Concepts of Modern Mathematics I (Math 202)
Virginia Intermont College

Jason Riedy

Fall semester, 2008

These pages are available as PDF, either as one growing PDF document for the entirety or as individual documents for each session's notes.

If you have difficulties viewing these or have particular accessibility needs, please mail me at `jason@acm.org`.

Contents

Part I

Introduction

Chapter 1

Syllabus

1.1 Concepts of Modern Mathematics I

Initial home page: http://jriedy.users.sonic.net/VI/math202-f08/

Meets MWF 9.00am-9.50am in room 210 on the second floor of the J. F. Hicks Memorial Library.

The original syllabus is available, and notes will be posted as available.

Homework problems are posted in each session's notes.

1.2 Goals

- Gain practice in mathematical reasoning and problem solving.
- Review material relevant for elementary education.
- Fit mathematics into its historical and practical contexts.

1.3 Instructor: Jason Riedy

- email: Jason Riedy <`jason@acm.org`>
- instant messages (sometimes): `jason.riedy@gmail.com`
- office hours: MW 1.30pm-2.30pm in the Math Lab (see Section 33 below) or by appointment. Or you may find me many afternoons at Java J's in Bristol or Zazzy'z in Abingdon.

1.4 Text

Long, Calvin T. and DeTemple, Duane W. Mathematical Reasoning for Elementary Teachers, fourth edition. Addison Wesley, 2005. ISBN 0-321-28696-0

1.5 Grading

Standard 10-point scale, 3 points on either side for -/+ grades.

The homework is 20%, three mid-term exams are 20% each, and the final counts for 40%. This adds to 120%; the final counts as two 20% scores, and the lowest 20% score is dropped.

1.6 On homework

Some problems will be given in every class. The week's problems will be collected on the following Monday.

Mathematics is a social endeavour. Groups are encouraged, but everyone must turn in their own work. At some point, you will be asked to present a homework problem, its solution, and your reasoning to the class.

Also, there may be solutions available for problems. But try tackling the problem **yourself** (or with your group) first. Practice is important.

Write out sentences and not sequences of expressions. Explain your approaches. This class is as much about the reasoning process as the results.

1.7 Submitting homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 2

Syllabus schedule

Chapters 1 and 2 Scheduled for 18 August through 17 September. Roughly 2.5 weeks on chapter 1, then 1.5 weeks on chapter 2.

First exam Scheduled for 19 September.

Chapters 3, 4, and 5 Scheduled for 22 September through 29 October.

Second exam Scheduled for 31 October.

Chapters 6 and 7 Scheduled for 3 November through 26 November.

Third exam Scheduled for 28 November.

Review Scheduled for 1 and 3 December.

Final exam Official time: Saturday, 6 December from 3.30pm until 5.30pm.

Part II

Notes for chapters 1 and 2

Chapter 3

Notes for 18 August

Notes also available as PDF.

3.1 Syllabus and class mechanics

The original syllabus is available.

3.2 Introductions

- Backgrounds
- Goals? (*i.e.* which grade levels?)

Remember: I'm a mathematician, not an elementary educator. help keep me on track for what **you** need.

Reminder that elementary is not a judgement, it's a description. when a mathematician or scientist uses "elementary", they mean to understand or solve a problem almost from first principles.

(*e.g.* Elementary functions like sine and cosine cannot be built simply from other functions.)

3.3 First "homework"

After checking the table of contents, for which topics in chaps 2-7 would you like the most review?

Via email, please. I'd like to have them while planning the next few classes.

3.4 Problem solving

- Goal is to build up mathematical "common sense"

3.4.1 Categories

- Problems to find
- Problems to prove

Emphasis for early years is the first, problems to find.

3.4.2 Pólya's stages

- Understand the problem
- Divise a plan
  - We will explore a taxonomy of plans
- Carry out the plan
- Examine the solution

Continuing example from Plya; uses the geometry of right triangles. A bit past elementary level, but it illustrates the right aspects.

3.4.3 Understand the problem

- What is known, the data?
- What is unknown?
- What is the relation or condition linking the data with the unknown?
- initial guess: is it possible to satisfy the condition?

Find the diagonal of a box (rectangular parallelpiped, like the classroom) of which the length, width, and height are known.

draw the figure

(dialog not including additional prodding, etc)

Me What is the unknown?

class length of diagonal

Me What is the data?

class length, width, and height

Me Help me write it. What notation should be use?

class x for the unknown, a, b, c for the sides.

Me So what is the relationship between x, a, b, and c in words? Don't be fancy, *etc.*

class x is the diagonal of the box with side lengths a, b, and c.

Me Does the problem sound reasonable? Can the condition be satisfied at all?

class yes, a, b, and c completely determine the box, and so also the diagonal

3.4.4 Devise a plan

Do you know of a related problem?

(tea kettle joke about reducing to an already solved problem)

Look at the unknown. Do you know of a similar problem with the same type of unknown? It's a length.

If remembering length of a hypotenuse, good!

Otherwise: can you think of a similar but simpler problem?

Keep close to the actual problem by checking that all relevant data are used, and that the entire condition is used.

(most explicit hint to use: Can you find a triangle?)

3.4.5 Carry out the plan

Add additional notation for the new length, d.

Apply Pythagorus.

Smaller triangle: $a^2 + b^2 = d^2$.

Apply to larger triangle: $d^2 + c^2 = x^2$.

So: $a^2 + b^2 + c^2 = x^2$.

3.4.6 Looking back

Can you check or verify the result? Test it?

Did you use all the data?

Can you reach the same conclusion differently?

Does this reduce to the simpler case? Do the dimensions match?

Can you think of similar problems to which this may apply? (*e.g.* distance from the center to a corner)

Chapter 4

Notes for 20 August

Notes also available as PDF.

4.1 Review

4.1.1 Problem solving

- Goal is to build up mathematical "common sense"

4.1.2 Categories

- Problems to find
- Problems to prove

4.2 Today's goal: Problem solving principles

- Review the principles
- Two tactics: Guessing and tabling.

4.3 Pólya's principles

These are **principles** and not a recipe. Use these to form a problem-solving plan. (problem solving as a problem...)

- Understand the problem
- Divise a plan
  - We will explore a taxonomy of plans
- Carry out the plan
- Examine the solution

4.3.1 Understand the problem

- Often helps to rephrase a few ways.
  - In English (or whatever is appropriate)
  - With mathematical notation
- Determine what may be relevant.
- Sketch the problem graphically, with numbers, with physical items... Whatever works for **you** on this problem.
- Decide if the problem may **have** a reasonable solution.

4.3.2 Divise a plan

- Taxonomy of plans in the text.
- Will explore shortly.
- The last "be ingenious"... Don't take it seriously. Far more work is accomplished by being systematic.
- The "ingenious" part comes with practice, building up connections in your mind.

  Sure I'm lucky. And the more I practice, the luckier I get. – Gary Player, golfer
- One goal: Turn a strategy into a list of questions to ask students.
- When I think about the strategy, I consider what I want to write about it. A major goal of mathematics is communicating ideas well.

4.3.3 Carry out the plan

- Details depend on the plan...
- May work, may not work.

- Dead-ends are common when approaching new styles of problems.
- Moving through the plan requires attention to detail.
  - Mathematicians and scientists grow to **loath** +/- signs.
  - Eventually, you learn which details can be "fixed" later.

4.3.4 Examine your solution

- Very, very important.
- Check your results somehow, possibly by varying the problem a little.
- Try to generalize a little.
- **Interpret** your results. Often provides a check in itself, or leads to an alternate route.
  - Common in mathematics: First publication of a result is long and hairy. Interested people being interpreting it, and a short or more direct proof is found.
  - Erdős and the "book proof".

4.4 Two closely related tactics, guessing and making a list

- Both are forms of **searching**
- Guessing: heuristic
- Tabling: methodical

4.4.1 Guessing

- Begins as a hunch
- A few examples later becomes a guess
- More examples (fitting into a mathematical dialog) becomes a conjecture.

4.4.2 Example 1.3 from the text

- Note: Phrases like "pretty clear" and "obvious" are dangerous.
- First problem to solve: What is the problem?

  - Want to extend the pattern. What is the pattern?
- Rephrase the problem. Variables?
  - Not for elementary students, but it helps to stay ahead of them...
- Before guessing **look for relationships**. A little larger here a little smaller there.
- Now start guessing and checking.
  - Use the relationships, and look for more. This helps target your guesses.
  - That is the search...
- Now have two examples. Look back at what we've done, and look ahead to what we can do.
  - Look for other relationships.
  - Construct another problem with a solution

4.4.3 Tabling / Making a list

- Search through the space of answers methodically.
- Ensures you won't miss anything.
- Blind table construction can be **long**...

4.4.4 Example 1.4 from the text: a counting problem.

When you read it, note the follow,

- The technique is to be methodical in constructing the table.
- Take care to chose **one** method and follow it.
- If you remember truth tables from logic, same idea.

Example 1.4, page 15 (?):

> **Make an orderly list**
>
> How many different total scores could you make if you hit the dartboard shown with three darts?
>
> (Three nested circles. Scores 10 for the innermost, 5 for the middle, and 1 for the outer ring.)
>
> **Understand the problem**

Three darts hit the dartboard and each scores a 1, 5, or 10. The total score is the sum of the scores for the three darts. There could be three 1s, two 1s and a 5, one 5 and two 10s, and so on. The fact that we are told to find the total score when throwing three darts is just a way of asking what sums can be made using three numbers, each of which is either 1, 5, or 10.

Devise a plan

If we just write down sums hit or miss, we will almost surely overlook some of the possibilities. Using an orderly scheme instead, we can make sure that we obtain all possible scores. Let's make such a list. We first list the score if we have three 1s. then two 1s and one 5, then two 1s and no 5s, and so on. In this way, we can be sure that no score is missed.

Carry out the plan

Number of 1s	Number of 5s	Number of 10s	Total Score
3	0	0	3
2	1	0	7
2	0	1	12
1	2	0	11
1	1	1	16
1	0	2	21
0	3	0	15
0	2	1	20
0	1	2	25
0	0	3	30

The possible total scores are listed.

Look back

Here the key to the solution was in being very systematic. We were careful first to obtain all possible scored with three 1s, then two 1s, then no 1s. With two 1s there could be either a 5 or a 10 as shown. For one 1 the only possibilities are two 5s and no 10s, one 5 and one 10, or no 5s and two 10s. Constructing the table in this orderly way makes it clear that we have not missed any possibilities.

My additional notes:

Note the similarity with numbers. Consider listing all numbers that fit the following two properties:

1. Use only the digits 0, 1, 2, and 3.
2. Have at most three digits.

Then drop those numbers whose digits do not add to three.

That's another way to construct a table like this: Consider a larger table where it is easier to be systematic, then remove numbers that do not fit the problem.

4.4.5 Different example to show bisection

Modified problem 12.a from the text's chapter review exercises.

Geometric progression Sequence of numbers defined by a starting number and a constant. The second number is generated by multiplying by the constant, the third by multiplying again.

Consider the sequence where 3 is the starting number and two is the constant.

- First: $3 = 3$
- Second: $6 = 3 \cdot 2$
- Third: $12 = 6 \cdot 2 = 3 \cdot 2^2$
- and so forth.

Which term in the sequence is 768?

- Solve by a list? Could be long.
- What is 2^{10}? What is $3 \cdot 2^{10}$?
- Know third and 11th term. Third is smaller, 11th is larger.
- Which term to try next?
- Half-way is the 7th term: $2^6 \cdot 3 = 192$
- Now what region? ($>$ 7th, $<$ 11th)
- 9th: 768. **DONE**
- Calculated **three** terms (11th, 7th, 9th) rather than **five**.

4.5 Next time: More problem solving ideas.

4.6 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Problem set 1.1:
  - Problems 10, 13 (Hint: find a way to make a smaller table)

- Construct an example like 1.3 where there is **no** solution. Explain what lead you to its construction. (Hint:
- Problem set 1.2:
  - Problems 5, 7, 8
- Consider solving Example 1.3 with a table starting at a=1, b=1, c=1. How long would the table be if you step through the choices? How many entries would you check if you bisect the choices? (Hints:
  1. Don't make the lists, but rather count the steps in the method for making the list.
  2. Or just go ahead and use a program or spreadsheet to build the lists.)

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 5

Notes for 22 August

Notes also available as PDF.

5.1 Review

5.1.1 Pólya's problem solving principles

Principles are not a recipe, but they are a way to cook.

- Understand the problem
  - Rephrase it, play with examples, sketch it, determine your goals
- Divise a plan
  - Covered two search-based plans, guessing and tabling
- Carry out the plan
  - Requires attention to detail
- Examine the solution
  - Check your result, generalize, try different problems

5.1.2 Tactic: Guessing

- Good for finding a solution satisfying a relationship or emulating an example.
- While rephrasing the problem, look for relationships to guide the guesses.
- If stuck, try related or simpler examples.

- Looking back at the problem can help you target guesses better on similar future problems.
- Examples:
  - Number games
  - Getting started on just about any problem. Guessing helps find examples while understanding the problem.

5.1.3 Tactic: Tabling / Making an orderly list

- Good for listing problems and some counting problems.
  - Find the number of ways to make change given certain coins.
- Can be good for satisfying relationships when guesses run dry.
- Search through the space of answers methodically.
- Ensures you won't miss anything.
- Takes attention to detail in the **plan** of making the table.
- The simpler the plan, the fewer mistakes in execution.
- Examples:
  - Logic tables
  - Counting ways to make a particular sum
    - *(Amusingly, this is a computationally difficult problem. There is no known method that is fundamentally better than listing the possibilities.)*

5.1.4 Example of creating a list

Problem 11 in set 1.2:

> When Anita made a purchase she gave the clerk a dollar and received 21 cents in change. Complete this table to show what Anita's change could have been.

# dimes	# nickles	# pennies
2	0	1

- Why does the list start with one penny?
  - *Only way to make any change ending in 1.*
- Can you use that to simplify the problem?

  - *Use 20 cents rather than 21, then add 1 to the last column.*

Removing extraneous details can help simplify a table-making method.

- What now? Decide on a **systematic method** for filling in the table.
- Methods for making methods:
  - Find a rule each row of the table must satisfy.
    - A conserved quantity is good, here the total amount.
  - Find rules relating the columns.
    - How many nickles per dime? Pennies per. . . ?
  - Decide on a transformation style from one row to the next.
    - Try to push from one side to the other.
    - Will need to back-track sometimes.
  - Look for groups to separate the table, possibly nested.
    - How many dimes can be used? Each number determines a group.
    - Within each dime group, how many nickels?
    - Defines a recursive function, may recall from Math 131.
  - Sometimes careful construction leads to a direct solution.
    - Not this time, at least not without some number theory. (See linear Diophantine equations and how to solve them.)
- Extra idea: Extend the table by one column to have a total. Check along the way.
  - The goal of self-checks is not only to find errors earlier but also to help **locate** the error.
  - Designing good checks is an art in itself, but can help with the table design.
  - An aphorism from computer programming:

    Everyone knows that debugging is twice as hard as writing a program in the first place. So if you're as clever as you can be when you write it, how will you ever debug it? – Brian Kernighan (C, Unix, awk, . . .)

Ideal end results:

- One dime becomes two nickels, one nickel becomes five pennies
- Each dime quantity defines a group. Each nickel quantity defines a (fairly trivial) group.

- Within a group, push change across the row.

No number means a zero.

# dimes	# nickles	# pennies	total cents = 20
2			2*10 = 20
1	2		10+2*5 = 20
1	1	5	10+5+5*1 = 20
1		10	10+10*1 = 20
	4		4*5 = 20
	3	5	3*5+5*1 = 20
	2	10	2*5+10*1 = 20
	1	15	1*5+15*1 = 20
		20	20*1 = 1

Remember: The "real" answer has one extra penny, so add 1 to the penny column.

5.1.5 Tactic not from the text: Orderly creation of a partial list

- One example is **bisection**.
- Works when there is a natural order in the result values.
  - Example last time was finding a term in an **increasing** sequence.
- Pick a place to check the result value.
- Consider an increasing sequence like the example in `the last session`:
  - If it's too small, pick a second larger place. Let's call it A.
    - If still too small, repeat. Replace the old staring point A.
  - If too large, pick a second smaller place.
    - If still too large... Same idea.
  - Once you find a bracketing point, B, consider a point half-way between A and B.
    - If the half-way point is too small, replace A and repeat.
    - If it's too large, replace B and repeat.

5.2 New tactic: Drawing a diagram

Talk about a coincidence, although clearly the example has no relationship to actual car models. Example 1.5 from the text, but done a little differently.

Example 1.5: Draw a diagram

In a stock car race the firist five finishers in some order were a Ford, a Pontiac, a Chevy, a Buick, and a Dodge.

1. The Ford finished seven seconds before the Chevy.
2. The Pontiac finished six seconds after the Buick.
3. The Dodge finished eight seconds after the Buick.
4. The Chevy finished two seconds before the Pontiac.

In what order did the cars finish the race?

5.2.1 Understanding the problem

What information do we have?

- Make of five different finishers.
- Only one dimension is involved: time.
- Four statements relating their finishing times.
- Four relative time relationships.
- The Buick is mentioned most often, but every make is mentioned at least once and no relationships are obviously repeated.

Is this enough information?

- Five cars, four relationships, one dimension.
- Consider: (car)-(car)-(car)-(car)-(car). Four relationships.
- Could be exactly enough information.

Try rephrasing the problem.

- Place five points (F, P, C, B, and D) on a line such that
  1. F is seven units to the right of C,
  2. P is six units to the left of B,
  3. D is eight units to the left of B, and
  4. C is two units to the right of P.

5.2.2 Devise a plan

- All distances are relative. We need a starting point.
- Pick one. B volunteers by appearing twice.
- Apply all relationships with B on the right.
- Then we will have two new cars placed. Use all relationships with those on the right.
- Repeat until finished or stuck.
- If stuck with this method, is there any solution?
  - *No. All times are relative. There would be at least two groups of cars with no relationships between the groups.*

5.2.3 Carry out the plan

Now we get to draw. Sorry, but I'm just using tables.

Using relationship 2 and 3,

		P(6)	-(5)	-(4)	-(3)	-(2)	-(1)	B
D(8)	-(7)	-(6)	-(5)	-(4)	-(3)	-(2)	-(1)	B

Simplifying the presentation:

D	-	P	-	-	-	-	-	B

- Now we have D and P available for resolving the rules.
- Only one appears on the right of a rule, P in rule 4.

Place C by rule 4:

D	-	P	-(1)	C(2)	-	-	-	B

Now C is available, so place F by rule 1:

D	-	P	-	C	-(1)	-(2)	-(3)	B(4)	-(5)	-(6)	F(7)

Or without the counts:

D	-	P	-	C	-	-	-	B	-	-	F

So the final finishing order is F, then B, then C, then P, and then D.

5.2.4 Looking back

- How can we check this result?
  - Did we place all the cars? *Yes.*

  - Did we use all the statements? *Yes, so there can be no inconsistency.*

- What helped with executing the plan?
  - The way the statements were written let us build a concrete plan.
  - We could follow the chain of cars.
- Variations on the problem:
  - Would three statements be enough?
    - *No.* One car would be left out of the relationships. Counting to determine if a problem is soluble will return.
  - Would more statements guarantee a solution?
    - *No.* Not if the statements are inconsistent.
    - *No.* Some cars may not be related to others.
  - If the statements were consistent and not repeated, how many would we need to guarantee a solution exists?
    - The total number of consistent relationships possible is a counting problem in itself. The result is every way to choose two cars from five, "5 choose 2" = 5!/(2!(5-2)!) = 10, where 5! is "5 factorial" or 5*4*3*2*1.
    - The minimum number of relationships is 4 (from above), the maximum is 10.
    - There's a kind of order here from a threshold. If a solution is guaranteed by K consistent relationships, it also is guaranteed by $K + 1$.
    - You could search for counter-examples from 5 to 9, or you could use the order here to bisect.

5.3 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Problem set 1.2:
  - Problem 13, for making a list.
  - Problem 18, for drawing a diagram.

- Problem 20, somewhat combining all of the above. Hints: Try techniques on a smaller problem. Find a numerical property about the number of edges exposed. And consider two limiting cases to govern how many possibilities exist.

