then prove that addition and multiplication are well-defined in $\mathbf{Z}_n$ and find the units in $\mathbf{Z}_n$ (20 min).

After a 10 minute break, have the groups construct a perpetual calendar (75 min). If time permits discuss Fermat's Little Theorem and how to use it.

Reality

We discussed the homework for 15 minutes. The warmups took 25 minutes. We discussed unsolved problems for 10 minutes. The basics of $\mod n$ arithmetic took 25 minutes. After a 15 minute break, they spent the rest of the time (90 minutes) working on the perpetual calendar. One group finally got a correct formula for d_n but the other needed to be shown. Homework: Complete the perpetual calendar, reporting $f(m)$ and the final reduced formula for d and use same to compute the day of the week on which they were born. Read 4.4-9. Do problems 4.9-13.

Class 8

Plan

Discuss homework 30 minutes (expect discussion on the perpetual calendar problem). Discuss Fermat's Little Theorem and how to use it (15 min). Have the groups find and prove the formula for $\phi(n)$ and use it to compute $\phi(54)$ (60 min).

After a 10 minute break, discuss Euler's generalization of Fermat's Little Theorem and have the groups use it computationally (15 min). Have the groups prove the Chinese Remainder Theorem constructively and then apply it to a specific computation (50 min). If time permits, solve

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 6 \pmod{9} \\ x &\equiv 9 \pmod{25}. \end{aligned}$$

If still time have them prove Euler's generalization of Fermat's Little Theorem using Fermat's Little Theorem and the Chinese Remainder Theorem.

Reality

There was a long discussion of the Pascal triangle problem during which two different proofs that the 2^nth row was all black were presented by two students. After that I discussed why that was only one direction and showed them a proof that that not only showed that the 2^nth row was all black but those were the only all black rows. We also discussed Cantor's proofs, so we spent 55 minutes going over the homework. Proving Fermat's Little Theorem and using it took 20 minutes. They then started to work on Euler's ϕ function. Finding the formula for the power of a prime was done quickly by both groups and proved quickly by one and after 10 minutes by the other. The rest of the time was spent on proving $\phi(st) = \phi(s)\phi(t)$ when s, t are relatively prime. Those 90 minutes included a break of 10 minutes. Even with the hint of making a matrix whose ijth entry is $i + (j-1)s$ did not help them enough to complete the proof. We finished the proof together. Homework: Read 4.10, 4.11 and 5.1. Do Problem 4.14. Work on paper.

Class 9

Plan

Discuss homework problem if necessary (unlikely) but reserve discussion of reading - 5 minutes. Have the groups prove Euler's generalization of Fermat's Little Theorem by induction and have use it computationally (20 min). Have the groups prove the Chinese Remainder Theorem constructively and then apply it to the problem in the course book, then to

$$
\begin{aligned}
x &\equiv 3 \pmod 4\\
x &\equiv 6 \pmod 9\\
x &\equiv 9 \pmod{25}.
\end{aligned}
$$

(60 min) Then have them prove Euler's generalization of Fermat's Little Theorem using Fermat's Little Theorem and the Chinese Remainder Theorem (one group says they have done so already, so perhaps just have them present it to the other group) (15 min).

After a 10 minute break, discuss the reading on exact solutions to systems of equations and have them solve a system using the two variants in the reading (60 min). Have them figure out why the procedure works (25 min). If time permits, have them work on product ciphers.

Reality

Discussed alternate proof of FLT for 15 minutes. No questions on homework. Euler's generalization of FLT took 75 minutes. 15 minute break. One group spent 45 minutes, other 65 on the Chinese Remainder Theorem. The first group proved Euler's generalization using FLT and CRT during the 45 min, so spent the rest of class on exact solutions, finishing the computations using a prime. The second group started the exact solutions but will turn in both parts of ex 4.14 for homework. Homework: Read 5.2, 5.3, 5.4 pages.1-5; do Ex 4.14 (one part or both parts as is appropriate) and Problem 4.15; finish rough draft of project.

Class 10

Plan

Go over homework (exact solutions) (30 minutes). Have them figure out why the procedure for exact solutions works (30 minutes). Have them solve two problems on product ciphers (20 minutes). After a 10 minute break, have them solve the two problems on Vigenère ciphers (30 min), then have them work the four problems on RSA codes (60 min). Of time permits, have them prove the distance function problem in error-correcting codes.