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 6

Solutions for first week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

6.1 Problem Set 1.1

6.1.1 Problem 10

Part a

Following the construction rules for one pass forward:

3	*4*	*?*
7	*7*	
14		

What remains is to fill in the upper-right corner. The rule is that the 7 below the "?" is the sum of 4 and the missing number "?". So the final result is

3	*4*	**3**
7	*7*	
14		

Part b

In this case, no side-by-side numbers are provided. One must start by working on the rule from the apex backward. In the first step, the row above 16 must add to 16, so the missing number is 7. Subtracting 7 from the left and right sides produces the two corner numbers. The final figure is

0 *7* **2**
7 *9*
16

Part c

Here there is not enough information to progress in either direction. A solution comes from guessing, building a table, or finding relationships. A table would include numbers from 0 to 9 for each of the four open spots.

For finding *one* solution, note the problem is symmetric. So the numbers along the left side are equal to the numbers along the right. We can use this information to produce a smaller table.

However, symmetry provides sufficient information to work up the figure. The two numbers above the 10 are the same and add to 10, so each is five. Then the corners must be four, and one solution is

4 *1* **4**
5 **5**
10

Part d

Both parts a and b were formed by applying the rules directly. There was no room for changing any of the values, so these are the only solutions.

For part c, the solution above reduced the problem until there was a unique solution. But the original problem did not require that the numbers down each side stay the same, so we are free to try other patterns. Given the rule for adding adjacent entries in one row to form the next, we know we can shift numbers so long as their sums are the same.

Pushing a one from the left to the right produces a few more examples from the initial solution on the left:

4 *1* **4**
5 **5**
10

3 *1* **5**
4 **6**
10

2 *1* **6**
3 **7**
10

6.1.2 Problem 13

One way to create a table for this problem would be to list all sequences of the numbers 2, 3, 4, 5, and 6. The consider mapping the sequences to the diagrams row-wise; the first three numbers fill the three circles in first row, the next number fills the next circle down, *etc.*

Filling in the table first by rotating the initial sequence,

2	3	4	5	6	**No**, $2+3+4 \neq 3+5+6$
6	2	3	4	5	**YES**, $6+2+3 = 2+4+5$
5	6	2	3	4	**YES**, $5+6+2 = 6+3+4$

This order happens to answer both part a and b almost immediately. In the worst case, however, there are $5! = 120$ rows in this table.

So two examples satisfying the relationship are

6	2	3			5	6	2
	4					3	
	5					4	

Answering part c by an exhaustive table requires all 120 rows because the answer is **no**. This part also indicates how to reduce the table.

The top row of three and the middle column of three add to the same quantity. They also share one number where they intersect. That number does not matter at all. And the order of the remaining numbers within the row or column also does not matter.

So each row of a full table need provide only which number is left out and then two pairs. And note that after picking the number and the first pair, only a single pair remains. So chosing to drop 2 and then picking the pair $(3, 5)$ leaves 5 and 6 which forms only one pair. There are five numbers to drop out and six ways to pick a pair from the remaining four numbers, so a complete table was only 30 lines and not 120.

To check the last part, however, we know 3 will be the number left out. This leaves only *six* lines to check, far fewer than 120.

left out	first pair	second pair	
3	2, 4	5, 6	$6 \neq 11$
	2, 5	4, 6	$7 \neq 10$
	2, 6	4, 5	$8 \neq 9$
	4, 5	2, 6	$9 \neq 8$
	4, 6	2, 5	$10 \neq 7$
	5, 6	2, 4	$11 \neq 6$

Examining the sums in the table, note that one always is odd and one always is even. Dropping 3 from the initial sequence leaves 2, 4, 5, and 6. Of those, three

are even and only one is odd. The sum of two even numbers is even, and the sum of an even and an odd number is odd. So there is no way to choose two pairs from 2, 4, 5, 6 such that both add to an even or to an odd number. Hence the sums cannot be equal.

Sometimes taking care in reducing a table is more work, but it can make plain relationships you can use in future problems to avoid making any table at all.

6.2 Example like 1.3 with no solution

I apologize for chopping off the hint. It suffered from a cut and paste error and should have pointed you to the even/odd idea.

Guessing and creating small tables of examples are perfectly good approaches. Another is to use a similar even/odd relationship.

The sum of the smaller circles is half the sum of the larger circles. So if the larger circles add to an odd value, there is no way to fill the smaller circles with integers adding to half that odd value.

Fill the outer circles with odd number of odd numbers. The resulting sum is odd.

Without the hint, you may simply fill the larger circles with 1, 1, and 1. Then you need a zero somewhere in the smaller circles, and I disallowed zeros or negative numbers during class. I did not realize that the text allowed non-integers and negative numbers in the problem.

6.3 Problem Set 1.2

6.3.1 Problem 5

Generally, it is far easier to see the rule if the guesses are placed in order, answering a portion of part c. Assume that each of the childrens' rules are determined by a relatively simple formula of the chosen number.

Part a

Make a table to see if the guesses could satisfy the rule:

Chosen:	0	2	4	5	8
Returned:	-3	7	17	22	37
First guess:	-3	7	17	22	37
Second guess:	-3	7	17	22	37

So the guesses *may* have found the rule. If the guesses really are the same, that is more evidence. However, the problem does not provide rules for the initial rules. A student's rule could be "return a random number." If the rules are required to be *linear*, that is of the form $ax + b$ where the chosen number is x, then the five choices above are more than the two required to determine the line. (Two points determine a line, and each guess places a point.)

The two guesses appear the same. Consider the guesses algebraically, so the first guess is $5i - 3$ and the second is $5(i - 1) + 2$ where i is the chosen number. Expanding the latter, $5i - 5 + 2 = 5i - 3$, so the rules really are the same.

Part b

The table of provided data:

Chosen:	0	1	3	7	9
Returned:	1	2	10	50	82

The following questions could help guide your guesses,

- Is the sequence formed by a line like $ax + b$? Such a curve grows slowly.
- The next step up is a quadratic curve like a parabola. Does the data fit some simple formula $ax^2 + bx + c$?
- The next step is a cubic with x^3. Do the numbers increase *very* quickly?

Starting at zero helps; you see the constant term must be one. Subtracting one from the other returned numbers,

Chosen:	0	1	3	7	9
Returned -1:	0	1	9	49	81

So a reasonable guess is $x^2 + 1$.

Another route to this result:

The curve grows a little more quickly than we would expect from a line. Also, if this were a line, the first two points determine its structure as $x + 1$, but this does not fit the third point, $3 + 1 = 4 \neq 10$.

A quadratic is determined by three points. From the first, $(0, 1)$, we see that $c = 1$. Then the second $(1, 2)$ and third $(3, 10)$ points set up the equations $a + b = 1$ and $9a + 3b = 9$. We already know this cannot be a line, so $a \neq 0$. Assuming a and b are integers, that leaves $a = 1$ and $b = 0$. So the rule *may* be $x^2 + 1$. That fits the other data.

Part c

The table of provided data:

Chosen:	0	1	2	3	4
Returned:	7	10	13	16	19

This grows slowly, so it's reasonable to guess a linear relationship. The zero term gives a constant 7, and the first term suggests a slope of 3 so $3 \cdot 1 + 7 = 10$. Continuing with the other points confirms that this is a reasonable guess.

Choosing the first few numbers starting from zero definitely helps make the relationship clear. However, it can be useful to pick a few consecutive numbers further away to see how quickly the function grows. In this case, we would expect choosing 10 and 11 to result in two numbers as close together as the results from 0 and 1 if the problem were linear. If the student had returned two numbers much further apart, we could avoid trying to fit the data to a line.

6.3.2 Problem 7

There are many straight-forward ways to build a table here.

One starts by placing all four coins in one denomination, then moves a coin to the right:

N	D	Q	total
4	0	0	20
3	1	0	25
3	0	1	**40**
2	2	0	30
2	1	1	45
2	0	2	60
1	3	0	35
1	2	1	50
1	1	2	65
1	0	3	80
0	4	0	**40**
0	3	1	55
0	2	2	70
0	1	3	85
0	0	4	100

There are 15 lines, two of which are shared. So there are 14 different quantities possible.

Another method would write out denominations first and then try to form them with some combination of coins. The smallest possible amount is 20 for using four nickles, and the largest possible is 100 for four quarters. There are

$(100-20)/5 = 16$ possible table entries. But 75 and 90 cannot be formed, leaving 14 different possible quantities.

6.3.3 Problem 8

This is a classical problem used in discrete mathematics and introductory computer science classes, although often starting with a dollar to make tabling less practical.

There are 49 ways.

There are at most two quarters, at most five dimes, at most 10 nickles, and at most 50 pennies per line of a table with the following heading:

Pennies	Nickles	Dimes	Quarters	total

To generate the table, start with two quarters and then shift amounts over as in other problems. You used the conserved quantity, the total amount, to guide your next choice.

Another method for solving this problem is to set up recurrence relationships and build a slightly different table.

Consider making change for an amount N. And consider four different ways for making such change:

A_N with only pennies,
B_N with nickles and pennies,
C_N with dimes, nickles, and pennies, and
D_N with quarters, dimes, nickes, and pennies.

Say we start at N and the full collection of possible coins. Then either the change contains a quarter or it does not. If it does contain with a quarter, then we change the remaining $N - 25$ in the same way, possibly with more quarters. If not, then we change N no quarters. So

$$D_N = C_N + D_{N-25}.$$

Similarly,

$$C_N = B_N + C_{N-10}, \text{ and}$$
$$B_N = A_N + B_{N-5}.$$

We can begin constructing a table of values by N starting from the extreme case $N = 0$. There is only one way of making no change at all, so $A_0 = B_0 = C_0 = D_0 = 1$. There also is only one way of making change with pennies, so $A_N = 1$ for all N. And the relations above show we need only rows where N is a multiple of five and provide formulas for every entry.

N	A_N	B_N	C_N	D_N
0	1	1	1	1
5	1	2	2	2
10	1	3	4	4
15	1	4	6	6
20	1	5	9	9
25	1	6	12	13
30	1	7	16	18
35	1	8	20	24
40	1	9	25	31
45	1	10	30	39
50	1	11	36	**49**

6.4 Consider solving Example 1.3 with a table

Note that each of a, b, and c can be at most one less than the smallest number adjacent to them (I ruled out zeros in class). So there are at most 10 possibilities for a, 14 for b, and 10 for c. Listing all would require $10 \cdot 10 \cdot 14 = 1400$ entries.

But also one variable is completely determined by the other two, so we would need a list of $10 \cdot 14 = 140$ possibilities for a and b (or c and b), or $10 \cdot 10 = 100$ for a and c.

Or we could note that each choice of a immediately determines a possible choice of c. Then we simply verify that some b satisfies the sums. This leaves a total table of 10 lines.

Assume there is a reasonable order for bisection. A *worst case* sequence of entries we could check would be 1, 10, 5, 7, 8, 9; so 6 entries total. The actual sequence here would be 1, 10, 5, 7, 6; so 5 entries.

6.5 More in Problem Set 1.2

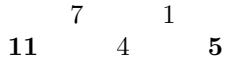
6.5.1 Problem 6: whoops, not assigned

Whoops. I solved this but never assigned it. Keeping the solution here for examples.

There are many approaches. I provide a few overly clever ones below.

The first two parts only require following the rules to fill the triangles.

Part a only requires following the rules to fill the triangle:



Part b is similar, but requires filling in $\mathbf{8} = 19 - 11$:

		19		
	8		11	
9		1		**12**

The next two fall to the same tabling technique outlined in the solution above with some minor modifications.

For part c, the outer sum is odd, so there is no integer solution. The text apparently allows non-integer solutions. Then the following triangle suffices and can be found by doubling all the entries, solving, and halving all the entries again:

		7		
	2.5		**4.5**	
11		**8.5**		13

In part d, the negative numbers can be dealt with by adding a sufficiently large number to the vertices of the triangle, solving the problem, and then subtracting half that number from the intermediate nodes.

The first number we add should be even to maintain the even/odd balance (even+even is even, even+odd is odd, so adding an even doesn't change the number of evens and odds). And adding a number larger than the largest given number will shift all the intermediates above zero. So we chose the smallest even number larger than 11 and hence add 12 across the outer nodes. Solving:

		10		
	3		**7**	
19		**16**		23

Subtracting half 12 (or 6) from the intermediate notes gives a solution to the original problem:

		-2		
	-3		**1**	
7		**10**		11

6.5.2 Problem 13

The area is the product of the length and width. Knowing the lengths are whole numbers, we can write a list of all integers that divide into 120 cleanly. We need only include "half" the entries; the length and width are interchangable.

The perimeter is twice the sum of the length and width. Including the perimeter in the table solves the second part of the problem.

length	width	area	perimeter
1	120	120	242
2	60	120	124
3	40	120	86
4	30	120	68
5	24	120	58
6	20	120	52
8	15	120	46
10	12	120	44

So the shape with the smallest perimeter is the nearly square 10×12. This is true in general: The shape with the least perimeter or surface area enclosing the greatest volume is the closest to a circle or sphere. Here, a square is as close to a circle as you can get with four sides, and 10×12 is as close as you can get to a square.

6.5.3 Problem 18

Drawing diagrams for smaller problems reveals the sequence in the following table:

Sections on each side	Number of posts
1	4
2	8
3	12
4	16

The relationship above is that there are four times as many posts as sections, so the final result is 40 posts for 10 sections.

6.5.4 Problem 20

Each square has four edges, and joining two squares along one edge removes one from both but two from their sum. Hence all possible perimeters all are even.

What is the largest number of exposed edges?

Simple counting arguments give an overestimate. Given nine squares, there can be at most 36 edges exposed, or four for each square. But each square must be joined to at least one other. Again, joining reduces the number of exposed edges by one per square. Each square must be joined, so each contributes at most three edges to the total. So there can be at most 27 edges exposed, or 26 taking into account the previous paragraph.

But they squares are all connected. The form hiding the fewest edges occurs when placing all squares in a line. Shifting around squares from this shape only hides more edges, so we know the largest perimeter is **20**.

And what is the smallest number? There must be at least four edges exposed, as all the squares are linked and there must be at least four larger edges of at least one edge each.

In general, the most "circle-like" figure has the least exposed surface. In this case, the shape would be square, exposing 12 edges. Shifting any block around a square exposes more edges, so the square is the smallest with a perimeter of **12**.

The remaining problem is to take the largest (or smallest) shape and shift blocks around to form all the intermediates. Forming each of **14**, **16**, and **18** is fairly simple.

Chapter 7

Notes for 25 August

Notes also available as PDF.

7.1 Review

7.2 Draw a diagram, follow dependencies

Talk about a coincidence, although clearly the example has no relationship to actual car models. Example 1.5 from the text, but done a little differently.

> **Example 1.5: Draw a diagram**
>
> In a stock car race the firist five finishers in some order were a Ford, a Pontiac, a Chevy, a Buick, and a Dodge.
>
> 1. The Ford finished seven seconds before the Chevy.
> 2. The Pontiac finished six seconds after the Buick.
> 3. The Dodge finished eight seconds after the Buick.
> 4. The Chevy finished two seconds before the Pontiac.
>
> In what order did the cars finish the race?

7.2.1 Understanding the problem

What information do we have?

- Make of five different finishers.
- Only one dimension is involved: time.

- Four statements relating their finishing times.
- Four relative time relationships.
- The Buick is mentioned most often, but every make is mentioned at least once and no relationships are obviously repeated.

Is this enough information?

- Five cars, four relationships, one dimension.
- Consider: (car)-(car)-(car)-(car)-(car). Four relationships.
- Could be exactly enough information.

Try rephrasing the problem.

- Place five points (F, P, C, B, and D) on a line such that
  1. F is seven units to the right of C,
  2. P is six units to the left of B,
  3. D is eight units to the left of B, and
  4. C is two units to the right of P.

7.2.2 Devise a plan

- All distances are relative. We need a starting point.
- Pick one. B volunteers by appearing twice.
- Apply all relationships with B on the right.
- Then we will have two new cars placed. Use all relationships with those on the right.
- Repeat until finished or stuck.
- If stuck with this method, is there any solution?
  - *No. All times are relative. There would be at least two groups of cars with no relationships between the groups.*

7.2.3 Carry out the plan

Now we get to draw. Sorry, but I'm just using tables.

Using relationship 2 and 3,

		P(6)	-(5)	-(4)	-(3)	-(2)	-(1)	B
D(8)	-(7)	-(6)	-(5)	-(4)	-(3)	-(2)	-(1)	B

Simplifying the presentation:

D	-	P	-	-	-	-	-	B

- Now we have D and P available for resolving the rules.
- Only one appears on the right of a rule, P in rule 4.

Place C by rule 4:

D	-	P	-(1)	C(2)	-	-	-	B

Now C is available, so place F by rule 1:

D	-	P	-	C	-(1)	-(2)	-(3)	B(4)	-(5)	-(6)	F(7)

Or without the counts:

D	-	P	-	C	-	-	-	B	-	-	F

So the final finishing order is F, then B, then C, then P, and then D.

7.2.4 Looking back

- How can we check this result?
  - Did we place all the cars? *Yes.*
  - Did we use all the statements? *Yes, so there can be no inconsistency.*
- What helped with executing the plan?
  - The way the statements were written let us build a concrete plan.
  - We could follow the chain of cars.
  - Following dependencies often is called "working backwards."
- Variations on the problem:
  - Would three statements be enough?
    - *No.* One car would be left out of the relationships. Counting to determine if a problem is soluble will return.
  - Would more statements guarantee a solution?
    - *No.* Not if the statements are inconsistent.
    - *No.* Some cars may not be related to others.
  - If the statements were consistent and not repeated, how many would we need to guarantee a solution exists?
    - The total number of consistent relationships possible is a counting problem in itself. The result is every way to choose two cars from

five, "5 choose 2" = 5!/(2!(5-2)!) = 10, where 5! is "5 factorial" or 5*4*3*2*1.

* The minimum number of relationships is 4 (from above), the maximum is 10.
* There's a kind of order here from a threshold. If a solution is guaranteed by K consistent relationships, it also is guaranteed by $K + 1$.
* You could search for counter-examples from 5 to 9, or you could use the order here to bisect.

7.3 Look for a pattern

- Incredibly important at many levels.
- Mathematics generally is about characterizing patterns.
- Immediately useful for
  - extending from provided data, and
  - continuing *relationships* found when considering problems.

7.3.1 Example: What is the last digit of 7^{100}

The initial problem is straight-forward; there appears to be little more to understand. One useful relationship is that there are at most 9 possible finial digits. (Zero is not possible.)

With so few possible digits, a good initial plan is forming a table:

Number	Last digit
7^1	7
7^2	9
7^3	3
7^4	1
7^5	7
7^6	9
$\vdots$	$\vdots$

We certainly don't want to extend this to 7^{100}. However, note that the last digit of 7^4 is 1. Then $7 \cdot 1 = 7$ begins the pattern anew.

To check, we could guess that the last digit of 7^8 is 1. Continuing the table confirms the guess.

So 7^i has the last digit 1 for all i that are multiples of four. And thus the last digit of 7^{100} is 1.

7.4 Patterns and representative special cases

- A *special case* is quite literally a case set aside as special.
- A *representative* special case is a special case that accurately represents the general case.
- Consider teaching a property over all cases by illustrating with a specific case.
- The specific case must not depend on *which* case is used...
- Will use text's example: sums of rows of Pascal's triangle

7.4.1 Sums over Pascal's triangle

- A wonderful source of examples and relationships
  - Related to polynomials, probability distributions, and even fractals.

Written in rather boring table form, each entry is the sum of the entry directly above and above to the left:

#					
0	1				
1	1	1			
2	1	2	1		
3	1	3	3	1	
4	$1 = \mathbf{0} + 1$	$4 = 1 + 3$	$6 = 3 + 3$	$4 = 3 + 1$	$1 = 1 + \mathbf{0}$

Problem: What is the sum of the 20^{th} row? The 200^{th}?

Understanding the problem:

- How is the triangle formed?
  - *Each entry is the sum of the two above.*
- Can we continue this pattern? *Yes.*
- Do we want to write 200 rows? *No.*
- What else can we do?

Plan:

- Form the sums.
- Look for a pattern.
- *Reason about all cases given a representative case.*

The result:

#						sum
0	1					1
1	1	1				2
2	1	2	1			4
3	1	3	3	1		8
4	1	4	6	4	1	16

A guess:

- Each row's sum is twice the previous row's sum.
- Starting from the "zeroth" row as 1, the n^{th} row is 2^n.

- The next few rows check.