Reality

Almost no questions on homework so took only 5 minutes. They spent 55 minutes figuring out why the procedure worked in the case of a prime, then another 15 to see what was going on with the CRT. Product ciphers took 15 minutes and were followed by a 10 minute break. Vigenère took one group 20 minutes and the other 25. The first group went on to RSA codes and spent 20 minutes (other group 15) on 5.3 and 5.4. We then spent 15 minutes in which I gave a flow chart for the square and multiply method of exponentiation and we did an example together. They then did 5.5 in 10 minutes by having one member of the group do one letter and putting them together. After they did 5.6 in in about 10 minutes, I used the rest of the time to give an overview of error-correcting codes, emphasizing those parts of linear algebra that they would need to know. Homework: Read and study 5.4. Do problems 5.1-5.3.

Class 11

Plan

Go over homework (10 minutes). Exercises 5.7-5.10 on error-correcting codes should take about 90 min. After a 10 minute break, spend the rest of the time solving the problem of winning at Nim - have one group do the greedy game and the other the dieting game.

Reality

We discussed various parts of TEX for the paper as well as how and when to use references in the paper plus how to put a reference style at the end of the paper. I then showed them how to work an affine transfer system when the matrix is singular (as happened in problem 1). So over homework took 35 minutes. Ex 5.7 took 25 minutes as did 5.8. After a 10 minute break they spent 70 minutes on 5.9 and 15 on 5.10. They needed to have cosets explained to them as well as standard arrays. They did not understand the connection between syndromes and coset leaders. Homework: Read handout on algebra for constructibility and do problems 5.4-5.11.

Class 12

Plan

Over homework (30 min). Solve the problem of winning at Nim with one group doing the greedy game and the other the diet game (60 min). After a 10 minute break, have them learn about what is constructible (Exercises 6.3.1-3) up to the point of needing algebra. Start algebra if time permits.

Reality

We spent only 5 minutes on homework because they want to wait until next week to discuss the error-correcting code homework. They spent 85 minutes finding a winning strategy for Nim, one group doing the greedy game, the other the dieter's game. They needed to be told to look at the numbers in binary. After a 10 minute break they did 6.1 (30 minutes), 6.2 (20 minutes), and 6.3 (30 minutes). Homework: Papers due. For those who did not read the handout on algebra for constructibility, they must do so in order to be able to do the work next week.

Class 13

Plan

Over error-correcting code homework and show how to construct a square root in an easier fashion (45 minutes). Continue with 6.4 - 6.7 and further if time permits.

Reality

Over error-correcting code homework and show how to construct a square root in an easier fashion (35 minutes). 6.4: one group 35 min, other 40. 6.5: one group 10 minutes, other 15. 6.6: both groups 10 min. 6.7: one group 5 minutes, other 10. break: one group 25 min, other 10. 6.8: one group got in 15 min and then took 15 min to do presentation to other group (who was close to a solution when we started the presentation). 6.9: 5 minutes of discussion, then both groups took 25 minutes to complete. Homework: Read on Factoring. Do 6.1-6.3.

Class 14

Plan

Over homework and discuss term papers(10 minutes). Set up for last class (10 minutes). Do 6.10 (5 minutes) and 6.11 (60 minutes). After a 10 minute break, introduce axiomatic systems and have them do the first exercise. If time permits have them do problems 6.4-6.10.

Reality

Going over homework, discussing term papers, and setting up for the last class took 20 minutes. 6.10 took 5 minutes. 6.11 took one group 35 minutes and the other 50, but when I then asked them to look at the homework problems and determine which followed from 6.11 and why, the first group took 25 and the second 10, finishing at the same time. After a 20 minute break, during which I discussed some points on the term papers individually, we discussed course evaluations and the pros and cons of scantron versus essay types for 20 minutes. We discussed axiomatic systems, models, consistency and independence, then they did 8.1, all in 20 minutes. We then spent 25 minutes on Cantor's diagonal proof and Gödel's incompleteness theorems. They spent the last 15 minutes working on the homework. Homework: fill in the course evaluation and do problems 6.4, 6.5, either 6.8 or 6.10, and 6.11.

Class 15

At the final class, I discussed some problems they had had with the homework. Then the students gave oral presentations of their projects in lieu of a final examination. We did all this at the home of one of the students at which we ate dinner to which all contributed. Harold Boas joined us for this class to ease the transfer to him next semester.

B.4 Spring 1998

The idea of this course being to foster understanding, rather than to cover a specific body of material, the instructor did not formulate detailed lesson plans. What follows is a record of what actually took place in class.

Class 1

General housekeeping chores and the section on intuitive limits took up the whole period. The students had to ask for a hint about computing the limit $\lim_{n\to\infty} \sum_{k=1}^{n} \frac{n}{n^2+k^2}$, but they could do it after getting the idea to use Riemann sums. The snowflake curve interests them, but they find the analysis slow going.