Consider a specific case, forming the fourth row:

#						sum
3	1	3	3	1		8
4	$1 = \mathbf{0} + 1$	$4 = 1 + 3$	$6 = 3 + 3$	$4 = 3 + 1$	$1 = 1 + \mathbf{0}$	16

- What do we know about the sum of each row?
  - It's the sum of each entry.
  - In turn, each entry is the sum of two entries from the previous row.
  - So the sum must be the sum of sums of pairs from the previous row, or twice the previous row's sum.

By looking at a special case but applying only general reasoning, we have *proven* that each row's sum is twice the previous row's sum.

- We used no properties specific to the third or fourth rows.
- We could have chosen ("without loss of generality") any row and applied the same reasoning.
- Thus the reason applies to *all* rows.

And the final answers:

- $2^{20} = 1\,048\,576$. A megabyte (MiB in correct units, not MB) is 2^{20} bytes.
- 2^{200} has 61 digits, none of which are particularly elucidating. For this style of problem, leaving 2^{200} unevaluated is much better. But, for completeness, the answer is in the notes.

1 606 938 044 258 990 275 541 962 092 341 162 602 522 202 993 782 792 835 301 376

7.5 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Patterns: What is the 87^{th} digit past the decimal point in the expansion of $1/7$?
- Patterns and related patterns: Using the result of 7^{100} above, what is the last digit of 3^{100}?
- From problem set 1.3:

- Arithmetic progressions: problem 6 (see the text, esp. around examples 1.8 and 1.9)
- Problem 9, and feel free to criticize the use of "likely" or "probably" here as well.
- Problem 11.
- Problem 20.

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 8

Notes for 27 August

Notes also available as PDF.

8.1 Review

- A *special case* is quite literally a case set aside as special.
- A *representative* special case is a special case that accurately represents the general case. with a specific case.
- The specific case must not depend on *which* case is used...
- We *proved* that the sum of the i^{th} row is 2^{i-1}.
- Will return to proofs next time. Today, two tactics / principles and discussion of general mathematical reasoning.

8.2 Ruling out possibilities

- We've already seen this in building tables, guessing, etc.
  - If the result must be even, don't list odd numbers.
  - In the diagram where we filled in circles along the sides of a triangle to equal integers in the vertices, we never needed to guess larger than the smallest integer.
- Generally, use whatever rules apply to reduce your problem.
- In an extreme case, only one result may be left standing.

8.2.1 Logic puzzles

- Classical problem structure. Provide lists of items along with properties linking the lists. Then derive the only possible matching between the lists.
- Zillions of logic puzzles available on-line or in puzzle magazines.

  Each of Bill, John, Fred, and Jim are married to one of Judy, Gretchen, Margie, and Loretta.

  1. Judy's husband's name does not begin with J.
  2. Margie's husband's name has the same letter twice.
  3. The name of Loretta's husband has three letters.
- General strategy: Form a table to track possibilities.
- Fill in what is known from each rule (noted (1), (2), (3) below).
- Cross out possiblities that cannot occur (similar notation).
- What possibilities remains? *Judy and Fred*
- That leaves one spot left, *John and Gretchen*

	Judy	Gretchen	Margie	Loretta
Bill	—(2)	—(2)	Yes(2)	—(2)
John	No(1)	Yes	—(2)	—(3)
Fred	Yes		—(2)	—(3)
Jim	No(1)	—(3)	—(2)	Yes(3)

For an example that *does not work*, see problem 8 in set 1.4 (page 49). Whoever wrote that has no idea what is in a decent banana split or double-dip cone.

8.3 The pigeonhole principle

If there are more pigeons than pigeonholes, then at least one hole holds more than one pigeon.

Thought to have been presented first by Dirichlet in 1834 as the "shelf principle".

- Useful for proving or demonstrating a fact through counting.
- Assume there are 14 black socks and 6 white socks in the drawer. Without looking, how many socks must you retrieve to have two of the same color?
  - How might you consider solving this? *Write out all possibilities for each number of socks you retrieve. Yuck.*
  - Here there are two "holes", black and white.
  - You need draw three socks to guarantee two of the same color!

- Frighteningly powerful principle.
  - Ignoring baldness, there are at least two people in the tri-cities area with the same number of hairs on their head.
    - There are about 150 thousand hairs in a typical head of hair.
    - According to the 2000 census, there are 480 091 people in the tri-cities area.
    - If we assume no one has over 480 000 hairs, and each "hair count" is a category / pigeonhole, then there must be two people with the same number of hairs.
  - A "lossless" file compression system must *expand* some files.
    - Compressed files are pigeonholes.
    - There are fewer possible files of smaller size.
    - Hence if all files can compress to smaller sizes, there will be two files that compress to the *same* file.

The pigeonhole principle and its variations are an indispensable tool of mathematics!

There is a wonderful description and exploration of different phrasings from Edgar Dijkstra:

http://www.cs.utexas.edu/users/EWD/transcriptions/EWD09xx/EWD980.html

Even more examples through the references at

http://www.maa.org/editorial/knot/pigeonhole.html

8.4 Mathematical reasoning

Two key forms of reasoning in mathematics:

Inductive Making an "educated" guess from prior observations.

Deductive If premises are satisfied, conclusion follows.

Premises also are known as hypotheses, suppositions, or other similar terms.

Typically,

problems to find use inductive reasoning, and

problems to prove apply deductive reasoning.

But *finding a proof* is in many ways inductive.

Problem solving so far has been inductive. Take example problems and their solutions. Emulate the solutions on similar problems.

History from the western view:

- Old example: Egyptian papyri (1900bc-1800bc)
  - Consisted of arithmetic tables followed by a list of worked problems.
  - Solve "new" problems by imitating previous ones.
  - No pure "symbols"; only count or calculate with "real" items. (Hieroglyphics hurt.)
- Continued through to Greek times
  - Geometry replaced explicit counting.
  - No "variables" but rather geometric figures.
    - Every concept had to be illustrated geometrically.
    - Pythagoras constructed proportions from lengths.
  - However, *deductive reasoning* began in earnest.
    - Around 600bc, Greek mathematicians began discussing and proving theorems.
    - Euclid's Elements, 300bc, developed systematic and rigorous proofs.
  - Proofs complicated by the restriction to geometric figures.
- Algebra, the beginning of fully abstract proofs:
  - 500bc for Babylonians!
  - 200ad for Greeks (Diophantus of Alexandria)
  - Spread widely from Persians, Muhammad ibn Mūsā al-khwārizmī in 820ad.
    - (transliteration of his book's title gave "algebra", his name gives "algorithm")
- **So modern "proof" only became feasible 1200 years ago.**
- Wasn't widely adopted until the nineteenth century, **200** years ago.
- So if *proof* seems difficult, remember that humanity took a long, long time to develop the idea.
- The concept of *proof* still is evolving!
- Historical summary from Prof. Steven Krantz at

http://www.math.wustl.edu/ sk/eolss.pdf

Remember to take great care with the premises in both forms of reasoning!

- Inductive reasoning *generalizes* from examples.
- If the examples are not appropriate, the result will be incorrect.
- Say there is a line of women waiting for a rest room. You assume it's the lady's room. But if there is only *one* rest room...

8.5 Next time: structures and kinds of proofs

8.6 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- In problem set 1.4 (p48):
  - For reducing the number of possibilites: problem 7
  - Logic puzzle: problem 9
  - Pigeonholes: Problems 12 (ignoring leap years), 13, 14
    - Note that 12 wants the number that *guarantees* two people have the same birthday.
- Which of these statements demonstrate inductive reasoning, and which demonstrate deductive reasoning? Justify.
  - It has rained for the past week. It will rain tomorrow.
  - All men are mortal. Socrates is a man. Therefore, Socrates is mortal.
  - Satellite-based network access does not function through heavy rain. It is raining heavily. I cannot upload the notes right now.
  - The next number after 3, 8, 13, 18, and 23 is **28**.

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 9

29 August: Review of previous notes

See Chapter 8.

Chapter 10

Solutions for second week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

10.1 Patterns: The 87th digit past the decimal in 1/7?

What are the digits of 1/7? A computer or calculator computes something like 0.142857142857143. We start to see a pattern: 142857 is repeated. The chunk has length six, so digit $6i + 1$ will be 1, $6i + 2$ will be 4, and so on. Digit $87 = 6 \cdot 14 + 3$, so we expect the 87^{th} digit will be 2.

We could prove this in a few ways if desired. One would be to carry out long division for seven steps. On the seventh, we would see the same problem as the initial problem, namely 1.0/7. The same problem with the same data must have the same solution, and thus the pattern must repeat.

10.2 Patterns: Units digit of 3^{100}

The quick solution is to note that 3 appears in the "orbit" of 7^{100} directly before 1, because $7 \times 3 = 21$. So in a sense which we will formalize later, 3 is the inverse of 7 with respect to the units digit. We need merely to count backwards in the table generated by powers of 7.

The more direct approach is to note that powers of 3 give a final digit sequence of 3, 9, 7, and 1 repeating after the 1. The sequence works in chunks of four, and we see that the entry for $100 = 4 \cdot 25 + 4$ is 1.

10.3 Problem set 1.3

10.3.1 Arithmetic progressions: Problem 6

Part a. The number of increments by seven is $(86 - 2)/7 = 12$. To check, form $2 + 12 \cdot 7$ and verify it is 86.

Part b. One method is to re-apply Gauss's technique (using inductive reasoning). There are **13** entries in the sequence, 2 and then 12 increments by 7. Pairing these up, we have 6 added terms of the form $2 + 86 = 9 + 79 = 72 + 16 = 65 + 23 = 58 + 30 = 51 + 37 = 88$ and one remaining term of 44. So the result is $6 \cdot 88 + 44 = 572$.

Note that the paired terms added to 88, while the lone term was $88/2 = 44$. Playing with the form above $6 \cdot 88 + (1/2)88 = 88 \cdot (12 + 1)/2$, recalling the $n(n + 1)/2$ form for the sum from 1 to n.

Another method is to work with the summation form directly to find

$$\begin{aligned}\sum_{i=0}^{12}(2 + 7i) &= 13 \cdot 2 + 7\sum_{i=0}^{12} i \\ &= 26 + 7 \cdot \frac{12(12 + 1)}{2} \\ &= 572.\end{aligned}$$

Part c. There is a slight trick to this. Often it is more obvious to start with the zero$^{\text{th}}$ term as I have above. Then the form of the i^{th} term is $2 + 7i$, showing the initial term directly. However, many people prefer counting from one. To convert the form, substitute $n - 1$ for i and see that $2 + 7(n - 1) = -5 + 7n$ is the form of the n^{th} form.

Part d. One method of computing the sum again is to emulate Gauss's trick with the observation from Part a. We expect the sum to be the number of terms, n, times the first plus the last, $2 + (-5 + 7n) = -3 + 7n$, divided by two. So the sum is $n(7n - 3)/2$.

Another method is to work with summation form,

$$\begin{aligned}\sum_{i=0}^{n}(2 + 7i) &= (n + 1) \cdot 2 + 7\sum_{i=0}^{n} i \\ &= 2(n + 1) + 7 \cdot \frac{n(n + 1)}{2}.\end{aligned}$$

With sufficient algebra, this does simplify to the other form.

10.3.2 Problem 9

Part a. Personally, I'd point out that in their limited imagination, the writers likely intend 16 to be the next number.

Part b.

n	2^n	$n^2 - n + 2$	$n^3 - 5n^2 + 10n - 4$
1	2	2	2
2	4	4	4
3	8	8	8
4	16	14	20

Part c. There are many, many functions that could generate 2, 4, and 8. One needs more information to decide on which function.

And the wording of the first problem uses "likely." To me, "likely" infers some probability, but there is none.

Better wording would ask for the *reason* why the student believes the sequence extends to their guesses.

10.3.3 Problem 11

Following the hint, consider rearranging `B B R R` to `B R B R`. That requires one swap in the middle. The number of swaps cannot be fewer, so this is the minimum number.

Now rearrange `B B B R R R` to `B R B R B R`. Two swaps move the left-most `R` into position, `B R B B R R`. The first two letters are correct, and the rest match the previous problem. No fewer swaps could have moved an `R` into the second-left-most position; there must be at least one swap for each position moved. So we know the fewest swaps beyond the first case is two, for a minimum total of three.

At this point, it's reasonable to guess that the number of swaps is either $2^{\#\mathtt{B}-1}-1$ or $\sum_{i=1}^{\#\mathtt{B}-1} i$. Either fits the data so far. However, at each stage we moved one `R` into place and then reduced to a known subproblem. This *adds* moves, so the summation seems the most likely.

To verify that $\sum_{i=1}^{\#\mathtt{B}-1} i = 4 * (4+1)/2 = 10$ swaps suffices, use the following:

Start with:	B B B B B R R R R R
4 swaps later:	B R B B B B R R R R
3 swaps later:	B R B R B B B R R R
2 swaps later:	B R B R B R B B R R
1 swap later:	B R B R B R B R B R
Total number of swaps:	10

To support that this is the *minimum*, we rely on inductive reasoning. At each stage, we add the minimum number of necessary swaps to the subproblem, which in turn is solved minimally. To formalize this, we could apply *mathematical induction*.

10.3.4 Problem 20

Part a. The sums are 12, 24, 48, and 64. One pattern is that the sum is four times the repeated quantity on the anti-diagonal. Another is to note that the repeated quantity is one larger than the upper-left corner and one smaller than the lower-right corner.

So adding along "opposite" anti-diagonals is like adding the same number entries from the main anti-diagonal. So given a block of the form

$$\begin{matrix} k-1 & k \\ k & k+1 \end{matrix}$$

we can add the two far anti-diagonals to get $(k-1)+(k+1)=2k$. Along with the main diagonal, the total sum is $(k-1)+(k+1)+k+k=4k$.

Part b. The sums are 54, 108, and 144.

Part c. The blocks follow a similar pattern as the previous part:

$$\begin{matrix} k-2 & k-1 & k \\ k-1 & k & k+1 \\ k & k+1 & k+2 \end{matrix}$$

Again, add along "opposite" anti-diagonals to match $+2$ and -2, $+1$ and -1. So the sum must be $9k$.

Part d. In each case, the sum is the number of squares times the element repeated along the main anti-diagonal. If the square is side-length n and the main anti-diagonal holds k, the sum is n^2k.

10.4 Problem set 1.4

10.4.1 Reducing possibilities: Problem 7

Part a. Writing out the conditions that are easy to express gives

$$\begin{aligned}
&x = 2k + 1 \text{ for some } k,\\
&x > 1,\\
&x < 100,\\
&x > 20,\\
&x < 5 \cdot 7 = 35, \text{ and}\\
&x = 5i \text{ for some } i.
\end{aligned}$$

Combining the first and last, we know x is an odd multiple of five, or $x = 5(2j+1)$ for some j. The inequalities reduce to $20 < x < 35$. The only possibility in this range is $x = 25$, and the digits here add to seven.

Part b. Again, translating the conditions and rewriting them to be *positive* rather than negated (so "not even" becomes "odd") gives

$$\begin{aligned}
&x = 2k + 1 \text{ for some } k,\\
&x = 11i \text{ for some } i,\\
&x > 20,\\
&x = 3j \text{ for some } j, \text{ and}\\
&x < 79.
\end{aligned}$$

An odd multiple of three and nine can be expressed by composing the requirements, so $x = 3 \cdot 11 \cdot (2p + 1) = 33(2p + 1)$ for some integer p. The bounds here are not redundant, so $20 < x < 79$. The only multiples of 33 in this region are 33 and 66. Both have digits whose sums are even (divisible by two). So there are two possible results.

Part c. Translating this is not quite as useful, giving

$$\begin{aligned}
&x = 2k \text{ for some } k,\\
&x = 3j_1 + i_1 \text{ for some } j \text{ and } i \neq 0,\\
&x = 4j_1 + i_1 \text{ for some } j \text{ and } i \neq 0,\\
&x \leq 81, \text{ and}\\
&x \geq 64.
\end{aligned}$$

One observation helps: An even number not divisible by four has only one factor of 2. So the first and third requirements become

$$x = 2 \cdot (2p + 1) \text{ for some } p.$$

So we are looking for *even* numbers in $64 \leq x \leq 80$ with only one factor of two and that are not multiples of three. This reduces to looking for an odd $z = x/2$ in $32 \leq x \leq 40$ that is not a multiple of three.

The odd non-multiples of three in this range are 35 and 37. So z is either 35 or 37, and x is either 70 or 74.

10.4.2 Logic puzzle: Problem 9

The problem assumes neither bigamy nor marriage to immediate relations is allowed, which is reasonable in the US. The true (T) and false (F) values are subscripted by a number if they are a direct implication of that rule. The forth rule was useless.

	Kitty	Sarah	Josie	Anne
David	F_3	F_5	T	F
Will	F_3	T_5	F_1	F_5
Floyd	F_3	F_5	F_2	T
Gus	T_3	F_3	F_3	F_3

10.4.3 Pigeonholes: Problem 12

Part a. To fill 365 days and guarantee one is repeated, you need 366 people. As an amazing aside, though, with only 23 people the chance of two sharing a birthday is over 50%!

Part b. The result here is twice 365 plus one, or 731.

10.4.4 Pigeonholes: Problem 13

There are only ten units digits possible, zero through nine. If one digit is repeated, the difference between the two numbers with the same units digit must have units digit zero and be divisible by ten. With eleven numbers, we must have two with the same units digit.

10.4.5 Pigeonholes: Problem 14

Part a. Note there are six ways single-digit numbers (or the units digit) can add to ten, $1 + 9$, $2 + 8$, $3 + 7$, $4 + 6$, and $5 + 5$. If we use those as pigeonholes for the units digit, then we know one of those holes must be filled twice with seven numbers. Now *within* the holes we have another set of holes with one hole for each digit. If both holes are filled, then the sum is divisible by ten. If only one hole is filled, then the numbers share a units digit and their difference is divisible by ten.

Part b. With six numbers, we can fill each hole once. Any consecutive sequence of six numbers suffice, *e.g.* 1, 2, 3, 4, 5, 6.

10.5 Inductive or deductive?

- It has rained for the past week. It will rain tomorrow.

  This is *inductive* because it is based solely on repeated observations.

- All men are mortal. Socrates is a man. Therefore, Socrates is mortal.

  Deductive reasoning begins with premises and draws a conclusion as in this example.

- Satellite-based network access does not function through heavy rain. It is raining heavily. I cannot upload the notes right now.

  Again, this example sets up data and rules from which it draws a conclusion. This is *deductive* reasoning.

- The next number after 3, 8, 13, 18, and 23 is 28.

  This could fall either way, depending on how you decide on the next number. If you assume this is an arithmetic sequence and calculate the next term, this could be considered *deductive* reasoning. Recognizing an arithmetic sequence without further information is inductive in itself. If you just look and see a pattern, the process is completely *inductive*.

  Often the initial phase of problem solving, understanding the problem, is an exercise in reasoning inductively.

Chapter 11

Notes for 1 September

Notes also available as PDF.

11.1 Review

Two key forms of reasoning in mathematics:

Inductive Making a guess from prior observations.

Deductive If premises are satisfied, conclusion follows.

Typically,

problems to find use inductive reasoning, and

problems to prove apply deductive reasoning.

But *finding a proof* is in many ways inductive.

Problem solving so far has been inductive. Take example problems and their solutions. Emulate the solutions on similar problems.

Remember to take great care with the premises in both forms of reasoning!

- Inductive reasoning *generalizes* from examples.
- If the examples are not appropriate, the result will be incorrect.

Mathematics is representative reasoning.

- We model the real world and represent pieces of it with symbols (numbers, letters, digits, *etc.*).
- Then we reason about how the symbols interact.
- Only takes a few rules to build a massive system.

- Amazingly, the system often mimics some aspect of the real world.

11.2 Proof

1. You start with a guess, possibly after seeing a pattern.
2. A few tests, and the guess becomes a conjecture.
3. Once the conjecture is proven, you have a theorem.
    - A lemma is a theorem leading to other theorems. Typically a *technical* result leading to the main theorem.
    - A corollary is a subsequent theorem, a simple result after a primary theorem.

Other items:

- Definitions are difficult to define.
- Axioms are *fundamental* definitions. The classic example:

  Two points define a line.

11.3 Direct proof

Example 1.16 from the text:

Theorem: If n is a non-negative integer, then n^2 is either a multiple of 4 or one larger than a multiple of 4.

(A whole number is a non-negative integer.)

What are we trying to show? Rephrasing with mathematical symbols, we want to prove that for every non-negative integer n there is some integer k where $n^2 = 4k$ or $n^2 = 4k + 1$.

To prove this, it doesn't matter what k is for a given n or which of the two terms apply. For simpler forms like these, however, it's often useful to *construct* the result.

Initial exploration.

What else? Build a little table.

n	n^2	form
0	0	$4 \cdot 0$
1	1	$4 \cdot 0 + 1$
2	4	$4 \cdot 1$
3	9	$4 \cdot 2 + 1$
4	16	$4 \cdot 4$
5	25	$4 \cdot 6 + 1$

Recognize a pattern: Evens have one form, odds another. This breaks the problem into two cases.

If n is even, then $n = 2i$ for some integer i. Then $n^2 = 4i$ and $k = i$.

If n is odd, then $n = 2i+1$ for some integer i. Then $n^2 = (2i+1)^2 = 4i^2+4i+1 = 4(i^2 + i) + 1$ and $k = i^2 + i$.

To summarize, we have proven the following:

> If n is a non-negative integer, then n^2 is either $4i$ or $4(i^2 + i) + 1$ for some integer i.

11.4 Proof by contrapositives

Sometimes called indirect reasoning, often called proof by contradiction. Purists hate that phrase.

Logically, if p then q is equivalent to if not q then not p. This is the *contrapositive*.

Thus if you prove that the negation of your conclusion q implies the negation of your hypothesis p, you have proven that your hypothesis p implies the conclusion q. Clear? No? This is why the method often is called proof by contradiction. That route is often easier to understand.

For a demonstration, remember the definition of a prime number. A prime is an integer $p \neq 1$ that only can be divided cleanly by 1 and p itself.

Theorem: There are infinitely many prime numbers.

Proof: Suppose there is some largest prime P. Then form the (very large) integer $Q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot P + 1$, one larger than the product of all primes. Now Q is not divisible by any prime, so Q must itself be prime. But Q is larger than P, contradicting the assumption that P is the largest prime. □

What have we actually proven? If there is a largest prime P, then there is a larger prime Q. Thus, there can be no largest prime.

(The symbol □is one traditional ending for a proof. It is used instead of the letters *QED*, for *quod erat demonstrandum*. Literally it means "that which was to be demonstrated.")

The text's Example 1.17 is another very nice example of this style.

11.5 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Prove the formula for the sum of the first n positive integers by mathematical induction. That is, prove $1 + 2 + 3 + \cdots + n = n(n+1)/2$. The base case here is $n = 1$. Then show that the n^{th} term transforms into the $(n+1)^{\text{th}}$ term by adding $n + 1$.

Note that you *may* email homework. However, I don't use Microsoft$^{\text{TM}}$ products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 12

Notes for 3 September

Notes also available as PDF.

12.1 Proof review

1. You start with a guess, possibly after seeing a pattern.
2. A few tests, and the guess becomes a conjecture.
3. Once the conjecture is proven, you have a theorem.
    - A lemma is a theorem leading to other theorems. Typically a *technical* result leading to the main theorem.
    - A corollary is a subsequent theorem, a simple result after a primary theorem.

Other items:

- Definitions are difficult to define.
- Axioms are *fundamental* definitions. The classic example:

    Two points define a line.

A *direct proof* takes the given hypotheses and applies rules directly to produce the conclusion. We used a direct proof to show that n^2 is either a multiple of four (can be written as $4k$ for some k) or one larger than a multiple of four $(4k + 1)$ when n is a non-negative integer.

An *indirect proof*, often called *proof by contradiction* or *proof by contrapositive*, proves that the opposite of the conclusion implies the opposite of the hypothesis. Thus if the hypothesis is true, the conclusion must be true. We used proof by contradiction to show that there are infinitely many primes. We actually proved

that if there is a largest prime, then there is a larger number not divisible by any known prime and thus prime itself. The contradiction, constructing a prime larger than the largest prime, proved that there is no largest prime. Along with the known existence of primes, the fact there is no largest prime implies there must be infinitely many primes.

12.2 Inductive proof

Remember Pascal's triangle? We proved that the sum of the n^{th} row is 2^n if we start counting rows from zero.

Written in rather boring table form, each entry is the sum of the entry directly above and above to the left:

#					
0	1				
1	1	1			
2	1	2	1		
3	1	3	3	1	
4	$1 = \mathbf{0} + 1$	$4 = 1 + 3$	$6 = 3 + 3$	$4 = 3 + 1$	$1 = 1 + \mathbf{0}$

We will use our result as an example of *mathematical induction*. This is a proof technique that formalizes inductive reasoning and using a representative case.

1. Start with verifying a *base case*.
2. Then assume the n^{th} case.
3. Use that to prove the $(n+1)^{\text{st}}$ case.

We want to prove the following:

Theorem: The sum of the n^{th} line of Pascal's triangle is 2^n.

Proof:

Here, the base case is the 0^{th} line:

#		sum
0	1	$1 = 2^0$

Then let line n be the sequence

#						sum
n	$P_{n,1}$	$P_{n,2}$	$P_{n,3}$	$\cdots$	$P_{n,n+1}$	2^n

Now we need to prove that line $(n+1)$ holds true. In our notation, item j^{th} on line $(n+1)$ is formed be $P_{n+1,j} = P_{n,j-1} + P_{n,j}$, setting the entries outside the table ($P_{n,0}$ and $P_{n,n+2}$) to zero.

Then we need to show that $\sum_{j=1}^{n+2} P_{n+1,j} = 2^{n+1}$.

$$\begin{aligned}
\sum_{j=1}^{n+2} P_{n+1,j} &= \sum_{j=1}^{n+2} (P_{n,j-1} + P_{n,j}) \\
&= \sum_{j=1}^{n+2} P_{n,j-1} + \sum_{j=1}^{n+2} P_{n,j} \\
&= \left(P_{n,0} + \sum_{j=1}^{n+1} P_{n,j} \right) + \left(P_{n,n+2} + \sum_{j=1}^{n+1} P_{n,j} \right) \\
&= \sum_{j=1}^{n+1} P_{n,j} + \sum_{j=1}^{n+1} P_{n,j} \\
&= 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.
\end{aligned}$$

□

12.3 Starting with set theory

Our coverage of set theory mostly will cover definitions. We will use some concepts to work with problem solving and to illustrate proofs. Then we will use sets to build up whole numbers (0, 1, 2, ...) and basic arithmetic on those numbers.

12.4 Language of set theory

- We will cover just enough set theory to use later.
- Cardinalities are important for probability. We don't have time to cover probability sufficiently well, so we will not explore the sizes of sets deeply.
- This is known as naïve set theory. We do not define absolutely everything, nor do we push set theory's logical limits. Much.

Goals:

- Impart some of the language necessary for later chapters.
- Practice reasoning in a formal setting.
  - One key aspect is what to do in extreme cases like empty sets.
- Set up straight-forward examples for logic.

12.5 Basic definitions

To start, we require unambiguous definitions of terms and items. When a term or item is unambiguously defined, it is called *well-defined*.

set An *unordered* collection of *unique* elements.

- Curly braces: $\{A, B, C\}$ is a set of three elements, A, B, and C.
- Order does not matter: $\{\text{cat}, \text{dog}\}$ is the same set as $\{\text{dog}, \text{cat}\}$.
- Repeated elements do not matter: $\{1, 1, 1\}$ is the same set as $\{1\}$.
- Can be *implicit*: $\{x \mid x \text{ is an integer}, x > 0, x < 3\}$ is the same set as $\{1, 2\}$.
- Read the implicit form as "the set of elements x *such that* x is an integer, $x > 0$, and $x < 3$". Or "the set of elements x *where* ..."
- Other symbols that sometimes stand for "such that": :, $\ni$ (reversed $\in$)
- Implicit (or set-builder) form can include formula or other bits left of the bar. $\{3x \mid x \text{ is a positive integer}\}$ is the set $\{3, 6, 9, \ldots\}$.

element Any item in a set, even other sets. (Also entry, member, item, *etc.*)

- This is not ambiguous. If something is in a set, it is an item of that set. It doesn't matter if the item is a number or a grape.
- $\{A, \{B, C\}\}$ is a set of *two* elements, A and $\{B, C\}$.
- None of the following are the same: $\{A, \{B, C\}\}$, $\{A, B, C\}$, $\{\{A, B\}, C\}$.

empty set Or null set. Denoted by $\emptyset$ rather than $\{\}$.

- This is a *set* on its own.
- $\{\emptyset\}$ is the set of the empty set, which is not empty.
- Think of sets as bags. An empty bag still is a bag, and if a bag contains an empty bag, the outer bag is not empty.
- Implicit definitions can hide empty sets.
- For example, the set $\{x \mid x \text{ is an odd integer divisible by } 2\}$ is $\emptyset$.

singleton A set with only one element.

- $\{1\}$ and $\{\emptyset\}$ both are singletons (or sometimes singleton sets).

12.6 Translating sets into (and from) English

From English:

- The days of the week:
  - $\{\text{Monday}, \text{Tuesday}, \text{Wednesday}, \text{Thursday}, \text{Friday}, \text{Saturday}, \text{Sunday}\}$
  - Of course, we're using a *representation* of the days and not the days themselves. That is how we reason about things; we model them and represent them by symbols.
- The days when homework is due:
  - $\{25^{\text{th}}$ of August, 1^{st} of September, $\ldots\}$
  - We *could* list them all.
  - { every Monday after the 18^{th} of August 2008 until after the 1^{st} of December }
  - Or: $\{x \mid x$ is a Monday, x is after the 18^{th} of August, and x is on or before the 1^{st} of December }

To English:

- $\{2, 3, 4\}$:
  - The set containing two, three, and four.
- $\{x \mid x \text{ is an integer and } x > 0\}$:
  - The positive integers, also called the counting numbers or the natural numbers.
  - Often written as $\mathbb{J}^+$. The integers often are written as $\mathbb{J}$ (because the "I" form can be difficult to read), rationals as $\mathbb{Q}$ (for quotients), the reals as $\mathbb{R}$.
- $\{2x - 1 \mid x \in \mathbb{J}^+\}$
  - The set whose members have the form $2x - 1$ where x is a positive integer.
  - Cannot list all the entries; this is an *infinite* set.
  - Here, the odd integers.

12.7 Next time: Relations between and operations on sets

12.8 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Prove the formula for the sum of the first n positive integers by mathematical induction. That is, prove $1 + 2 + 3 + \cdots + n = n(n + 1)/2$. The base case here is $n = 1$. Then show that the n^{th} term transforms into the $(n + 1)^{\text{th}}$ term by adding $n + 1$.
- Problem set 2.1 (p83):
  - Problems 1, 2, 4, 5, 6, 27

Note that you *may* email homework. However, I don't use Microsoft$^{\text{TM}}$ products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 13

Notes for 8 September

Notes also available as PDF.

13.1 Review

set An *unordered* collection of *unique* elements.

- Curly braces: $\{A, B, C\}$ is a set of three elements, A, B, and C.
- Can be *implicit* or in *set builder notation*: $\{x \mid x \text{ is an integer}, x > 0, x < 3\}$ is the same set as $\{1, 2\}$.
- Order does not matter, repeated elements do not matter.

element Any item in a set, even other sets. (Also entry, member, item, *etc.*)

empty set Or null set. Denoted by $\emptyset$ rather than $\{\}$.

- This is a *set* on its own.
- $\{\emptyset\}$ is the set of the empty set, which is not empty.

singleton A set with only one element.

13.2 Relations and Venn diagrams

(Someday I will include Venn diagrams for these in the notes.)

element of The expression $x \in A$ states that x is an element of A. If $x \notin A$, then x is *not* an element of A.

- $4 \in \{2, 4, 6\}$, and $4 \notin \{x \mid x \text{ is an odd integer }\}$.

- There is no x such that $x \in \emptyset$, so $\{x \mid x \in \emptyset\}$ is a long way of writing $\emptyset$.

subset If all entries of set A also are in set B, A is a subset of B.

superset The reverse of subset. If all entries of set B also are in set A, then A is a superset of B.

proper subset If all entries of set A also are in set B, but some entries of B are *not* in A, then A is a *proper* subset of B.

- $\{2, 3\}$ is a proper subset of $\{1, 2, 3, 4\}$.

equality Set A equals set B when A is a subset of B and B is a subset of A.

- Order does not matter. $\{1, 2, 3\} = \{3, 2, 1\}$.

The symbols for these relations are subject to a little disagreement.

- Many basic textbooks write the subset relation as $\subseteq$, so $A \subseteq B$ when A is a subset of B. The same textbooks reserve $\subset$ for the *proper* subset. Supersets are $\supset$.
- This keeps a superficial similarity to the numerical relations $\leq$ and $<$. In the former the compared quantities may be equal, while in the latter they must be different.
- Most mathematicians now use $\subset$ for any subset. If a property requires a "proper subset", it often is worth noting specifically. And the only non-"proper subset" of a set is the set itself.
- Extra relations are given for emphasis, *e.g.* $\subsetneq$ or $\subsetneqq$ for proper subsets and $\subseteq$ or $\subseteqq$ to emphasize the possibility of equality.
- Often a proper subset is written out: $A \subset B$ and $A \neq B$.
- **I'll never remember to stick with the textbook's notation. My use of $\subset$ is for subsets and not proper subsets.**

13.3 Translating relations into (and from) English

From English:

- The train has a caboose.
  - It's reasonable to think of a train as a set of cars (they can be reordered).
  - The cars are the members.
  - Hence, caboose $\in$ train

- The VI volleyball team consists of VI students.
  - VI volleyball team $\subset$ VI students
- There are no pink elephants.
  - pink elephants $= \emptyset$

To English:

- $x \in$ today's homework set.
  - x is a problem in today's homework set.
- Today's homework $\subset$ this week's homework.
  - Today's homework is a subset of this week's homework.

13.4 Consequences of the set relation definitions

Every set is a subset of itself. Expected.

If $A = B$, then every member of A is a member of B, and every member of B is a member of A. This is what we expect from equality, but we did not define set equality this way. Follow the rules:

- $A = B$ imples $A \subset B$ and $B \subset A$.
- Because $A \subset B$, every member of A is a member of B.
- Because $B \subset A$, every member of B is a member of A.

The empty set $\emptyset$ is a subset of all sets. Unexpected! This is a case of carrying the formal logic to its only consistent end.

- For some set A, $\emptyset \subset A$ if every member of $\emptyset$ is in A.
- But $\emptyset$ has no members.
- Thus all of $\emptyset$'s members also are in A.
- This is called a *vacuous* truth.

The alternatives would not be consistent, but proving that requires more machinery that we need.

13.5 Operations

union The *union* of two sets A and B, denoted by $A \cup B$, is the set consisting of all elements from A and B.

- $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

- Remember repeated elements do not matter: $\{1,2\} \cup \{2,3\} = \{1,2,3\}$.

intersection The *intersection* of two sets A and B, denoted $A \cap B$, is the set consisting of all elements that are in *both* A and B.

- $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
- $\{1,2\} \cap \{2,3\} = \{2\}$.
- $\{1,2\} \cap \{3,4\} = \{\} = \emptyset$.

set difference The *set difference* of two sets A and B, written $A \setminus B$, is the set of entries of A that are not entries of B.

- $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$.
- Sometimes written as $A - B$, but that often becomes confusing.

If A and B share no entries, they are called *disjoint*. One surprising consequence is that every set A has a subset disjoint to the set A itself.

- No sets (not even $\emptyset$) can share elements with $\emptyset$ because $\emptyset$ has no elements.
- So all sets are disjoint with $\emptyset$.
- The empty set $\emptyset$ is a subset of all sets.
- So all sets are disjoint with at least one of their subsets!

Can any other subset be disjoint with its superset? *No.*

13.6 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Problem set 2.1 (p83):
  - Problems 7, 8, 10, 20, 24

Note that you *may* email homework. However, I don't use Microsoft™ products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 14

Solutions for third week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

14.1 Induction: Sum of first n integers

> Prove the formula for the sum of the first n positive integers by mathematical induction. That is, prove $1+2+3+\cdots+n = n(n+1)/2$. The base case here is $n = 1$. Then show that the n^{th} term transforms into the $(n+1)^{\text{st}}$ term by adding $n+1$.

Theorem: Let n be a positive integer. Then the sum of the first n positive integers is

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof: We proceed by induction. First note that

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}.$$

Now assume that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

We must show that

$$\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}.$$

To proceed, we pull the $n+1$ term out of the sum to see that

$$\sum_{i=1}^{n+1} i = n+1+\sum_{i=1}^{n} i = (n+1)+\frac{n(n+1)}{2}.$$

Then we factor out $n+1$ and simplify to obtain

$$\begin{aligned}(n+1)+\frac{n(n+1)}{2} &= (n+1)\left(1+\frac{n}{2}\right)\\ &= (n+1)\frac{2+n}{2}\\ &= \frac{(n+1)(n+2)}{2},\end{aligned}$$

proving the result. □

14.2 Problem set 2.1 (p83)

14.2.1 Problem 1

Wikipedia can be very useful.

Part a. {California, Oregon, Idaho, Utah, Arizona}. (Note that we could include Nevada; it certainly shares a border with itself.)
Part b. {Mississippi, Missouri, Maine, Montana, Maryland, Massachusetts, Michigan, Minnesota}
Part c. {Arizona}

(Thanks to Chris Fields for pointing out the states I missed.)

14.2.2 Problem 2

Part a. {a, c, e, h, i, l, m, n, o, s, t, y}, possibly including capital "L" if you treat that as a separate letter.
Part b. {a, e, m, t}.

14.2.3 Problem 4

Many answers are reasonable.

Part a. $\{x|x \in \mathbb{J}, 10 < x < 15\}$, or perhaps $\{10 + i|i \in \mathbb{J}, 0 < i < 5\}$.
Part b. $\{2i|i \in \mathbb{J}, 3 \leq i \leq 8\}$.
Part c. $\{4 + 4i|i \in \mathbb{J}, 0 \leq i < 5\}$.
Part d. $\{i^2 + 2i + 2|i \in \mathbb{J}, 0 \leq i < 4\}$ or
$\{1 + i|i =$ the sum of the first j positive odd integers where $j \leq 4\}$

14.2.4 Problem 5

Many answers are reasonable.

Part a. $\{2i|i \in \mathbb{J}, i > 6\}$.
Part b. $\{(2i + 1)^2|i \in \mathbb{J}, i \geq 12\}$.
Part c. $\{3i|i \in \mathbb{J}^+\}$

14.2.5 Problem 6

Part a. No, there are many cities with each name.
Part b. Yes, the cities are specific. There is only one Idaho, Montana, or Texas in the world. There are two Georgias, but only one has a town called Duluth. (The other Georgia does not use the same alphabet, but I am pretty sure no town there transliterates to Duluth.)
Part c. No, there is no universal measure of "smart".
Part d. Yes, this is specific. However, this likely is empty. How many people have a GPA of *exactly* 3.5? If you have an odd number of credits, that is not possible. And if you have an even number, you would have to have exactly as many As as Bs.

14.2.6 Problem 27

These are just my rambling responses.

A *set of china* is a collection of dishware. However, there are many repeated elements that are identical (until chipped), so this is not entirely a mathematical set. If you label each piece, however, then each element has its own identity and you do have a set.

In a *family*, pretty much everyone has their own identity and is not repeated, even if they are twins. So families could be considered sets. If you rank the family by age or otherwise, the ranked family is *ordered* and thus not a set.

An *aggregate* in my mind is a summary and not a listing, but I'm poisoned by programming. So to me, an aggregate is a function you apply to a set to find a value. For example, the mean or the median is an aggregate. But I'm sure there are other uses.

A *class* in a class room definitely is a set. Each member is unique and identifiable. And by the time there is a final ranking (grade), the class is over. Mathematically, however, *class* means something beyond *set*. The collection of all sets is a class and not a set; no set can contain itself as an element.

In my wife's *collection* of antique sewing machines, each is identifiable and appears unique. Thus, a set.

Chapter 15

Notes for 10 September

Notes also available as PDF.

15.1 Review

15.1.1 Definitions

set An *unordered* collection of *unique* elements.

element Any item in a set, even other sets. (Also entry, member, item, *etc.*)

empty set Or null set. Denoted by $\emptyset$ rather than $\{\}$.

singleton A set with only one element.

15.1.2 Relations

element of The expression $x \in A$ states that x is an element of A. If $x \notin A$, then x is *not* an element of A.

subset $A \subset B$ if all entries of set A also are in set B.

superset The reverse of subset. $B \supset A$ when $A \subset B$.

proper subset If all entries of set A also are in set B, but some entries of B are *not* in A, then A is a *proper* subset of B.

equality $A = B$ when $A \subset B$ and $B \subset A$.