Class 2

More than half the time was spent discussing the previous homework. Only one of the students had a reasonably complete proof that $\sin n$ fails to approach a limit, although the others had an intuitive understanding. None of the students had nailed down the convergence of towers of exponents, so we worked on that. Then we discussed the notion of arc length, what it means for curves to converge, the question of when the limit of the lengths is the length of the limit, and why the way in which the sawtooth curves approach a line segment is different from the way in which the iterates of the snowflake construction approach their limit. The students had not fully explained the existence of subsequential limits for the function $\cos\left(\frac{1}{x} \cdot \tan^{-1}\left(\frac{1}{x}\right)\right)$, so we looked at that. One of the students presented a solution to the problem about rearrangements of the alternating harmonic series.

After a break, we had a little over an hour left. The students were able to get most of the way through the section on continued fractions.

Class 3

After a brief discussion of previous homework, the students worked on a task that was not previously in the guide: namely, to guess a recursive formula for the numerator and denominator of the approximants of a continued fraction, and to use induction to prove the formula. This activity took up half the class period.

After a break, the students began the section on p-adic numbers.

Class 4

We discussed the problem about the density of the values $\sin(n)$ for about 45 minutes. The students had various ideas about attacking the problem, but they had not succeeded in finding a complete solution.

Then we continued the section on p-adic numbers. Determining the cases of equality in the strong triangle inequality took the students a surprisingly long time. It seems that they are not experienced in dividing problems into cases efficiently.

Finishing the last problem in the section was assigned as part of the homework.

Class 5

After some discussion of the homework, the students presented what they had understood from the difficult reading about construction of p-adic series with special convergence properties. The reading was somewhat beyond their capabilities. They could follow some of the details, but they missed the big picture.

In the second part of the class, we began the unit on functions.

Class 6

In the first part of the class, we worked on something that had not been in the handout. We split into three subgroups. One subgroup revisited the homework problem on dividing p-adic series and uncovered the problem of division of fractions that underlies it. Another subgroup found an induction proof of Alhazen's formula discussed in one of the distributed readings:

$$(n+1)\sum_{i=1}^{n} i^k = \sum_{i=1}^{n} i^{k+1} + \sum_{p=1}^{n}\left(\sum_{i=1}^{p} i^k\right).$$

The third subgroup deduced from Alhazen's formula the closed form expressions for $\sum_{i=1}^{n} i^k$ for $k = 1$, 2, 3, and 4. Then the original groups reassembled, and the members explained to each other what the subgroups had worked out.

In the second part of the class, we continued with the unit on functions. The students ran out of steam when they tried to find a geometric proof of the addition formula for the sine function.

Class 7

We finished the material on exponential, logarithmic, and hyperbolic functions, and began working on loxodromic distance.

Class 8

Two hours were spent finishing the unit on functions. Experience shows that the students take a long time to work out the details of the Mercator map and the computation of loxodromic distance. After a break, the students started on the geometry unit.

Class 9

After returning from Spring Break, we began with a couple of warm-up problems. One was a review problem about measuring distance on the surface of Mars. (This problem has since been incorporated into the notes.)

The second was the problem of showing that for a finite collection of points in the plane, not all on a single line, there must be some pair of the points such that the line through them misses all the other points. Proof: from all pairs (ℓ, p), where ℓ is a line through two of the points and p is one of the points not on ℓ, select the pair such that the distance from p to ℓ is minimal. Then ℓ is a line of the required type. This is the Gallai-Sylvester theorem. For discussion, see Béla Bollobás, To prove and conjecture: Paul Erdős and his mathematics, *American Mathematical Monthly* **105** (1998), number 3, 209–237.

We then continued with the unit on plane geometry and finished the classification of conic sections.

Class 10

We mostly finished the section on plane curves. Some of the verifications concerning the group law on a cubic curve were left for homework.

Class 11

We began the section on non-Euclidean geometry.

Class 12

Student presentations on the Γ function and on Legendre polynomials.

Class 13

Student presentations on Laguerre polynomials and on the Riemann ζ function.

Class 14

Student presentations on Bessel functions and on hypergeometric functions.

Class 15

We met at the instructor's home for dinner and then did a test run of the newly revised and expanded unit "Beyond the real numbers".

B.5 Lesson Plans, Fall 1998

Class 1

Plan

Spend about 15 minutes on housekeeping, 80 minutes on logical paradoxes, 10 minutes break, and 80 minutes on logical formalisms. Start induction if time permits.

Reality

Spent 15 minutes on housekeeping, 30 minutes on warm up and logical paradoxes, 20 minutes on formalism (truth tables, 1.2, 1.4), 40 minutes on Alice with a 10 minute break after 25 minutes, 50 minutes on negation, and 15 minutes reading the play on logic and induction. Assignment: Read #1,2,4,5. Do Alice #17-25, Negations #7-8, Problems 1.1-1.2. Also decide on which Paradox to investigate.