15.1.3 Operations

union $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

intersection $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

set difference $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$.

complement and universe The complement of a set **with respect to a given universal set U** is the set $A^c = U \setminus A = \{x \mid x \in U \text{ and } x \notin A\}$. Sometimes written $\overline{A}$ or A'. Take care with the universal set; there is no "universal" universal set.

15.2 From sets to whole numbers

Now we'll show how to construct whole numbers from sets.

nominal A number used for *indentification*, like your student ID.

ordinal A number used for *ordering*, as in first, second, *etc.*

cardinal A number that *counts* the number of entries in some set.

We are moving into *counting* elements of sets. This can extend into probability and other topics, but for now we are interested just in counting and numbers.

Two more definitions are useful:

one-to-one correspondence Two sets A and B are in one-to-one correspondence if there is a pairing of elements (a, b) such that each $a \in A$ and $b \in B$ belongs to exactly one pair. The pairing is also called a *bijection*.

equivalent sets Two sets A and B are equivalent if they are in one-to-one correspondence. We write $A \sim B$ for equivalence and $A \not\sim B$ for non-equivalence.

So what do equivalent sets share? Consider establishing a one-to-one correspondence between two sets A and B. If the sets do not have the same number of elements, then at least one element will not be paired. Remember indirect proof, or proof by the contrapositive? We have just *proven* that all equivalent sets have the same number of elements.

The number of elements is a rather important property and gains its own notation:

cardinality Writen $|A|$, or rarely $n(A)$, the *cardinality* of A is the number of elements in A. So $|\{a, b, 7\}| = 3$.

We now have a link from the *cardinality* of sets to *cardinal* integers ≥ 0. These are the **whole numbers**. Moreover, now we can *construct* the whole numbers. Starting from the unique empty set, $|\emptyset| = 0$.

Define an operation $S(x) = x \cup \{x\}$. This is the **successor function**. Then $S(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$, a set with one element. Continue applying the successor to see:

$\emptyset$	$\lvert\emptyset\rvert$	0	
$S(\emptyset)$	$\lvert\{\emptyset\}\rvert$	1	$\{0\}$
$S(S(\emptyset))$	$\lvert\{\emptyset, \{\emptyset\}\}\rvert$	2	$\{0, 1\}$
$S(S(S(\emptyset)))$	$\lvert\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\rvert$	3	$\{0, 1, 2\}$

By applying the successor function n times to the empty set, we obtain a set of cardinality n. Starting from nothing (literally, $\emptyset$), we obtain the whole numbers! This is a construction from Giuseppe Peano, a 19th century Italian mathematician. After the association between $\emptyset$ and 0, we identify the number k with the set of all numbers preceding k.

The text has examples of building numbers with different physical gizmos. It's worth thinking about the 2-D block idea, particularly in regards to factors and factorization. Here, you could imagine S as adding one more unit onto a line. Starting from a point, $\emptyset$, applying S grows the numbers one at a time.

We also can impose an ordering on these numbers. Given two sets A and B with $|A| = a$ and $|B| = b$, we say that $a < b$ if A is equivalent to some *proper* subset of B, or $A \sim C$ where $C \subsetneq B$. We say $a \leq b$ if A is equivalent to some subset of B.

Now we also can see the difference between **finite** sets and the concept of **infinite** sets. A finite set is equivalent to some number of successor applications to the empty set. You can count finite numbers.

An infinite set, however, is equivalent to no number of successor applications. If it were, we could add one more to have a larger set. There are different kinds of infinities, but we won't worry about that right now. And note that you can have a one-to-one correspondence between infinite sets. For example, $\{x \mid x \in \mathbb{J}^+\}$ has a one-to-one correspondence with $\{\frac{1}{x} \mid x \in \mathbb{J}^+\}$. Each integer in the first set is matched with exactly one in the second set.

15.3 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Problem set 2.2 (p97):
  - Problems 1, 2, 6, 13, 21, 23
  - Why would answering problem 32 be a bad idea?

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 16

Notes for 12 September

Notes also available as PDF.

16.1 Review

nominal A number used for *indentification*, like your student ID.

ordinal A number used for *ordering*, as in first, second, *etc.*

cardinal A number that *counts* the number of entries in some set.

one-to-one correspondence Two sets A and B are in one-to-one correspondence if there is a pairing of elements (a, b) such that each $a \in A$ and $b \in B$ belongs to exactly one pair. The pairing is also called a *bijection*.

equivalent sets Two sets A and B are equivalent if they are in one-to-one correspondence. We write $A \sim B$ for equivalence and $A \not\sim B$ for non-equivalence.

cardinality Writen $|A|$, or rarely $n(A)$, the *cardinality* of A is the number of elements in A. So $|\{a, b, 7\}| = 3$.

We now have a link from the *cardinality* of sets to *cardinal* integers ≥ 0. These are the **whole numbers**. Moreover, now we can *construct* the whole numbers. Starting from the unique empty set, $|\emptyset| = 0$.

Define an operation $S(x) = x \cup \{x\}$. This is the **successor function**. Then $S(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$, a set with one element. Continue applying the successor to see:

$\emptyset$	$\lvert\emptyset\rvert$	0	
$S(\emptyset)$	$\lvert\{\emptyset\}\rvert$	1	$\{0\}$
$S(S(\emptyset))$	$\lvert\{\emptyset,\{\emptyset\}\}\rvert$	2	$\{0,1\}$
$S(S(S(\emptyset)))$	$\lvert\,\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}\,\rvert$	3	$\{0,1,2\}$

After the association between $\emptyset$ and 0, we identify the number k with the set of all numbers preceding k. Thus we follow Guiseppe Peano's construction of the whole numbers from nothing but sets.

finite set Equivalent to some number of successor applications $S()$ to the empty set.

infinite set Cannot be equivalent to *any* number of successor applications, as we could apply once more to obtain a larger set.

16.2 Addition of whole numbers

So how do we define addition? The text has one method that assumes A and B are disjoint. That is, $A \cap B = \emptyset$. Then $|A \cup B| = |A| + |B|$, so we could define addition by the cardinality of a union of disjoint sets.

It's worth a brief detour to discuss what happens to the cardinality when the sets are *not* disjoint. This is a tool used frequently in probability.

$|\{a,b\} \cup \{c,d\}| = |\{a,b,c,d\}| = 4$, where $|\{a,b\}| = |\{c,d\}| = 2$. If they share an element, though, the union's cardinality still is four. $|\{a,b,c\} \cup \{c,d\}| = |\{a,b,c,d\}| = 4$. But now $|\{a,b,c\}| = 3$.

The rule for counting elements for a union of two sets is $|A \cup B| = |A| + |B| - |A \cap B|$. The first two terms count shared elements twice, and the last term removes one of those. For three terms, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$, where you add back in elements you removed too many times.

But for general addition, we start by defining $a + 0 = a$ using $A \cup \emptyset = A$ as a guide. Then we define addition for other numbers recursively by

$$a + 0 = a, \text{ and}$$
$$a + S(b) = S(a + b).$$

So $a + 1 = a + S(0) = S(a + 0) = S(a)$, the successor of a. If we think of $S(b)$ as $b + 1$, then the second rule is $a + (b + 1) = (a + b) + 1$.

A small example working through the recursive definition:

$$\begin{aligned} 1 + 2 &= 1 + S(1) \\ &= S(1 + 1) \\ &= S(1 + S(0)) \\ &= S(S(1 + 0)) \\ &= S(S(1)) \\ &= S(2) \\ &= 3. \end{aligned}$$

Obviously, we don't want to work through many of these.

So we define addition as decomposing one number into its sequence of successors and then applying those successors. For the line model, we extend one line by the length of the other.

Some properties of addition on whole numbers:

closure If a and b are two whole numbers, $a + b$ is a whole number. Whole numbers are closed over addition.

commutative $a + b = b + a$

associative $a + (b + c) = (a + b) + c$

identity $a + 0 = a$

Each of these is straight-forward to prove using the text's model of unions of disjoint sets. Working with Peano arithmetic is trickier but possible.

Terminology: The terms being added are called **addends** or **summands**.

16.3 Subtraction of whole numbers

Subtraction is the first property we will define *implicitly*. The difference of a and b, written $a - b$, is defined to be the whole number c where $a = b + c$. If no such c exists, then subtraction is not defined. There is no integer $c \geq 0$ such that $1 = 5 + c$, so $1 - 5$ is not defined.

Thus subtraction is **not closed** over the whole numbers. It also is **not commutative** and **not associative**. However, because $a + 0 = a$, we know that $a - 0 = a$. Thus subtraction does have an identity on one side. However, $0 - a$ is not defined unless $a = 0$. There is no c such that $0 = a + c$ unless $a = c = 0$.

Terminology: In $a - b$, a is the **minuend** and b is the **subtrahend**.

16.4 Multiplication of whole numbers

We are accustomed to thinking of multiplication as repeated addition. For example, $4a = a + a + a + a$. Or we can rearrange the repeated addition as in $4a = a + 3a = a + (a + 2a) = a + (a + (a + a))$. This arrangement provides the recursive definition of multiplication:

$$\begin{aligned} a \cdot 0 &= 0, \text{ and} \\ a \cdot S(b) &= a + (a \cdot b) \end{aligned}$$

Again, thinking of $S(b)$ as $b + 1$, $a \cdot (b + 1) = a + (a \cdot b)$. We pull apart one side into a sequence of ones and repeatedly add the other side.

We will jump ahead and assume multiplication is commutative. So write the example of $4a$ as $a \cdot 4$:

$$\begin{aligned} a \cdot 4 &= a \cdot S(3) \\ &= a + (a \cdot S(2)) \\ &= a + (a + a \cdot S(1)) \\ &= a + (a + (a + a \cdot S(1))) \\ &= a + (a + (a + (a + a \cdot 0)) \\ &= a + a + a + a + 0. \end{aligned}$$

And with this recursive definition,

$$\begin{aligned} a \cdot 1 &= a \cdot S(0) \\ &= a + (a \cdot 0) \\ &= a + 0 = a, \end{aligned}$$

and one is the **multiplicative identity**.

Defining multiplication in terms of repeated addition lets multiplication inherit the **closure** property. The product $a \cdot b$ exists and is a whole number for every pair of whole numbers a and b. And we could push through and show that multiplication is **commutative** and **associative**. Another less formal model makes these properties more clear, however.

A quick note on terminology: In $15 = 5 \cdot 3$, 15 is the **product**, and five and three are **factors**. The term *factor* only applies to integers. Two other terms applied to the operands (5 and 3) in the context of repeated addition are **multiplicand** and **multiplier**. If you consider $15 = 5 \cdot 3 = 5+5+5$, then five is the multiplicand and three is the multiplier. These terms still are used when building multiplier circuits. One term, the multiplicand, is shifted and added according to the multiplier. We will return to this later.

But for the less formal models, consider multiplication of two numbers as tracing out areas and volumes.

The drawing can have its axes flipped around without changing the area. Thus, $ab = ba$ and multiplication is commutative.

For the associative property, consider a volume traced out by three numbers. Putting parenthesis in different places is the same as counting in different directions, but the final count always is the same. Thus multiplication is associative.

There is one additional property that combines addition and multiplication: the **distributive** property. Here $a(b+c) = ab+ac$. Drawing a box and separating it into two pieces demonstrates the distributive property well. Thinking of repeated addition here also is simple. We have either $b + c$ copies of a, or b copies of a added to c copies.

16.5 Monday: Division and exponentials

I need to cover these still. They provide examples of *undefined* behavior; it's worth exploring that a bit.

To be followed by a little review.

16.6 Homework

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

Write out (briefly) your approach to each problem.

- Problem set 2.3 (p111):
  - 2, 5, 11, 24
- Write $2 + 3$ using disjoint sets.
- Illustrate $2 + 3$ using Peano arithmetic.
- Problem set 2.4 (p130):
  - 5, 10
  - 26
- Illustrate $2 \cdot 3$ using Peano arithmetic. You do not need to expand addition.
- Illustrate $(1 \cdot 2) \cdot 3 = 1 \cdot (2 \cdot 3)$ using a volume of size six.

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 17

Solutions for fourth week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

17.1 Problem set 2.2

17.1.1 Problem 1

(a) June 13^{th}: nominal, first: ordinal

(b) eleventh: ordinal, second: ordinal, 6-iron: nominal, 160 yards: cardinal

(c) 7 pin: nominal, sixth frame: ordinal, 9: cardinal

17.1.2 Problem 2

(a) There are five letters in the phrase, {P,A,N,M,B}, so we can associate $1 \leftrightarrow$ P, $2 \leftrightarrow$ A, *etc.* The two sets are **equivalent**.

(b) The second set has one more element than the first, so the sets are **not equivalent**.

(c) We can associate $o \leftrightarrow t$, $n \leftrightarrow w$, and $e \leftrightarrow o$, where the left quantities come from $\{o, n, e\}$ and the right from $\{t, w, o\}$. The two sets are **equivalent**.

(d) $\{0\}$ has in element, and $\emptyset$ has none, so the sets are **not equivalent**.

17.1.3 Problem 6

(a) We can use the function $f(w) = w + 1$ to construct a bijection between W and N.

(b) The function $f(d) = d + 1$ creates a one-to-one mapping between D and E.

(c) The function $f(n) = 10^n$ creates a one-to-one mapping between N and $\{10, 100, \ldots\}$.

17.1.4 Problem 13

The drawing will have

- $|B \cap C| - |A \cap B \cap C| = 5$ in the unlabeled portion of $B \cap C$,
- $|B| - |A \cap B| - |B \cap C| + |A \cap B \cap C| = 28$ in the remaining unlabeled portion of B,
- $|A \cap C| - |A \cap B \cap C| = 8$ in the unlabeled portion of $A \cap C$,
- $|A| - |A \cap B| - |A \cap C| + |A \cap B \cap C| = 15$ in the remaining unlabeled portion of A,
- $|C| - |B \cap C| - |A \cap C| + |A \cap B \cap C| = 10$ in the remaining unlabeled portion of C, and
- $|U| - (10 + 7 + 5 + 28 + 8 + 15 + 10) = 17$ in U but outside A, B, and C.

17.1.5 Problem 21

(a) The function $f(a) = a$ is the one-to-one correspondence from A to itself.

(b) If $A \sim B$, there is a function $f(a) = b$ where each $b \in B$ appears for exactly one $a \in A$ and the function is defined for every $b \in B$ and $a \in A$. The *inverse* function $g(b) = a$ where $b = f(a)$ shows $B \sim A$.

(c) If $A \sim B$ and $B \sim C$, then there are one-to-one functions $f(a) = b$ and $g(b) = c$ for each mapping. The function $h(a) = g(f(a))$ then is a one-to-one mapping between A and C.

17.1.6 Problem 23

For **(a)** and **(b)**, the table is Pascal's triangle, which we already have in the notes. For **(c)**, we want the entry $P_{6,3}$ in our earlier notation. There are 20 such ways.

17.1.7 Why answering problem 32 would be a bad idea.

Wow. Never, **ever** give someone a list of all your identifying numbers. Identity theft is a serious problem. While quite often all these numbers are available for a little work, at least make a criminal work for them.

17.2 Problem set 2.3

17.2.1 Problem 2

Substituting into $|A \cup B| = |A| + |B| - |A \cap B|$, we see that $10 = 5 + 8 - |A \cap B|$, or that $|A \cap B| = 3$.

17.2.2 Problem 5

I'm just going to show these as lines. Illustrating them on a "number line" is equivalent. A better diagram for the last would wrap portions of the result in parentheses to show how the line extended.

(a) $3 + 5 =$ ●—●—●—● + ●—●—●—●—●
$=$ ●—●—●—●—●—●—●—●
$= 8$

(b) $5 + 3 =$
●—●—●—●—● + ●—●—●
$=$ ●—●—●—●—●—●—●—●
$= 8$

(c) $4 + 2 =$
●—●—●—● + ●—●
$=$ ●—●—●—●—●—●
$= 6$

(d) $0 + 6 =$
● + ●—●—●—●—●—●
$=$ ●—●—●—●—●—●
$= 6$

(e) $3 + (5 + 7) =$
●—●—● + (●—●—●—●—●—● + ●—●—●—●—●—●—●)
$=$ ●—●—● + ●—●—●—●—●—●—●—●—●—●—●
$=$ ●—●—●—●—●—●—●—●—●—●—●—●—●—●—●
$= 15$

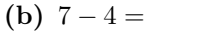
(f) $(3 + 5) + 7 =$
(●—●—●—● + ●—●—●—●—●) + ●—●—●—●—●—●—●

$=$  $+$
$=$
$= 15$

17.2.3 Problem 11

Again, I'm just going to show these as lines. Illustrating them on a "number line" is equivalent.

(a) $7 - 3 =$
 $-$
$=$
$= 4$

(b) $7 - 4 =$
 $-$
$=$ 
$= 3$

(c) $7 - 7 =$
 $-$
$= \bullet = 0$

(d) $7 - 0 =$

$=$ 
$= 7$

17.2.4 Problem 24

Draw with two shadings and show that the intersection is shaded twice.

17.3 Write 2 + 3 using disjoint sets.

If we let $2 \equiv \{a, b\}$ and $3 \equiv \{c, d, e\}$, then $2+3 \equiv \{a, b\} \cup \{c, d, e\} = \{a, b, c, d, e\}$.

17.4 Illustrate 2 + 3 using Peano arithmetic.

We defined addition with

$$a + 0 = a, \text{ and}$$
$$a + S(b) = S(a + b).$$

Here, $3 = S(2)$, so

$$\begin{aligned} 2+3 &= 2+S(2) \\ &= S(2+2) \\ &= S(2+S(1)) \\ &= S(S(2+1)) \\ &= S(S(2+S(0))) \\ &= S(S(S(2+0))) \\ &= S(S(S(2))) \\ &= 5. \end{aligned}$$

17.5 Problem set 2.4

17.5.1 Problem 5

(a) Any set that contains only 1 and some other number is **closed** because 1 is the multiplicative identity.

(b) Any set that contains only 1 and some other number is **closed** because 1 is the multiplicative identity.

(c) $2 \cdot 4 = 8 \notin \{0, 2, 4\}$, so this is **not closed**.

(d) The product of even numbers always is even, so this is **closed**.

(e) The product of odd numbers cannot be even, so they must be odd and this set is **closed**.

(f) $2^2 \cdot 2^3 = 2^5 \notin \{1, 2, 2^2, 2^3\}$, so this set is **not closed**.

(g) The product of powers of two is a power of two, so this set is **closed**.

(h) Similarly, the product of powers of seven is a power of seven so this set is **closed**. Both of these are closed because $\{0, 1, 2, \ldots\}$ is closed under addition; $a^i \cdot a^j = a^{i+j}$, moving the property up to the superscript.

17.5.2 Problem 10

Each product is equal to the appropriate shaded area, and the sum is equal to the entire rectangle. The letters correspond directly to the positions.

I had completely forgotten about the FOIL mnemonic. After long enough, it's just a part of what you do.

17.5.3 Problem 26

The operation is **closed** because no new shapes are introduced in the operator's table of results.

The operation is **commutative** because the operation table is symmetric across the diagonal axis. Thus $a \star b = b \star a$.

Because $\circ \star x = x$, the $\circ$ symbol is $\star$'s identity.

After the identity, there are only two symbols remaining. Thus the commutative property combined with the identity means that *this* operator must be **associative**.

17.6 Illustrate $2 \cdot 3$ using Peano arithmetic. You do not need to expand addition.

We defined multiplication with

$$\begin{aligned} a \cdot 0 &= 0, \text{ and} \\ a \cdot S(b) &= a + (a \cdot b). \end{aligned}$$

So

$$\begin{aligned} 2 \cdot 3 &= 2 \cdot S(2) \\ &= 2 + (2 \cdot 2) \\ &= 2 + (2 \cdot S(1)) \\ &= 2 + (2 + (2 \cdot 1)) \\ &= 2 + (2 + (2 \cdot S(0))) \\ &= 2 + (2 + (2 + 2 \cdot 0)) \\ &= 2 + 2 + 2 = 6. \end{aligned}$$

17.7 Illustrate $(1 \cdot 2) \cdot 3 = 1 \cdot (2 \cdot 3)$ using a volume of size six.

Draw two $1 \times 2 \times 3$ boxes made of $1 \times 1 \times 1$ boxes. To illustrate $(1 \cdot 2) \cdot 3$, show that the 1×2 portion is stacked 3 times. To illustrate $1 \cdot (2 \cdot 3)$, show that the 2×3 portion is stacked across 1 time.

Chapter 18

Notes for the fifth week: review

Notes also available as PDF.

18.1 Review

Structure of the upcoming test:

- Eight questions. Chose ***six*** and solve them.
- Thus expect about seven minutes per question.
- Remember to read and answer the ***entire*** question.
- Closed book, *etc.* Calculators are fine but not necessary.
- Bring scratch paper and paper for writing up your results. Separately.
- Answers and explanations need to be indicated clearly.
- No questions are intended to be "trick" questions.
- Will cover the following topics:
  - problem solving,
  - set theory,
  - operations on whole numbers.
- Remember that solutions for the homework problems are available on-line: `http://jriedy.users.sonic.net/VI/math202-f08/`.

18.2 Problem solving

Pólya's principles:

1. Understand the problem.
2. Devise a plan.
3. Carry out the plan.
4. Look back at your solution.

This is not a simple 1-2-3-4 recipe. Understanding the problem may include playing with little plans, or trying to carry out a plan may lead you back to trying to understand the problem.

18.2.1 Understand the problem

- Read the **entire** problem.

  Read the **whole** problem.

  Read **all of the** problem.

  One comment about the homeworks: Most people answer only part of any given problem.

- Determine what you **have** and what you **want**.

  To indicate an answer clearly to someone else (like me), you need to know what the answer is.

- Consider rephrasing the problem, either in English or symbolically.

  Rephrasing the problem may help you remember solution methods.

- Try some examples.

  This is close to devising a plan. Sometimes you may stumble upon an answer.

- Look for relationships between the data.

  Examples may help find relationships. The relationships may help you decide on a plan. Mathematics is about relationships between different entities; symbolic mathematics helps abstract away the entities themselves.

18.2.2 Devise a plan

Sometimes plans are "trivial," or so simple it seems pointless to make them specific. But write it out anyways. Often the act of putting a plan into words helps find flaws in the plan.

Try to devise a plan that you can check along the way. The earlier you detect a problem, the easier you can deal with it.

Some plans we've considered:

- Guessing and checking.

  Try a few combinations of the data. See what falls out. This is good for finding relationships and understanding the problem.

- Searching using a list.

  If you know the answer lies in some range, you can search that range systematically by building a list.

- Finding patterns.

  When trying examples, keep an eye open for patterns. Sometimes the patterns lead directly to a solution, and sometimes they help to break a problem into smaller pieces.

- Following dependencies / working backwards.

  Be sure to understand what results depend on which data. Look for dependencies in the problem. Sometimes pushing the data you have through all the dependencies will break the problem into simpler subproblems.

18.2.3 Carry out the plan

Attention to detail is critial here.

When building a list, be sure to carry out a well-defined procedure. Or when looking for patterns, be systematic in the examples you try. Don't jump around randomly.

18.2.4 Look back at your solution

Can you check your result? Sometimes trying to check reveals new relationships that could lead to a better solution.

Think about how your solution could help with other problems.

18.3 Set theory

18.3.1 Definitions and mappings

set An **unordered** collection of **unique** elements.

You can write a set by listing its entries, $\{1, 2, 3, 4\}$, or through set builder notation, $\{x \mid x \text{ is a positive integer}, x < 5\}$.

empty set The **unique** set with no elements: $\{\}$ or $\emptyset$. Be sure to know the relations between the empty set and other sets, and also how the empty set behaves in operations.

element of You write $x \in A$ to state that x is an element of A. The symbol is not an "E" but is almost a Greek ϵ. Think of a pitchfork.

Note that $1 \in \{1, 2\}$ and $\{1\} \in \{\{1\}, \{2\}\}$, but $\{1\} \notin \{1, 2\}$.

subset Given two sets A and B, $A \subset B$ if every element of A is also an element of B.

One implication is that $\emptyset \subset A$ for all sets A. This statement is **vacuously** true.

Here $\{1\} \subset \{1, 2\}$ and $\{1\} \not\subset \{\{1\}, \{2\}\}$.

superset Given two sets A and B, $B \supset A$ if every element of A is also an element of B.

proper subset or superset A subset or superset relation is **proper** if it implies the sets are not equal.

Venn diagram A blobby diagram useful for illustrating operations and relations between two or three sets.

union $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$. The union contains all elements of both sets.

intersection $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$. The intersection contains only those elements that exist in both sets.

set difference $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$. The set difference contains elements of the first set that are **not** in the second set. It cannot contain any elements of the second set.

You can write the result of multiple operations in set-builder notation,

$$\begin{aligned}(A \cap B) \cup C &= \{x \mid x \in A \text{ and } x \in B\} \cup C \\ &= \{x \mid (x \in A \text{ and } x \in B) \text{ or } x \in C\}.\end{aligned}$$

18.3.2 Cardinality and one-to-one correspondence

The **cardinality** of a set is a count of its elements. So $|\{a, b, c\}| = 3$. An infinite set like the set of all positive integers has no simple cardinality.

To sets are **equivalent**, or $A \sim B$, if there is a **one-to-one correspondence** between the two sets. With such a correspondence, each element of one set is matched with exactly one element of the other set.

For finite sets, the two sets must be the same size. If they weren't, there would be at least one unmatched element.

For finite sets, establishing a one-to-one correspondence is straight-forward. You just need to list which entries correspond. For $\{1, 2, 3\}$ and $\{a, b, c\}$, such a list might be

$$1 \leftrightarrow c, \quad 2 \leftrightarrow a, \quad 3 \leftrightarrow b.$$

Or you could provide a formula. For $A = \{1, 2, 3\}$ and $B = \{2, 4, 6\}$, a mapping could be $a \in A \leftrightarrow f(a) \in B$ where

$$f(a) = 2a.$$

For infinite sets, a formula is the most straight-forward way. Consider the extending the above sets to be infinite. For sets $A = \{1, 2, 3, \ldots\}$ and $B = \{2, 4, 6, \ldots\}$. the same mapping as before shows they are equivalent. For the sets $A = \{1, 2, 3, \ldots\}$ and $B = \{2, 3, 4, \ldots\}$, a mapping function would be $f(a) = a+1$.

18.4 Operations and whole numbers

closure For any operation, the result of the operation always lies in the set. For whole numbers, $x + y$ is closed but $x - y$ is not.

commutative For numbers, $x+y = y+x$ and $xy = yx$. For sets, $A \cap B = B \cap A$ and $A \cup B = B \cup A$.

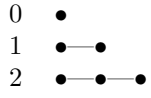
associative For numbers, $x + (y + z) = (x + y) + z$ and $x(yz) = (xy)z$. For sets, $A \cap (B \cap C) = (A \cap B) \cap C)$ and $A \cup (B \cup C) = (A \cup B) \cup C$.

distributive For numbers, the only version is the distribution of multiplication over addition or $x(y+z) = xy+xz$. For sets, both unions and intersections distribute. So $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

There are multiple ways to illustrate addition and multiplication.

For addition, one illustration is "piles of rocks" or symbols. This is somewhat like set unions, except we assume every element of each set is unique. Equivalently, we assume all sets are disjoint. Then $|A \cap B| = |\emptyset| = 0$, so $|A \cup B| = |A| + |B| - |A \cap B| - |A| + |B|$.

Another illustration is the number line. Each number is represented by a length:



Then addition appends lines:

This makes the commutative and associative properties fairly obvious; the line has the same final length regardless.

This is essentially the same as Peano arithmetic covered earlier, except addition in Peano arithmetic moves a bar from one number to the other until the sum is reached.

Multiplication often is best illustrated by areas or volumes.

Chapter 19

First exam and solutions

Available as PDF.

Part III

Notes for chapters 3, 4, and 5

Chapter 20

Notes for the sixth week: digits, bases, and operations

Notes also available as PDF.

What we will cover from Chapter 4:

- Numbers and digits in different bases, with historical context
- Arithmetic, digit by digit

And additionally, I'll give a brief summary of computer arithmetic.

20.1 Positional Numbers

A number is a concept and not just a sequence of symbols. We will be discussing ways to express numbers.

Before our current form of expressing *cardinal* numbers:

- Piles of rocks don't work well for merchants.
- **Marks** on sticks, then marks on papyrus.

Marking numbers is costly. A large number becomes a large number of marks. Many marks lead to many errors. Merchants don't like errors. So people started using symbols rather than plain marks.

An intermediate form, **grouping**:

- Egyptian: Different symbols for different levels of numbers: units, tens, hundreds. Grouping within the levels.

- Roman: Symbols for groups, with addition and subtraction of symbols for smaller groups.
- Greek (and Hebrew and Arabic): Similar, but using all their letters for many groups.
- Early Chinese: Denote the number of marks in the group with a number itself...

Getting better, but each system still has complex rules. The main problems are with skipping groups. We now use zero to denote an empty position, but these systems used varying amounts of space. Obviously, this could lead to trade disagreements. Once zeros were adopted, many of these systems persisted in trade for centuries.

Now into forms of positional notation, shorter and more direct:

- Babylonian:
  - Two marks, tens and units.
  - Now the marks are placed by the number of 60s.
  - Suffers from complicated rules about zeros.
  - (Using 60s persists for keeping time...)
- Mayan:
  - Again, two kinds of marks for fives and units.
  - Two positional types: by powers of 20, and by powers of 20 except for one power of 18.
  - (Note that $18 \cdot 20 = 360$, which is much closer to a year.)
  - Essentially equivalent to what we use, but subtraction in Mayan is much easier to see.
- (many other cultures adopted similar systems (*e.g.* Chinese rods)

Current: **Hindu-Arabic numeral system**

The characters differ between cultures, but the idea is the same. The characters often are similar as well. Originated in the region of India and was carried west through trade. No one knows when zero was added to the digits. The earliest firm evidence is in Arab court records regarding a visitor from India and a description of zero from around 776 AD. The first inscription found with a zero is from 876 AD in India. However, the Hindu-Arabic system was not adopted outside mathematics even in these cultures. Merchants kept to a system similar to the Greek and Hebrew systems using letters for numbers.

Leonardo Fibonacci brought the numerals to Europe in the 13^{th} century (after 1200 AD) by translating an Arabic text to Latin. By 15^{th} century, the nu-

meral system was in wide use in Europe. During the 19^{th} century, this system supplanted the rod systems in Asia.

The final value of the number is based on the positions of the digits:

$$1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0.$$

We call ten the **base**. Then numbers becomes polynomials in terms of the base b,

$$1234 = b^3 + 2 \cdot b^2 + 3 \cdot b^1 + 4.$$

Here $b = 10$.

So we moved from marks, where 1000 would require 1000 marks, to groups, where 1000 may be a single mark but 999 may require dozens of marks. Then we moved to positional schemes where the number of symbols depends on the *logarithm* of the value; $1000 = 10^3$ requires $4 = 3 + 1$ symbols.

After looking at other bases, we will look into operations (multiplication, addition, *etc.*) using the base representations.

20.2 Converting Between Bases

Only three bases currently are in wide use: base 10 (decimal), base 2 (binary), and base 16 (hexadecimal). Occasionally base 8 (octal) is used, but that is increasingly rare. Other conversions are useful for practice and for seeing some structure in numbers. The structure will be useful for computing.

Before conversions, we need the digits to use. In base b, numbers are expressed using digits from 0 to $b - 1$. When b is past 10, we need to go beyond decimal numerals:

Value:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit:	0	1	2	3	4	5	6	7	8	9	**A**	**B**	**C**	**D**	**E**	**F**

Upper- and lower-case are common.

So in hexadecimal, DECAFBAD is a perfectly good number, as is DEADBEEF. If there is a question of what base is being used, the base is denoted by a subscript. So 10_{10} is a decimal ten and 10_2 is in binary.

To find values we recognize more easily, we convert to decimal. Then we will convert *from* decimal.

20.2.1 Converting to Decimal

Converting to decimal using decimal arithmetic is straight-forward. Remember the expansion of 1234 with base $b = 10$,

$$\begin{aligned} 1234 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0 \\ &= b^3 + 2 \cdot b^2 + 3 \cdot b^1 + 4. \end{aligned}$$

Each digit of DEAD has a value, and these values become the coefficients. Then we expand the polynomial with $b = 16$. In a straight-forwart way,

$$\begin{aligned} \mathsf{DEAD} &= \mathsf{D} \cdot 16^3 + \mathsf{E} \cdot 16^2 + \mathsf{A} \cdot 16^1 + \mathsf{D} \\ &= 13 \cdot 16^3 + 14 \cdot 16^2 + 10 \cdot 16 + 13 \\ &= 13 \cdot 4096 + 14 \cdot 256 + 10 \cdot 16 + 13 \\ &= 57005. \end{aligned}$$

We an use **Horner's rule** to expand the polynomial in a method that often is faster,

$$\begin{aligned} \mathsf{DEAD} &= ((13 \cdot 16 + 14) \cdot 16 + 10) \cdot 16 + 13 \\ &= (222 \cdot 16 + 10) \cdot 16 + 13 \\ &= 3562 \cdot 16 + 13 \\ &= 57005. \end{aligned}$$

Let's try a binary example. Convert 1101_2 to decimal:

$$\begin{aligned} 1101_2 &= (((1 \cdot 2 + 1) \cdot 2 + 0) \cdot 2 + 1 \\ &= (3 \cdot 2 + 0) \cdot 2 + 1 \\ &= 6 \cdot 2 + 1 \\ &= 13. \end{aligned}$$

Remember the rows of a truth table for two variables? Here,

$$\begin{aligned} 11_2 &= 2 + 1 = 3, \\ 10_2 &= 2 + 0 = 2, \\ 01_2 &= 0 + 1 = 1, \text{ and} \\ 00_2 &= 0 + 0 = 0. \end{aligned}$$

20.2.2 Converting from Decimal

To convert to binary from decimal, consider the previous example:

$$\begin{aligned} 13 &= 8 + \mathbf{5} \\ &= 8 + 4 + \mathbf{1} \\ &= 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1101_2. \end{aligned}$$

At each step, we find the largest power of two less than the remaining number. Another example for binary:

$$\begin{aligned} 293 &= 256 + \mathbf{37} \\ &= 256 + 32 + \mathbf{5} \\ &= 256 + 32 + 4 + 1 \\ &= 1 \cdot 2^8 + 1 \cdot 2^5 + 1 \cdot 2^2 + 1 \\ &= 100100101_2. \end{aligned}$$

And in hexadecimal,

$$\begin{aligned} 293 &= 256 + \mathbf{37} \\ &= 1 \cdot 256 + 2 \cdot 16 + 5 \\ &= 125_{16}. \end{aligned}$$

You can see why some people start remembering powers of two.

If you have no idea where to start converting, remember the relations $b^{\log_b x} = x$ and $\log_b x = \log x / \log b$. Rounding $\log_b x$ up to the larger whole number gives you the number of base b digits in x.

The text has another version using remainders. We will return to that in the next chapter. And conversions to and from binary will be useful when we discuss how computers manipulate numbers.

20.3 Operating on Numbers

Once we split a number into digits (decimal or binary), operations can be a bit easier.

We will cover multiplication, addition, and subtraction both

- to gain familiarity with positional notation, and
- to compute results more quickly and mentally.

Properties of positional notation will help when we explore number theory.

We will use two properties frequently:

- Both multiplication and addition **commute** ($a + b = b + a$) and re-**associate** $(a + b) + c = a + (b + c)$.
- Multiplication **distributes** over addition, so $a(b + c) = ab + ac$.
- Multiplying powers of a common base adds exponents, so $b^a \cdot b^c = b^{a+c}$.

20.3.1 Multiplication

Consider multiplication. I once had to learn multiplication tables for 10, 11, and 12, but these are completely pointless.

Any decimal number multiplied by 10 is simply shifted over by one digit,

$$\begin{aligned} 123 \cdot 10 &= (1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0) \cdot 10 \\ &= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 \\ &= 1230. \end{aligned}$$

Multiplying by $11 = 1 \cdot 10 + 1$ is best accomplished by adding the other number to itself shifted,

$$123 \cdot 11 = 123 \cdot (10 + 1) = 1230 + 123 = 1353.$$

And for $12 = 1 \cdot 10 + 2$, you double the number,

$$123 \cdot 12 = 123 \cdot (10 + 2) = 1230 + 246 = 1476.$$

Multiplying longer numbers quickly follows the same pattern of shifting and adding. We can expand $123 \cdot 123 = 123 \cdot (1 \cdot 10^2 + 2 \cdot 10 + 3)$ to

$$\begin{array}{r} 123 \\ \times\ 123 \\ \hline 369 \\ 2460 \\ 12300 \\ \hline 15129 \end{array}$$

Another method expands the product of numbers as a product of polynomials, working one term at a time. This is essentially the same but not in tabular form:

$$\begin{aligned} 123 \cdot 123 &= (1 \cdot 10^2 + 2 \cdot 10 + 3) \cdot (1 \cdot 10^2 + 2 \cdot 10 + 3) \\ &= (1 \cdot 10^2 + 2 \cdot 10 + 3) \cdot (1 \cdot 10^2 + 2 \cdot 10) + (1 \cdot 10^2 + 2 \cdot 10 + 3) \cdot 3 \\ &= (1 \cdot 10^2 + 2 \cdot 10 + 3) \cdot (1 \cdot 10^2 + 2 \cdot 10) + (3 \cdot 10^2 + 6 \cdot 10 + 9) \\ &= \ldots \end{aligned}$$

This form splits the sums apart as well; we will cover that next.

Bear in mind that short-term memory is limited to seven to eight pieces of information. Structure mental arithmetic to keep as few pieces in flight as possible. One method is to break multiplication into stages. In long form, you can group the additions. For example, expanding $123 \cdot 123 = 123 \cdot (1 \cdot 10^2) + (123 \cdot 23) = 123 \cdot (1 \cdot 10^2) + (123 \cdot 2 \cdot 10 + 123 \cdot 3)$,

$$\begin{array}{r} 123 \\ \times\ 123 \\ \hline 369 \\ 2460 \\ \hline 2829 \\ 12300 \\ \hline 15129 \end{array}$$

Assuming a small number uses only one slot in your short-term memory, need track only where you are in the multiplier, the current sum, the current product, and the next sum. That leaves three to four pieces of information to use while adding.

One handy trick for 15% tips: divide by ten, divide that amount by two, and add the pieces. We can use positional notation to demonstrate how that works,

$$\begin{aligned} x \cdot 15\% &= (x \cdot 15)/100 \\ &= ((x \cdot (10 + 5))/100 \\ &= ((x \cdot 10) + (x \cdot (10/2)))/100 \\ &= x/10 + (x/10)/2 \end{aligned}$$

20.3.2 Addition

Digit-by-digit addition uses the commutative and associative properties:

$$\begin{aligned} 123 + 456 &= (1 \cdot 10^2 + 2 \cdot 10 + 3) + (4 \cdot 10^2 + 5 \cdot 10 + 6) \\ &= (1 + 4) \cdot 10^2 + (2 + 5) \cdot 10 + (3 + 6) \\ &= 579. \end{aligned}$$

Naturally, when a digit threatens to roll over ten, it **carries** to the next digit. Expanding the positional notation,

$$\begin{aligned} 123 + 987 &= (1 \cdot 10^2 + 2 \cdot 10 + 3) + (9 \cdot 10^2 + 8 \cdot 10 + 7) \\ &= (1 + 9) \cdot 10^2 + (2 + 8) \cdot 10 + (3 + 7) \\ &= 10 \cdot 10^2 + 10 \cdot 10 + 10. \end{aligned}$$

Because the coefficients are greater than $b - 1 = 9$, we expand those coefficients. Commuting and reassociating,

$$\begin{aligned} 123 + 987 &= 10 \cdot 10^2 + 10 \cdot 10 + 10 \\ &= (1 \cdot 10 + 0) \cdot 10^2 + (1 \cdot 10 + 0) \cdot 10 + (1 \cdot 10 + 0) \\ &= 1 \cdot 10^3 + 1 \cdot 10^2 + 1 \cdot 10 + 0 \\ &= 1110. \end{aligned}$$

However, when working quickly, or when the addition will be used in another operation, you do not need to expand the carries immediately. This is called a **redundant representation** because numbers now have multiple representations. You can represent 13 as $1 \cdot 10 + 3$ or simply as 13.

If you work that way mentally, you need to keep the intermediate results in memory. So during multiplying, you only need to work out the carries every three to four digits...