Class 2

Plan

Spend 20 minutes answering questions, 70 minutes on induction, 10 minutes break, 20 minutes more on induction, then 50 minutes on probability, 10 minutes wrap-up.

Reality

Spent 10 minutes discussing homework and readings, then 15 on 1.9 and introduction to induction, 75 on 1.10-1.12, 10 on a break, 20 on 1.13-1.14, 25 on 1.15, 5 on 2.1-2, 5 on 2.3 and 10 on 2.4. We will start with 2.4 next time. Wrap up took 5 minutes. Assignment: Read *The Bottle Imp* and the reading of Chapter 2. Do Problems 1.3-1.5.

Class 3

Plan

Spend 30 minutes going over homework being returned, esp. negations, and questions on homework collected. Spend 45 minutes finishing the chapter on Probability. Distribute and have them read *The Lottery.* After a 10 minute break, discuss the probability issues raised in the short story. Use remaining time to start Graph Theory.

Reality

Spent 20 minutes going over the homework that was returned and discussing the reading, esp. *The Bottle Imp.* Spent 55 minutes on the rest of the probability chapter, then 15 minutes reading *The Lottery.* After a 10 minute break we spent 30 minutes discussing the whether the man who was at his 77th lottery was there because his name started with W – i.e., was it really equally likely. The rest of the time was spent on introducing graph theory and them working exercises 3.1-3.3. Homework: Read: numbers 6-9 in the reading book (3.2 #1-3,9). Do problems 2.1-2.3, 3.1.

Class 4

Plan

Go over homework for about 50 minutes (expect questions on Eddington and secretary problem). Have them do the exercises 3.4-3.7 in the section on Hamiltonian graphs. If time permits start work on Euler's formula.

Reality

We discussed the induction of 1.3 but there were no questions on the homework. They did exercises 3.4-3.9 and were working on 3.10 when class ended. Homework: Read numbers 10-14 (rest of reading for Chapter 3). Do problems 3.2-3.6.

Class 5

Plan

Spend 1 hour going over 2.1 part 3, Eddington's problem and the Secretary problem. Have them complete the work in Chapter 3 including proving the five color theorem.

Reality

Spent 1 hour going over 2.1 part 3, Eddington's problem and the Secretary problem. They completed the work in Chapter 3 including proving the five color theorem, then proved the existence part of the Fundamental Theorem of Arithmetic. Homework: Read 14a-17. Do Problems 3.7-3.10, 4.1- 4.6.

Class 6

Plan

Have them redo 3.2, 3.3, 3.4 part 3 - probably take 1 1/2 hours. Then back to number theory through unsolved problems.

Reality

Spent 1 1/2 hours having them redo 3.2 and 3.3, present same, then showed them 3.4 part 3. After a 10 minute break, I showed them the following proof in order to get the idea of using well-ordering into their heads:

Explain the following proof of the irrationality of the square root of 2.

If $\sqrt{2}$ were rational, then there would be a smallest positive integer n such that $n\sqrt{2}$ is an integer; but $n\sqrt{2} - n$ is a smaller such integer.

Then they finished the proof of 4.1, I showed them an alternate for the uniqueness:

Suppose $N = p_1...p_r = q_1...q_s$ is the smallest positive integer with two different factorizations. Then no p_i equals any q_j. WLOG, suppose $p_1 < q_1$. Let $N' = (q_1 - p_1)q_2...q_s$. Factor $q_1 - p_1$ into primes to turn this into a prime factorization of N' not including the factor p_1 (p_1 does not divide $q_1 - p_1$ since p_1 does not divide q_1). However, writing $N' = p_1(p_2...p_r - q_2...q_s)$ leads to a prime factorization containing p_1. This contradicts the minimality of N, since $0 < N' < N$.

We discussed algebraic and transcendental; they did 4.2, 4.3, then we discussed unsolved problems. Homework: Read 18-22. Do problems 4.7-12. Work on paper.

Class 7

Plan

Go over homework and reading - expect discussion on the proof that e and π are irrational/transcendental. Do basics on congruences, then go on to the perpetual calendar. If time permits discuss Fermat's Little Theorem and how to use it.

Reality

Amazingly they understood the basics of the proof of irrationality but were confused by the article on Cantor. So we went over the diagonal proof and how it connected to irrational/transcendental. They were happy campers after 15 minutes. They quickly did the basics on congruences, but spent the rest of the period on the perpetual calendar. Homework: Read 23-25. Do 4.13-14.

Work on paper. We also rescheduled 24 November (bonfire night) for 9-12 20 November but with the paper still due (but in my mailbox) on 24 November.