20.3.3 Subtraction

In systems with signed numbers, we know that subtracting a number is the same as adding its negation: $a - b = a + (-b)$. So we expect the digit-by-digit method to work with each digit subtracted, and it does. Because $-a = -1 \cdot a$, we can distribute the sign over the digits:

$$\begin{aligned} 456 - 123 &= (4 \cdot 10^2 + 5 \cdot 10 + 6) - (1 \cdot 10^2 + 2 \cdot 10 + 3) \\ &= (4 \cdot 10^2 + 5 \cdot 10 + 6) + (-(1 \cdot 10^2 + 2 \cdot 10 + 3)) \\ &= (4 \cdot 10^2 + 5 \cdot 10 + 6) + (-1 \cdot 10^2 + -2 \cdot 10 + -3) \\ &= (4 - 1) \cdot 10^2 + (5 - 2) \cdot 10 + (6 - 3) \\ &= 333. \end{aligned}$$

As with carrying, **borrowing** occurs when a digit goes negative:

$$\begin{aligned} 30 - 11 &= (3 \cdot 10^1 + 0) - (1 \cdot 10^1 + 1) \\ &= (3 - 1) \cdot 10^1 + (0 - 1) \\ &= 2 \cdot 10^1 + -1 \\ &= 1 \cdot 10^1 + (10 - 1) \\ &= 1 \cdot 10^1 + 9 \\ &= 19. \end{aligned}$$

Again, you can use a redundant intermediate representation of $2 \cdot 10^1 - 1$ if you're continuing to other operations. And if **all** the digits are negative, you

can factor out -1,

$$\begin{aligned} 123 - 456 &= (1 \cdot 10^2 + 2 \cdot 10 + 3) - (4 \cdot 10^2 + 5 \cdot 10 + 6) \\ &= (1 - 4) \cdot 10^2 + (2 - 5) \cdot 10 + (3 - 6) \\ &= (-3) \cdot 10^2 + (-3) \cdot 10 + (-3) \\ &= -(3 \cdot 10^2 + 3 \cdot 10 + 3) \\ &= -333. \end{aligned}$$

20.3.4 Division and Square Root: Later

We will cover these later with number theory.

20.4 Homework

- Problem Set 3.1 (p154)
  - 8, 16
  - 32, 34, 35
- Problem Set 3.2 (p161)
  - 3, 4, 5, 6, 8, 11, 20
- Problem Set 3.3 (p177)
  - 10, 12, 20 (the zeros are indicators; find the *least* base where the sum is correct)
- Problem Set 3.4 (p188)
  - 5
  - 17 (this is Napier's method; he made physical rods to accelerate the process)
  - 19, 33

Chapter 21

Solutions for sixth week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

21.1 Problem set 3.1

Problem 8 Assuming the accounting style and not the calender style, the first number to add is $5 \cdot 20^2 + 6 \cdot 20 + 13$ and the second is $11 \cdot 20 + 8$, but we don't *need* these forms. We can add Mayan digit by Mayan digit instead. The bottom digit is three bars and six dots, which simplifies to four bars and one dot, or one dot and one dot carried up to the next digit. The next digit is three bars and three dots, where one of those dots is the carry. There are no carries here, so the top digit is just a bar. The final result: **One dot in the bottom digit, three bars and three bars in the next digit up, then a single bar in the top-most digit.**

Problem 16 $24\,872 = \mathbf{2 \cdot 10^4 + 4 \cdot 10^3 + 8 \cdot 10^2 + 7 \cdot 10^1 + 2 \cdot 10^0}$, $3\,071 = \mathbf{3 \cdot 10^3 + 0 \cdot 10^2 + 7 \cdot 10^1 + 1 \cdot 10^0}$

Problem 32 $500 + \mathbf{60} + 9 = 569$

Problem 34 $300 + \mathbf{80} + 5 = 385$

Problem 35 $2 \cdot 10 + 18 = 2 \cdot 10 + 10 + 8 = (2 + 1) \cdot 10 + 8 = 3 \cdot 10 + 8 = \mathbf{38}$.

21.2 Problem set 3.2

Problem 3 The last digit, the one corresponding to $6^0 = 1$, is constant down the table. The first digit, the one corresponding to $6^1 = 6$, is constant across the table. Along each diagonal, both digits increase by one at each step. There are other patterns, but these are some of the most obvious.

Problem 4 The next two rows:

60	61	62	63	64	65
70	71	72	73	74	75

Problem 5

- $413_5 = 4 \cdot 5^2 + 1 \cdot 5 + 3 = 108$
- $2004_5 = 2 \cdot 5^3 + 4 = 254$
- $10_5 = 1 \cdot 5 = 5$
- $100_5 = 1 \cdot 5^2 = 25$
- $1000_5 = 1 \cdot 5^3 = 125$
- $2134_5 = 2 \cdot 5^3 + 1 \cdot 5^2 + 3 \cdot 5 + 4 = 294$

Problem 6

- $413_6 = 4 \cdot 6^2 + 1 \cdot 6 + 3 = 153$
- $2004_6 = 2 \cdot 6^3 + 4 = 436$
- $10_6 = 1 \cdot 6 = 6$
- $100_6 = 1 \cdot 6^2 = 36$
- $1000_6 = 1 \cdot 6^3 = 216$
- $2134_6 = 2 \cdot 6^3 + 1 \cdot 6^2 + 3 \cdot 6 + 4 = 490$

Problem 8

- $362 = 2422_5$
- $27 = 102_5$
- $5 = 10_5$
- $25 = 100_5$

Problem 11

- $2^0 = 1$
  $2^1 = 2$
  $2^2 = 4$
  $2^3 = 8$
  $2^4 = 16$
  $2^5 = 32$
  $2^6 = 64$
  $2^7 = 128$
  $2^8 = 256$
  $2^9 = 512$
  $2^{10} = 1024$

- $1101_2 = 13$
- $111_2 = 7$
- $1000_2 = 8$
- $10101_2 = 21$

- $24 = 11000_2$
- $18 = 10010_2$
- $2 = 10_2$
- $8 = 1000_2$

- $0 = 0_2 = 00000_2$
  $1 = 1_2 = 00001_2$
  $2 = 10_2 = 00010_2$
  $3 = 11_2 = 00011_2$
  $4 = 100_2 = 00100_2$
  $5 = 101_2 = 00101_2$
  $6 = 110_2 = 00110_2$
  $7 = 111_2 = 00111_2$
  $8 = 1000_2 = 01000_2$
  $9 = 1001_2 = 01001_2$
  $10 = 1010_2 = 01010_2$
  $11 = 1011_2 = 01011_2$
  $12 = 1100_2 = 01100_2$
  $13 = 1101_2 = 01101_2$
  $14 = 1110_2 = 01110_2$
  $15 = 1111_2 = 01111_2$
  $16 = 10000_2 = 10000_2$
  $17 = 10001_2 = 10001_2$
  $18 = 10010_2 = 10010_2$
  $19 = 10011_2 = 10011_2$
  $20 = 10100_2 = 10100_2$
  $21 = 10101_2 = 10101_2$
  $22 = 10110_2 = 10110_2$
  $23 = 10111_2 = 10111_2$
  $24 = 11000_2 = 11000_2$
  $25 = 11001_2 = 11001_2$
  $26 = 11010_2 = 11010_2$
  $27 = 11011_2 = 11011_2$
  $28 = 11100_2 = 11100_2$
  $29 = 11101_2 = 11101_2$
  $30 = 11110_2 = 11110_2$
  $31 = 11111_2 = 11111_2$

One of the more important patterns to see is how the digits repeat once

padded to the left by zeros. The units (or right-most) digit alternates $0, 1, 0, 1, \ldots$. The next alternates in pairs, $0, 0, 1, 1, 0, 0, 1, 1, \ldots$. The next in groups of four, the next in groups of eight, and so forth.

- In one sentence: They're the same thing.

Problem 20

- Base two digits take two values, so a three-digit numeral may take one of $2 \cdot 2 \cdot 2 = 8$ values.
- The problem is the same, so there are eight possible subsets. This is how we described the power-set operation, and $\mathcal{P}(A) = 2^{|A|}$ for any set A.
- The same argument or reference provides $2^4 = 16$ subsets.
- The general result is 2^n.

21.3 Problem set 3.3

Problem 10 In order, the steps are **associativity**, **associativity**, **commutativity**, **associativity**, **associativity**, and **distributivity of addition over multiplication**.

Problem 12

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Problem 20

- Here, $1 + 4 = 0$ in the units digit, so the base must be **5**.
- $2 + 4 = 0$ two places over, and $3 + 1 = 4$ without a carry before it, so the base must be **6**.
- There are no carries in the sum at all, so the base is indeterminant. The base can be **any integer at least 7** because the largest digit that appears is 6.
- $3 + 1 = 0$, but the before it $4 + 4 = 4$ must carry and itself be afffected by a carry. The base is **5**.
- Swap the subtraction around, so $236 + 254 = 523$. If $6 + 4 = 3$ plus a carry, the base is **7**.
- $247 + 254 = 523$. With $7 + 4 = 3$ plus a carry, the base is **8**.
- $28\mathsf{E} + 254 = 523$. Now $\mathsf{E} + 4 = 3$ plus a carry, so the base is $\mathsf{E} + 1 = \mathsf{F}$ or **15**.

21.4 Problem set 3.4

Problem 5 In order of blanks, **distributivity of addition over multiplication**, **commutativity of multiplication**, **associativity of addition**, and **distributivity of addition over multiplication**.

Problem 17

	3	7	4	
0	0/6	1/4	0/8	2
8	0/3	0/7	0/4	1
0	1/5	3/5	2/0	5
	4	1	0	

  So $374 \cdot 215 = 80410$.

- The lattice algorithm works digit by digit. This is the same as the method in class but using diagonals rather than writing in columns.

- I would hope so, but it hasn't so far. Working with a set of Napier's bones could help. Those are physical rods you use to build these columns.

Problem 19

- The Egyptian algorithm essentially converts the multiplier to binary. Then it doubles the multiplicand at each step and adds the intermediate product to the result if the corresponding bit of the multiplier is 1.

- I have never heard of the "duplation" algorithm (perhaps duplication?). But one way to write out the method is to convert 24 to binary, $24 = 11000_2$. Now start with an accumulator of 0:

bit of 17	doubling of 71	accumulator
		0
0	71	0
0	142	0
0	284	0
1	568	568
1	1136	1704

  So $71 \cdot 24 = 1704$.

Problem 33

Problem	Actual answer	Calculator's answer
8×3	24	34
9×5	45	55
4×2	8	18
8×4	32	42
$a \times b$	$x - 10$	x
9×6	$64 - 10 = 54$	64

When the decimal logic was done outside a chip (the early 80s), this type of failure could happen from a simple short-circuit. Now it's highly doubtful; a failure like this would require massive trauma to the chip, leading to general failure.

Chapter 22

Notes for the seventh week: primes, factorization, and modular arithmetic

Notes also available as PDF.

This week, we will cover the following topics from Chapter 4 and Chapter 5:

- divisibility and prime numbers,
- factorization into primes,
- modular arithmetic, and
- finding divisibility rules.

I'm pulling modular arithmetic (clock arithmetic) from Chapter 5 because it explains divisibility rules. We'll return to the clock form in the future.

Once upon a time, number theory was both decried and revered as being "pure mathematics" with no practical applications. That is no longer remotely true. There are oblique applications in error correction (*e.g.* how CDs still play when scratched), but one overwhelming, direct application is in **encryption**.

So I also will discuss at some point

- Euler's totient function ($\phi(n)$) and the RSA encryption algorithm.

The RSA algorithm is at the core of the ***s**ecure **s**ocket **l**ayer* (SSL) protocol used to secure web access (the `https` prefix, colored locks, *etc.*).

22.1 Divisibility

When defining operations on integers, we skipped division. As with subtraction, the integers are not closed over division; $1/2$ is not an integer. So we define division implicitly.

For any integers a and b, we can write

$$b = q \cdot a + r,$$

where q is an integer called the **quotient**, and $r < |a|$ is a *non-negative* integer called is the **remainder**, **residue**, or **residual**. We will see that requiring $0 \leq r < |a|$ is very important and makes division well-defined.

Then a **divides** b, or $a \mid b$, when $r = 0$. Alternately, b is a **multiple** of a and a is a **divisor** of b. If we cannot write $b = q \cdot a + r$ with $r = 0$, then a does not divide b, or $a \nmid b$. When $a \mid b$, then we define division as $b/a = q$.

For example,

$$\begin{aligned} 14 &= 2 \cdot 7 + 0, \text{ so } 7 \mid 14 \text{ and } 14/7 = 2, \text{ and} \\ 20 &= 2 \cdot 7 + 6, \text{ so } 7 \nmid 20 \text{ and } 20/7 \text{ is not an integer.} \end{aligned}$$

In the latter case, though, $20/7 = 2 + 6/7$, which rounds down to 2.

Some other examples showing extreme and negative cases,

$$\begin{aligned} -6 &= -3 \cdot 2 + 0, \text{ so } 2 \mid -6 \text{ and } -6/2 = -3, \\ -6 &= 3 \cdot -2 + 0, \text{ so } -2 \mid -6 \text{ and } -6/-2 = 3, \\ 6 &= -3 \cdot -2 + 0, \text{ so } -2 \mid 6 \text{ and } 6/-2 = -3, \\ -7 &= -4 \cdot 2 + 1, \text{ so } 2 \nmid -7, \\ -7 &= 4 \cdot -2 + 1, \text{ so } -2 \nmid -7, \\ 7 &= -3 \cdot -2 + 1, \text{ so } -2 \nmid 7 \text{ (\textbf{note}: not } -4 \cdot -2 - 1), \\ 5 &= 0 \cdot 10 + 5, \text{ so } 10 \nmid 5, \text{ and} \\ 0 &= 0 \cdot 13 + 0, \text{ so } 13 \mid 0 \text{ and } 0/13 = 0. \end{aligned}$$

What about when $a = 0$? Then $b = q \cdot 0 + b$ is true for any quotient q. Without further restrictions on q, division by zero is not be well-defined. In calculus and some applications, there are times when you fill in the hole left by a division by zero by some obvious completion.

But is the form $b = qa + r$ well-defined when $a \neq 0$?

Theorem: The expansion $b = qa + r$ with $0 \leq r < |a|$ is unique for $a \neq 0$, so division is well-defined.

Proof. We begin by assuming there are two ways of expanding $b = qa + r$. Then we show that the forms must be identical.

Let there be two distinct ways of writing $b = qa + r$ with $a \neq 0$,

$$b = q_1 a + r_1, \text{ and}$$
$$b = q_2 a + r_2,$$

with $0 \leq r_1 < |a|$ and $0 \leq r_2 < |a|$.

If $r_1 = r_2$, then $b - r_1 = b - r_2$. From the equations above $b - r_1 = q_1 a$ and $b - r_2 = q_2 a$, so $q_1 a = q_2 a$ or $(q_1 - q_2)a = 0$. Because $a \neq 0$, $q_1 = q_2$ and the forms are identicall.

For $r_1 \neq r_2$, we know one of them is larger. *Without loss of generality*, assume $r_1 < r_2$. Then there is some positive integer k such that increases r_1 to match r_2, or $r_2 = r_1 + k$. Note that $k \leq r_2$.

Substituting for r_2, we see that $b = q_2 a + r_1 + k$, or equivalently $b - k = q_2 a + r_1$. Now we can subtract this equation from $b = q_1 a + r_1$ to obtain

$$k = (q_1 - q_2)a = z \cdot a + 0$$

for some quotient z.

So $a \mid k$, but $k \leq r_2 < |a|$. The only way we can satisfy this is if $q_1 - q_2 = 0$ and $q_1 = q_2$. Thus also $k = 0$ and $r_1 = r_2$. So we cannot have to different ways to write $b = q \cdot a + r$, and our form of division is well-defined. □

Some useful properties of divisibility:

- If $d \mid a$ and $d \mid b$, then $d \mid ra + sb$ for all integers r and s. A quick proof: $a = q_a d$ and $b = q_b d$, so $ra + sb = rq_a d + sq_b d = (rq_a + sq_b)d$, then $d | ra + sb$.
- If $a \mid b$ and $b \mid c$, then $a \mid c$. Quick proof: $b = q_a a$, $c = q_b b$, so $c = q_b(q_a a) = (q_b q_a)a$.
- If $a \mid bc$ and $a \nmid b$, then $a \mid c$.

22.2 Primes

Divisibility gives a numbers a multiplicative structure that's different than the digit-wise structure we previously examined.

To build the structure, we start from numbers which cannot be decomposed. An integer $p > 1$ is called a **prime** number if its only divisors are 1 and p itself. We will explain why 1 is not considered prime when we discuss factorization. All other numbers are **composite** and must have some prime divisor.

Consider possible *divisors* of 11,

$$\begin{aligned} 11 &= 11 \cdot 1 + 0 \text{ so } 1 \mid 11, \\ 11 &= 5 \cdot 2 + 1 \text{ so } 2 \nmid 11, \text{ and} \\ 11 &= 3 \cdot 3 + 2 \text{ so } 3 \nmid 11. \end{aligned}$$

We can stop at 3. Because multiplication is commutative, any divisors come in pairs. The smaller of the pair must be $\leq \sqrt{11} \approx 3.3$; that's the point where any pairs $a \cdot b$ are repeated as $b \cdot a$.

So the only divisor less than $\sqrt{11}$ is 1, and 11 is prime.

How many primes are there?
Theorem: There are infinitely many primes.

Proof. Assume there are only k primes $p_1, p_2, \ldots, p_k$ and all other numbers are composite. Then let $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$, one larger than the product of all primes.

Consider dividing n by some prime, say p_k. Then we can write $n = (p_1 \cdot p_2 \cdot \cdots \cdot p_{k-1})p_i + 1$. Given the form is unique and $r = 1$, p_k does not divide n. We could have chosen any of the primes, so $p_i \nmid n$ for all $i = 1, \ldots, k$. Thus no prime divides n.

For a number n to be composite, it must have some factor or divisor other than 1 and n. If that factor is not prime, then the factor has another factor, and so forth until you reach some prime. Because of transitivity of division ($a \mid b$ and $b \mid c$ imply $a \mid c$), the prime must divide n. Here, though, no primes divide n, so n cannot be composite and must be prime itself.

So assuming there are k primes leads to a contradiction because we can construct one more. Thus there are either no primes or infinitely many. We demonstrated that 11 is prime, so there must be infinitely many primes. □

There are mountains of unanswered questions about prime numbers. Consider the pairs of primes $(3, 5)$, $(5, 7)$, $(11, 13)$, and $(17, 19)$. Each are separated by two. Are there infinitely many such pairs? No one knows. Similarly, there are **Mersenne primes** of the form $2^n - 1$. No one knows how many Mersenne primes exist.

22.3 Factorization

A **factorization** of a number is a decomposition into factors. So $24 = 8 \cdot 3$ is a factorization of 24, as is $24 = 4 \cdot 2 \cdot 3$. A **prime factorization** is a factorization

into primes. Here $24 = 2 \cdot 2 \cdot 2 \cdot 3$ is a prime factorization of 24. We use exponents to make this easier to write, and $24 = 2^3 \cdot 3$.

You can be systematic about prime factorization and discover the primes through the **sieve of Eratosthenes**. Consider finding a prime factorization of 110.

We start just by writing possible factors. Technically we need integers only $\leq \sqrt{1100} \approx 33.6$, but we only fill enough here to demonstrate the point.

	2	**3**	*4*	**5**	*6*	**7**	*8*	*9*	*10*
11	*12*	**13**	*14*	*15*	*16*	**17**	*18*	**19**	*20*

The first possible factor is 2, and $2 \mid 1100$. We divide by two until the result is not divisible by 2. This gives $1100 = 2^2 \cdot 275$. Then we cross out all multiples of 2; these cannot divide 275. Because $275 = 91 \cdot 3 + 2$, $3 \nmid 275$. But we also know no multiples of 3 divide 275, so we cross out all remaining multiples of 3.

The next not crossed out is 5, which divides 275. Now $1100 = 2^2 \cdot 5^2 \cdot 11$. We showed 11 is prime before, but let's continue this method. Cross out all multiples of five. The next number to try is 7, which does not divide 11. But we can cross out all multiples of 7. The next free number is 11, which we have again shown to be prime.

In our (short) list, it happens that only primes remain. We have sieved out all the non-primes. Actually, once we removed all multiples of primes $\leq \sqrt{20}$, only primes remained.

Moving from one prime to the next is a systematic method both for finding prime numbers and for finding a prime factorization.

Factorizations provide a useful mechanism for working

We will not prove the following, but is often called the **fundamental theorem of arithmetic**:
Theorem: Every integer greater than one has a unique prime factorization.