Class 8

Plan

Over homework (show them easier ways of doing what they did correctly) and answer questions on the perpetual calendar and readings. Have them do the exercises on Fermat's Little Theorem, Euler's ϕ function, and Euler's generaliztion of FLT. If time permits, have them do the Chinese Remainder Theorem.

Reality

We went over homework and looked at the distribution of their birthdays (4 on Thursday!) and discussed drawing conclusions from small samples. They spent the rest of the period on Fermat's Little Theorem Euler's ϕ function, and Euler's generalization of FLT. Homework: Reread 25. Read 26. Do problem 4.15. Work on paper.

Class 9

Plan

Go over homework. Have the do the exercises on the Chinese Remainder Theorem, and exact solutions. Start codes if time permits.

Reality

We went over the homework and they did the exercises on the Chinese Remainder Theorem and exact solutions, then figured out why the exact solution algorithm works. Homework: Read 27,28. Do problem 4.16. Rough draft of paper is due.

Class 10

Plan

Go over questions (if any) on the exact solutions. Do exercises on cryptography. Start error-correcting codes if time permits.

Reality

There were no questions on exact solutions. I spoke for about 10 minutes on the differences between error-correcting codes and cryptography and talked about the history of error-correcting codes. They spent about 2 hours (including break) on the cryptography exercises, then played Nim and devised strategies. Homework: read 29, 30, and section 1 of 31. Do problems 5.1, 5.2, 5.3.

Class 11

Plan

Go over general items on the rough drafts (everyone got the exact solution homework correct). Have them do the exercises on error-correcting codes. Start the chapter on constructibility if time permits.

Reality

I discussed general problems with the rough drafts and encouraged them to do a good job. They then did the exercises on error-correcting codes, needing me to show them what was meant by a standard array (I worked a small example). The last 5 minutes were spent tying up loose ends on Nim. Homework: Read #31. Do problems 5.4-5.11.

Class 12

Plan

Go over questions on homework. Do as much of chapter 6 as time permits. I estimate that they will do 6.1-6.8.

Reality

The students said that they had a lot of trouble with some of the problems but wanted me to look at their work before we discussed them or I gave them hints to finish them. The class was interrupted by a fire alarm at 7:30 so we lost 30 minutes. The rest of the class was spent on chapter 6. They did 6.1-6.5. Homework: Read #32. Do problems 6.1-6.3. These may be turned in Friday (bonfire night moved) or after Thanksgiving.

Class 13

Plan

Over the error-correcting code homework. Continue on chapter 6, possibly completing it.

Reality

Went over the problems on error-correcting they did not all get. The main problem seemed to be that they read more into the problems than was in the statement of the problem. They then did the rest of chapter 6. Homework: Read the articles on graph theory. Do problems 6.4-6.11. I reminded them that their term papers are due by 4pm Tuesday, 24 November.

Class 14

Plan

Do the exercise on building models to show consistency, independence, etc from Chapter 8, then do as much of Chapter 7 as possible in the time allotted.

Reality

Class 15

Plan

Have the class to dinner at my house and then have them make their presentations.

Reality

They came out to my house early, helped with the rest of the dinner preparations, then stayed late. After each presentation there was lively discussion not only on that presentation but on how that paradox fit with all the others. There were some excellent insights into how the paradoxes were the same.

B.6 Spring 1999

The idea of this course being to foster understanding, rather than to cover a specific body of material, the instructor did not formulate detailed lesson plans. What follows is a record of what actually took place in class.

Class 1

Housekeeping chores took 1/2 hour because we had two new students this semester (and 6 returning). They took 1 hour to do exercises 9.1-9.4 and had no trouble recognizing the Riemann sum. After a 10 minute break, they worked on the snow flake problem. One group got it in 30 minutes, the other said they had it in 40. Since the answers didn't match, we spent 10 minutes with the two groups checking what they did with each other until they arrived at a common (and correct) answer. They then spent 15 minutes doing 9.6-9.8 and started 9.9 in the remaining 15 minutes. The homework is to read # 1 and 4, finish exercise 9.9, and do problems 9.1-9.4, 9.6-9.7. I also asked them to look at 9.5 and tell me whether they preferred 9.2 or 9.5 since they are so similar.

Class 2

The students needed more time to do problems 9.3, 9.4 iii, and 9.7 which I agreed to. I asked them what they did with exercise 9.9 and they replied that the representation was unique. Since it is not, I gave them a counterexample and asked them to check the counterexample to see that I was right, then to find the error in their proofs and correct them. This took 45 minutes. They then took 50 minutes to do exercise 9.10, after which we had a 10 minute break. I then posed the following problem which I got off of the lessonplans from 98a.

Suppose one has a continued fraction $[a_1, a_2, \ldots]$. Let $s_n/t_n = x_n = [a_1, \ldots, a_n]$ be the nth approximant. Guess a recursive formula for s_n and for t_n, then prove the formulas using induction.

They did well finding the recursive formula but needed help developing notation for it. They had trouble with the induction proof until I suggested a change of variables in the approximant of $b_i = a_{n-i+1}$. We had a discussion of functional notation and how it affects (or not) induction. This problem took up the rest of the period. Assignment: Problems 9.3, 9.4 iii, 9.7, 9.8, 9.9.

Class 3

Since the students did not correctly solve some of the homework, I explained why what they did was incomplete or wrong and had them rework some of the problems. It took 90 minutes to redo problem 9.1 and to briefly discuss problems 9.3 and 9.7. After a 10 minute break, they took an hour to redo problem 9.2. I made a few comments on problems 9.4 and 9.8. They then did exercise 9.11 in ten minutes and worked on exercise 9.12 for the rest of the time, completing part 1 but misreading part 2. Homework: Exercise 9.12 parts 2 and 3, Problems 9.9, 9.10 for both of which I gave some hints as they had no clue how to do 9.9 (why it was held for a second week). Note that I graded their homework during the time they worked on problems 9.1 and 9.2. They really liked getting the homework back that night.

Class 4

We spent 55 minutes discussing a proof that the even and odd truncations converge to the same limit in problem 9.9. They then did exercise 9.13 quickly but took 40 minutes to do 9.14. There was a 10 minute break after 20 minutes of work on 9.14. It took them 10 minutes to do 9.15 and 9.16 but they then got hung up on 9.17 briefly because I insisted that they prove that the series converged to the limit they found. They did 9.18 i quickly but then stalled on 9.18 ii. We discussed again what convergence of a series meant. Some of them were confused about when to take the norm. Homework: Complete exercise 9.18 ii. Do problems 9.11 and 9.12. Reread reading #1.

Class 5

They understood the reading on p-adic series much better the second time but indicated they did not understand all of the steps of the proof. They did understand what was proved and how amazing it was. We discussed this for 10 minutes. They then took 35 minutes to do exercise 9.19 as it took a while to get the borrowing done correctly. They did 10.1 and 10.2 quickly and then we discussed them (20 minutes total), after which 10.3 took 5 minutes and 10.4, 25 minutes. They needed a hint to divide by e^{nx}. After a 10 minute break they spent the rest of the time working on 10.5, getting the first 4 parts easily, but having trouble with the geometric proofs of limits. They did not get to the geometric proof of the addtion formula for $\sin x$. Homework: Complete exercise 10.5. Read #2, 3. Do problems 9.13 and 10.1. I reminded them that the rough draft of their papers are due next week.

Class 6

Going over the homework took 10 minutes. They then did 10.6 in 60 minutes, 10.7 in 80 minutes (plus a 10 mintue break during it), then 10.8 and 10.9 in 10 minutes each. Homework: Read #5, 6, 7, 8. Do problems 10.2-10.5.

Class 7

We discussed the papers, presentations, and scheduling of same for 20 minutes at which time we had assigned everyone a day upon which to present and made the papers due by the class on 23 March. 10.10 took them 65 minutes. After a 10 minute break we went over problem 10.5 for fifteen minutes. The rest of the class was spent on 10.11. Homework: read # 9 and the handout on concise sherical trigonometry. Do problems 10.6, 10.7, 10.8.

Class 8

The class read me an hysterical story they wrote on why Gudermann studied the gudermannian. We discussed it for 20 minutes. They then spent 7 minutes on 11.1, 10 (resp., 15) on 11.2, 10 (resp., 20) on 11.3, then 40 (resp., 18) on 11.4. There was a break while they worked on 11.4. The group that took 40 minutes had forgotten a lot of the basics of calc 2 integration techniques and had to rederive some of them. Both groups then spent the remaining 60 minutes working on 11.5 but they did not remember how to rotate axes to eliminate the xy term in a quadratic nor could the derive it. Homework: Finish exercise 11.5. Do problems 1.1, 1.2, 1.3, 1.4. Read #10. Do the final draft of the paper.

Class 9

We started out with a discussion of what they had done over break on various math issues including a request for help in that they had a conflict with proctoring 27 April and our class (7 min). They did 11.6 plus that problem for an hyperbola in 8 minutes. 11.7 took them 15 minutes, 11.8 and problem 11.2 (undone on homework) 45. We then spent 20 minutes with Dusty presenting his solution to problem 11.3. After a 10 minute break, we spent 5 minutes discussing problem 11.4 (some of them copied the problem wrong) after which they did 11.9 in 5 minutes, 11.10 in 10 minutes, 11.11 in 20 minutes, 11.12 if 20 and 35 minutes resp, then 11.13 in 20 and 5 minutes resp. Homework: Read #11. Do problems 11.5, 11.6, 11.7, 11.8.

Class 10

Harold Boas took the class since I was sick. It took 10 minutes to orient Harold, then 65 minutes to finish Chapter 11. Harold then spent 10 minutes making comments on the homework they turned in. After a 10 minute break they started chapter 12 spending 30 minutes on 12.1-4, 10 minutes on 12.5-6, 30 minutes on 12.7, and 15 minutes on 12.8-12.9. Homework: Problems 11.9, 11.10, 11.11, 12.1.

Class 11

Student presentations on Laguerre polynomials and the Riemann Zeta function.

Class 12

Student presentations on Legendre polynomials and the Gamma function.

Class 13

Student presentations on Lambert's W function and Bessel functions.

Class14

Student presentations on Weierstrass ϕ function and hypergeometric series.

Class 15

Appendix C

List of materials for course packet

These materials will be available for purchase at a local copy center.

1. René Descartes, *Discourse on the Method of Rightly Conducting the Reason, and Seeking Truth in the Sciences*, excerpt from Part II; available from `gopher://wiretap.area.com:70/00/Library/Classic/reason.txt`.

2. René Descartes, *Philosophical Essays*, translated by Laurence J. Lafleur, Bobbs-Merrill Company, Indianapolis, 1964, pages 156–162.

3. Excerpt from *Alice in Puzzleland* by Raymond M. Smullyan, Penguin, 1984, pages 20–29.

4. Proofs without words from *Mathematics Magazine* **69** (1996), no. 1, 62–63.

5. Stephen B. Maurer, The recursive paradigm: suppose we already knew, *School Science and Mathematics* **95** (1995), no. 2 (February), 91–96.

6. Robert Louis Stevenson, "The Bottle Imp", in *Island Nights' Entertainments*, Scribner's, 1893; in the public domain and available on the world-wide web at `http://gaslight.mtroyal.ab.ca/bottleimp.htm`. (Compare the surprise examination paradox.)

7. "Chance and Chanceability", Chapter VII, pages 223–264, of *Mathematics and the Imagination* by Edward Kasner and James Newman, Simon and Schuster, 1940. This selection is an introduction to probability.

8. Richard J. Trudeau, *Dots and Lines*, Kent State University Press, 1976, pages ix–27. This introduces the notion of a graph and gives some examples.

9. William Dunham, *The Mathematical Universe*, Wiley, New York, 1994, pages 51–63. This is a biographical piece about Euler.

10. James R. Newman, *The World of Mathematics*, Volume One, Simon and Schuster, New York, 1956, pages 570–580. This is a commentary on and a translation of Euler's original paper on the seven bridges of Königsberg.

11. Sir Edmund Whittaker, "William Rowan Hamilton," *Scientific American*, May 1954, reprinted in *Mathematics in the Modern World*, Freeman, San Francisco, 1968, pages 49–52. This is a biographical piece about Hamilton.

12. Alan Tucker, The parallel climbers puzzle, *Math Horizons*, Mathematical Association of America, November 1995, pages 22–24.

13. Frank Harary, *Graph Theory*, Addison-Wesley, 1969, chapter 1, pages 1–7.

14. Richard J. Trudeau, *Dots and Lines*, Kent State University Press, 1976, chapter 4, pages 97–116.

15. *The Traveling Salesman Problem*, edited by E. L. Lawler, J. K. Lenstra, A. H. G. Rinnooy Kan, and D. B. Shmoys, Wiley, New York, 1985, pages 1–15. This is a historical piece by A. J. Hoffman and P. Wolfe on the traveling salesman problem.

16. Norman L. Biggs, E. Keith Lloyd, and Robin J. Wilson, *Graph Theory 1736–1936*, Oxford University Press, 1976, chapter 6, pages 90–108. This is a historical piece including Kempe's famous false proof of the four-color theorem and Heawood's correction.

17. Ralph P. Boas, Möbius shorts, *Mathematics Magazine* **68** (1995), no. 2, 127.

18. Ian Richards, "Number Theory," in *Mathematics Today: Twelve Informal Essays*, pages 37–63, edited by Lynn Arthur Steen, Springer-Verlag, 1978.

19. Ivars Peterson, "A Shortage of Small Numbers," in *Islands of Truth: A Mathematical Mystery Cruise*, pages 152–161, Freeman, 1990.

20. Victor Klee and Stan Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Dolciani Mathematical Expositions, No. 11, Mathematical Association of America, 1991, pages 173–181 and 203–214.

21. Robert Gray, "Georg Cantor and transcendental numbers," *American Mathematical Monthly* **101** (1994), no. 9, 819–832.

22. David M. Bloom, "A one-sentence proof that $\sqrt{2}$ is irrational," *Mathematics Magazine* **68** (1995), no. 4, 286.

23. Vincent P. Schielack, Jr., "Math Bite: A quick counting proof of the irrationality of $\sqrt[n]{k}$," *Mathematics Magazine*, **68** (1995), no. 5, 386.

24. Ivan Niven, "A simple proof that π is irrational," *Bulletin of the American Mathematical Society*, **53** (1947), 509.

25. Excerpts from Ivan Niven, *Irrational Numbers*, Mathematical Association of America, 1967, pages 16–27, 117–118, and 131–133.

26. Excerpt on Fermat theorems, in *A source book in mathematics, 1200-1800*, edited by Dirk Jan Struik, Harvard University Press, 1969, 1987, reprinted by Princeton University Press, pages 26–29.

27. Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, third edition, Addison-Wesley, 1992, pages 166–170 (the perpetual calendar).

28. Sue Geller, "Exact Solutions to Linear Systems," 1997.

29. Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, third edition, Addison-Wesley, 1992, 234–245.

30. Joseph Gallian, "Math on Money," *Math Horizons*, Mathematical Association of America, November, 1995, 10–11.

31. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* **21** (1978), 120–126. Available as LaTeX source and as PostScript on Rivest's home page at `http://theory.lcs.mit.edu/~rivest/publications.html`.

32. Sue Geller, An Introduction to Error-Correcting Codes, 1997.

33. Daniel Pedoe, *The Gentle Art of Mathematics*, Macmillan, 1959 (Collier, 1963; Dover, 1973), pages 18–21 (excerpt on Nim).

34. Sue Geller, Algebra for Constructibility, 1998.

35. Sue Geller, Factoring Polynomials, 1997.

36. Philip D. Straffin, *Game Theory and Strategy*, Mathematical Association of America, 1993, Part I, pages 3–61.

37. John G. Kemeny and J. Laurie Snell, "Game-theoretic solution of baccarat," *American Mathematical Monthly* **64** (1957), 465–469.

Traditionally, the preceding readings have been used during the fall semester, and the following readings have been used during the spring semester.

38. Stanisław Lem, "The extraordinary hotel, or the thousand and first journey of Ion the quiet", in *Stories about Sets* by N. Ya. Vilenkin, Academic Press, 1968.

39. Robert Gray, Georg Cantor and transcendental numbers, *American Mathematical Monthly* **101** (1994), no. 9, 819–832.

40. Edward B. Burger and Thomas Struppeck, Does $\sum_{n=0}^{\infty} \frac{1}{n!}$ really converge? Infinite series and p-adic analysis, *American Mathematical Monthly* **103** (1996), number 7, 565–577.

41. Zeev Barel, "A mnemonic for e," *Mathematics Magazine* **68** (1995), number 4, 253.

42. Wayne Barrett, "It had to be e", *Mathematics Magazine* **68** (1995), number 1, 15.

43. Chapter 47, “bentley’s theorems”, Pomona group (provided by one of the original members of the group).

44. B. C. Carlson, *Special Functions of Applied Mathematics*, Academic Press, 1977, pages 1–6.

45. John Fauvel, “Revisiting the history of logarithms,” *Learn from the Masters*, Frank Swetz et al., eds., Mathematical Association of America, 1995, pages 39–48.

46. Victor J. Katz, “Napier’s logarithms adapted for today’s classroom,” *Learn from the Masters*, Frank Swetz et al., eds., Mathematical Association of America, 1995, pages 49–55.

47. David Shelupsky, “Limitless integrals and a new definition of the logarithm,” *Mathematics Magazine*, **68** (1995), number 4, 294–295.

48. Victor J. Katz, “Ideas of calculus in Islam and India,” *Mathematics Magazine* **68** (1995), number 3, 163–174.

49. Jacques Redway Hammond, *Concise Spherical Trigonometry*, Houghton Mifflin Co., (1943), pages 29–37 and 98–101.

50. B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, 1985, pages 52–62, 94–102, and 177–186.

51. William Dunham, *Journey through Genius: The Great Theorems of Mathematics*, Wiley, 1990, Chapter 6: Cardano and the Solution of the Cubic, pages 133–154.

52. Uwe F. Mayer, “A Proof that Polynomials have Roots,” The College Math Journal, **28**, (1997), number 1, page 58.

53. David Eugene Smith, *A source book in Mathematics*, Dover, 1959, “Gauss”, pages 292–306.