22.4 Modular Arithmetic

Factorization itself will prove useful later. Now we will explore modular arithmetic and find some quick rules for determining when $d \mid a$ for some d.

Modular arithmetic is arithmetic on remainders.

Consider expressions of 7 and 4 in terms of multiples of 3 plus remainders: $7 = 2 \cdot 3 + 1$ and $4 = 1 \cdot 3 + 1$. Now $11 = 7 + 4 = (2 \cdot 3 + 1) + (1 \cdot 3) + 1 = 3 \cdot 3 + 2$. Note that the sum of the remainders was < 3 and was the new remainder itself.

If the remainder is ≥ 3, we can just pull a three out of it: $11 + 8 = (3 \cdot 3 + 2) + (2 \cdot 3 + 2) = 5 \cdot 3 + 4$. To convert this into the correct form, note that

$4 = 1 \cdot 3 + 1$, and $19 = 5 \cdot 3 + (1 \cdot 3 + 1) = 6 \cdot 3 + 1$. We need consider only the sum of remainders to compute the result's remainder.

The remainder of the sum just wraps around. Think about time. If you add a few hours and cross 12, the result just wraps around. So 1:00 is the same as 13:00 or 25:00.

We don't identify 1:00 as just one time but a member of a set of all times that are one hour after a multiple of 12. Similarly, we can identify numbers as elements of sets where all members have the same remainder relative to a given divisor.

The **congruence class** of r **modulo** a is $\{x \mid \exists q : x = qa + r\}$. If a number b is in the congruence class of r modulo a, we write $b \equiv r \pmod{a}$.

The canonical member of a congruence class is its least positive member. Just as we don't naturally consider 25:00 as 1:00, we tend to identify congruence classes by the least r. So while $13 \equiv 87 \pmod{2}$ is correct (both 13 and 87 are odd), we prefer $13 \equiv 1 \pmod{2}$.

We define addition and multiplication on entire congruence classes. For the operation to be defined, the **modulus** of each class must be the same. Then we're adding numbers of the form $b_1 = q_1 a + r_1$ for $b_1 \equiv r_1 \pmod{a}$ and $b_2 = q_2 a + r_2$ for $b_2 \equiv r_2 \pmod{a}$. As in our example above, the remainders add. Here $b_1 + b_2 = q_1 a + r_1 + q_2 a + r_2 = (q_1 + q_2)a + (r_1 + r_2) \equiv r_1 + r_2 \pmod{a}$.

Identifying congruence classes by their least positive element, we can write a table showing all additions modulo 4:

$+ \pmod 4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Addition of congruence classes maintains the **additive identity** that we expect, $b + 0 \equiv b \pmod{a}$.

Note that every class has an **additive inverse**, a class where $b + (-b) \equiv 0 \pmod{a}$. Remember that we forced the residual to be positive when we defined division. Then we can see that the inverse of 1 modulo 4 is $-1 = -1 \cdot 4 + 3 \equiv 3 \pmod{4}$.

Another way to see this is that the canonical representation of $-b$ is the least number which increases b to be equal to the modulus a. So the inverse of 1 is 3 because $1 + 3 = 4 \equiv 0 \pmod{4}$.

We also define multiplication on congruence classes.

If $b_1 = q_1 a + r_1$ and $b_2 = q_2 a + r_2$, then

$$\begin{aligned} b_1 \cdot b_2 &= (q_1 a + r_1) \cdot (q_2 a + r_2) \\ &= q_1 q_2 a^2 + q_1 r_2 a + q_2 r_1 a + r_1 r_2 \\ &= (q_1 q_2 a + q_1 r_2 + q_2 r_1) a + r_1 r_2 \\ &\equiv r_1 r_2 \pmod{a}. \end{aligned}$$

So we need only multiply remainders.

Identifying congruence classes by their least positive element, we can write a table showing all multiplications modulo 4:

$\times \pmod 4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Again, there is a **multiplicative identity**, $b \cdot 1 \equiv b \pmod{a}$.

Unlike plain integer division, some congruence classes have an inverse. The only integer that has an integer inverse is 1. But modulo 4, both 1 and 3 have **multiplicative inverses**. Here $3 \cdot 3 = 9 \equiv 1 \pmod 3$.

22.5 Divisibility Rules

Using modular arithmetic and positional notation, we can derive some quick divisibility tests.

First, consider divisibility by powers of 2 and 5. The factorization of $10 = 2 \cdot 5$, and so $10^k = 2^k \cdot 5^k$. So $2^k \mid 10^k$ and $5^k \mid 10^k$, or $10^k \equiv 0 \pmod 2^k$ and $10^k \equiv 0 \pmod 5^k$.

Now remember how to expand positional notation. We know that $1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4$. So $1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \equiv 0 + 0 + 0 + 4 \pmod 2 \equiv 0 \pmod 2$. Divisibility by 2 depends only on the final digit. Similarly, $1234 \equiv 0 + 0 + 0 + 4 \pmod 5$, and divisibility by 5 depends only on the final digit.

For $2^2 = 4$ and $5^2 = 25$, all but the last two digits are equivalent to zero. And for $2^3 = 8$ and $5^3 = 125$, all but the last three digits are equivalent to zero. So one divisibility rule:

> When testing for divisibility by 2^k or 5^k, we need only consider the last k digits.

Now consider divisibility by 3 or 9. We know that $10 \equiv 1 \pmod 3$ and $10 \equiv 1 \pmod 9$. Using modular arithmetic, $123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \equiv 1 + 2 + 3$

$(\text{mod } 3) \equiv 6 \ (\text{mod } 3) \equiv 0 \ (\text{mod } 3)$. Hence $3 \mid 123$ because the sum of its digits is divisible by 3.

Similarly, $10 \equiv 1 \ (\text{mod } 3)$. So $123 \equiv 1+2+3 \ (\text{mod } 9) \equiv 6 \ (\text{mod } 9)$, and $9 \nmid 123$. If the sum of the digits is greater than 9, simply add those digits.

> Test for divisibility by 3 or 9 by adding the number's digits and checking that sum. If that sum is greater than 9, add the digits again. Repeat until the result is obvious.

Other primes are not so straight-forward. Divisibility by 7 is a pain; there is an example method in the text's problems for Section 5.1.

The rule for 11 is worth exploring. Because $10 < 11$, the canonical member of its congruence class is just 10. But there is another member of interest, $10 \equiv -1$ (mod 1)1. So you can alternate signs on alternate digits from the right. So $123456 \equiv -1 + 2 - 3 + 4 - 5 + 6 \equiv 3 \ (\text{mod } 1)1$, and $11 \nmid 123456$.

For divisibility by 6, 12, 18, or other composite numbers, factor the divisor and test for divisibility by each factor. To test for divisibility by $72 = 2^3 \cdot 3^2 = 8 \cdot 9$, test for divisibility by 8 and by 9.

22.6 Homework

- Problem Set 4.1 (p242):
  - Problem 2, but don't repeat the drawings.
  - 4, 7, 9, 10, 13, 14, 23, 24
- Also draw diagrams showing that $8 \nmid 18$ and $3 \nmid 11$.
- Problem Set 4.2 (p252):
  - 1, 2, 8, 14, 15
- Take a familiar incomplete integer, _ 679 _. Using the expression of _ 679 _ as $N = 10^4 \cdot x_4 + x_0 + 6790$, use $8 \mid N$ to find x_0? Given that, use $9 \mid N$ to find x_4. Now if 72 turkeys cost $ _ 679 _, what is the total?

Chapter 23

Solutions for seventh week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

23.1 Problem set 4.1

Problem 2 The (non-repeated) factorizations are $1 \cdot 35$ and $5 \cdot 7$. Drawing those as boxes is straight-forward.

Problem 4

Factors of 18	1	2	3	6	9	18
Quotient	18	9	6	3	2	1

Problem 7

- $48 = 1 \cdot 48 = 2 \cdot 24 = 3 \cdot 16 = 4 \cdot 6$, so the factors are 1, 2, 3, 4, **6**, 16, 24, and 48.
- $54 = 1 \cdot 54 = 2 \cdot 27 = 3 \cdot 18 = 6 \cdot 9$, so the factors are 1, 2, 4, **6**, 9 18, 27, 54.
- The largest common factor then is **6**.

Problem 9

- $48 = 2^4 \cdot 3^1$
- $108 = 2^2 \cdot 3^3$
- $2250 = 2^2 \cdot 3^2 \cdot 5^3$
- $24\,750 = 2^1 \cdot 3^2 \cdot 5^3 \cdot 11^1$

Problem 10

- Yes, because all primes are shared and no powers of the primes exceed those of a.
- No, because 3^2 has a larger exponent than the 3^1 in a.
- $a/b = (2^3 \cdot 3^1 \cdot 7^2)/(2^2 \cdot 3^1) = 2^{3-2} \cdot 3^{1-1} \cdot 7^{2-0} = 2^1 \cdot 7^2$.
- There are $(2+1) \cdot (1+1) \cdot (2+1) = 18$ factors of a.
- We can make a list by running up the exponents:

$$
\begin{gathered}
2^0 \cdot 3^0 \cdot 7^0 \\
2^1 \cdot 3^0 \cdot 7^0 \\
2^2 \cdot 3^0 \cdot 7^0 \\
2^3 \cdot 3^0 \cdot 7^0 \\
2^0 \cdot 3^1 \cdot 7^0 \\
2^1 \cdot 3^1 \cdot 7^0 \\
2^2 \cdot 3^1 \cdot 7^0 \\
2^3 \cdot 3^1 \cdot 7^0 \\
2^0 \cdot 3^0 \cdot 7^1 \\
2^1 \cdot 3^0 \cdot 7^1 \\
2^2 \cdot 3^0 \cdot 7^1 \\
2^3 \cdot 3^0 \cdot 7^1 \\
2^0 \cdot 3^1 \cdot 7^1 \\
2^1 \cdot 3^1 \cdot 7^1 \\
2^2 \cdot 3^1 \cdot 7^1 \\
2^3 \cdot 3^1 \cdot 7^1 \\
2^0 \cdot 3^0 \cdot 7^2 \\
2^1 \cdot 3^0 \cdot 7^2 \\
2^2 \cdot 3^0 \cdot 7^2 \\
2^3 \cdot 3^0 \cdot 7^2 \\
2^0 \cdot 3^1 \cdot 7^2 \\
2^1 \cdot 3^1 \cdot 7^2 \\
2^2 \cdot 3^1 \cdot 7^2 \\
2^3 \cdot 3^1 \cdot 7^2
\end{gathered}
$$

Problem 13 No, it is only true that at least **one** prime factor cannot exceed $\sqrt{n}$. Consider $2 \cdot 47 = 94$, where both 2 and 47 are prime. We have $\sqrt{94} < 10$ but $47 > 10 > \sqrt{94}$. But $2 < \sqrt{94}$.

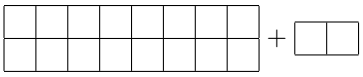
Problem 14 No. If n is not prime, some of its factors may split between b and c. For example, $2 \cdot 3 = 6 \mid 18 = 2 \cdot 9$, but $6 \nmid 2$ and $6 \nmid 9$. The factors of $n = 6$, 2 and 3, are split between $a = 2$ and $b = 9$.

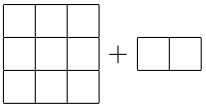
Problem 23 Here it **is** true. Consider the prime factorizations of b and c. If $p \mid bc$, then p must appear in one or both of those prime factorizations, and thus it must divide at least one of b and c.

Problem 24 Again, use the prime factorization of n. Because p and q are primes, they must appear in that factorization. Then $pq \mid n$ because both

appear, so you can commute products around to group (pq) and the rest of the factorization.

23.2 Two diagrams

$8 \nmid 18$**:** $18 = 2 \cdot 8 + 2$, so you can draw and count: 

$3 \nmid 11$**:** $11 = 3 \cdot 3 + 2$: 

23.3 Problem set 4.2

Problem 1

- 1554 is even, so **divisible by 2**, does not end in 5 or 0, so **is *not* divisible by 5**, and has digits that add to 0 (mod 3), so **is divisible by 3**.
- 1999 is not even, so **is *not* divisible by 2**, does not end in 5 or 0, so **is *not* divisible by 5**, and has digits that add to 1 (mod 3), so **is *not* divisible by 3**.
- 805 **is *not* divisible by 2**, **is divisible by 5**, and **is *not* divisible by 3**.
- 2450 **is divisible by 2**, **is divisible by 5**, and **is *not* divisible by 3**.

Problem 2

- 2 and 3
- 2 and 5
- 3 and 5
- 2, 3, and 5

Problem 8 The missing digit must be divisible by 2. Also, the sum of the digits must be congruent to 0 modulo 3. The non-blank digits already add to 0 (mod 3), so the missing digit must be a multiple of 3. There is only one even multiple of 3 less than 10, so the missing digit must be **6**.

Problem 14 Expanding the positional notation and simplifying, $abc, abc = a{\cdot}(10^5{+}10^2){+}b{\cdot}(10^4{+}10^1){+}c{\cdot}(10^3{+}10^0) = (a{\cdot}10^2{+}b{\cdot}10^1{+}c){\cdot}(10^3{+}10^0) = abc \cdot 1001$. Now $1001 = 7 \cdot 11 \cdot 13$, so abc, abc is divisible by each of those.

Problem 15

- $ab - ba = a \cdot 10 + b - (b \cdot 10 + a) = (a - b) \cdot 10 + (b - a)$. Because $10 \equiv 1 \pmod 9$, this becomes $a - b + b - a \equiv 0 \pmod 9$. The result always is a multiple of 9. Equivalently, we can rearrange

$(a-b)\cdot 10+(b-a) = (a-b)\cdot 10+-1\cdot(a-b) = (a-b)\cdot(10-1) = 9(a-b)$, giving also *which* multiple of 9.

- Here the difference is $(a-c)\cdot 10^2+0+(c-a)$ because the middle digit always cancels. Again, the result always is a multiple of 9 and we can rearrange $(a-c)\cdot 10^2+0+(c-a) = (a-c)\cdot 10^2+-1\cdot(a-c) = (a-c)\cdot(10^2-1) = 99(a-c)$ to see the result is a multiple of 99.

23.4 A familiar incomplete integer

> Take a familiar incomplete integer, _679_. Using the expression of _679_ as $N = 10^4\cdot x_4 + x_0 + 6790$, use $8 \mid N$ to find x_0. Given that, use $9 \mid N$ to find x_4. Now if 72 turkeys cost \$_679_, what is the total?

If $8 \mid N$ then 8 divides the last three digits, so $8 \mid 790 + x_0$. Thus $790 + x_0 \equiv 0 \pmod 8$. Because $790 \equiv 6 \pmod 8$, we know that $x_0 \equiv 2 \pmod 8$. The only decimal digit satisfying $x_0 \equiv 2 \pmod 8$ is $\mathbf{x_0 = 2}$.

Now we have $N = 10^4\cdot x_4 + 6792$. For $9 \mid N$, the sum of the digits must be zero modulo 9. Thus $x_4 + 6 + 7 + 9 + 2 \equiv 0 \pmod 9$, or $x_4 + 6 \equiv 0 \pmod 9$. Thus $\mathbf{x_4 = 3}$, and $\mathbf{N = 36792}$.

(I forgot the decimal place in the problem, so these are very expensive turkeys.)

So if 72 turkeys cost \$36792, each turkey costs \$511. If I had remembered the decimal place correctly, the turkeys cost \$5.11 each.

Chapter 24

Notes for the eighth week: GCD, LCM, and $ax + by = c$

Notes also available as PDF.

What we covered last week:

- divisibility and prime numbers,
- factorization into primes,
- modular arithmetic,
- finding divisibility rules,

This week's topics:

- review modular arithmetic and finding divisibility rules,
- greatest common divisors and least common factors,
- Euclid's algorithm for greatest common divisors, and
- solving linear Diophantine equations.

These all are useful when you deal with integral numbers of things

24.1 Modular arithmetic

Remember the divisibility form for b with respect to dividing by $a \neq 0$,

$$b = q \cdot a + r, \text{ with } 0 \leq r < |a|.$$

This form is *unique* for a given a and b.

Consider $a = 5$. There are only five possible values of r, zero through four. Because the form is unique, we can place every b into one of r **congruence classes**. Each congruence class is a set. For $a = 5$, we have the following classes:

$$\begin{array}{lrrrrrrl}
\{\ldots, & \text{-10}, & \text{-5}, & \mathbf{0}, & 5, & 10, & \ldots\} & = \{5k+0 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-9}, & \text{-4}, & \mathbf{1}, & 6, & 11, & \ldots\} & = \{5k+1 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-8}, & \text{-3}, & \mathbf{2}, & 7, & 12, & \ldots\} & = \{5k+2 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-7}, & \text{-2}, & \mathbf{3}, & 8, & 13, & \ldots\} & = \{5k+3 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-6}, & \text{-1}, & \mathbf{4}, & 9, & 14, & \ldots\} & = \{5k+4 \,|\, k \in \mathbb{J}\}
\end{array}$$

We say that two numbers are in the same congruence class for a given a by

$$b \equiv c \pmod{a}.$$

Or b is equivalent to c **modulo** a. A collection of one entry from each set is called a **complete residue system**. We typically select the least positive numbers, those in bold above.

We define arithmetic on congruence classes by arithmetic on the remainders. The remainders wrap around every multiple of the modulus. For example, addition modulo 4 and modulo 5 are defined as follows:

+ (mod 4)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+ (mod 5)	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

This works as you expect. Addition is **commutative** and **associative**. There is an **additive identity**, because $b + 0 \equiv 0 \pmod{a}$. Unlike the positive integers, there also is an **additive inverse** for every residue because $b + (a - b) \equiv 0 \pmod{a}$.

Multiplication likewise is **commutative** and **associative**, and there is a **multiplicative identity**, 1. The unusual aspect appears with the **multiplicative inverse**. Some residues have inverses, and some don't:

× (mod 4)	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

× (mod 5)	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The difference here is that 5 is prime while 4 is composite. Any factor of the modulus will not have a multiplicative inverse.

24.2 Divisibility rules

One common application of modular arithmetic (besides telling time) is in testing whether one integer divides another. We use modular arithmetic and positional notation. Both help us break the larger problem, testing divisibility of a potentially large number, into the smaller problems of breaking apart the number and evaluating expressions in modular arithmetic.

If $a \mid b$ (a divides b), then $b \equiv 0 \pmod{a}$. So we can test for divisibility by expanding b in positional notation and evaluating the operations modulo a.

When the divisor is small, a straight-forward evaluation is simplest. Because $10 \equiv 1 \pmod{3}$, we can test for divisibility by 3 by adding the number's digits modulo 3. For example,

$$\begin{aligned} 1234 &\equiv 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \pmod{3} \\ &\equiv 1^3 + 2 \cdot 1^2 + 3 \cdot 1 + 4 \pmod{3} \\ &\equiv 1 + 2 + 3 + 4 \equiv 1 + 2 + 0 + 1 \equiv 1 \pmod{3}. \end{aligned}$$

Hence $3 \nmid 1234$. The same "trick" applies to 9 because $10 \equiv 1 \pmod{9}$.

When the divisor is closer to a power of 10, using a negative element of the congruence class may be useful. For 11, remember that 10 and -1 are in the same congruence class because $10 = 0 \cdot 11 + 10$ and $-1 = -1 \cdot 11 + 10$. So $10 \equiv -1 \pmod{11}$ and we can expand the powers of ten,

$$\begin{aligned} 1234 &\equiv 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \pmod{11} \\ &\equiv (-1)^3 + 2 \cdot (-1)^2 + 3 \cdot (-1) + 4 \pmod{11} \\ &\equiv -1 + 2 + -3 + 4 \pmod{11} \equiv 2 \pmod{11}. \end{aligned}$$

Hence $11 \nmid 1234$. Here, the "trick" form is that you start from the units digit and then alternate subtracting and adding digits.

For more complicated examples, we can factor the divisor. To test if a number is divisible by 72, factor $72 = 2^3 \cdot 3^2 = 8 \cdot 9$. Then test if the number is divisible by 8 and by 9.

If $a \mid b$ and $c \mid b$, then it **may** be true that $ac \mid b$. This is certainly true of a and b are powers of different primes. The key point is that a and b share no common divisors. Note that $72 = 6 \cdot 12$, $6 \mid 24$, and $12 \mid 24$, but obviously $72 \nmid 24$ because $24 < 72$.

24.3 Greatest common divisor

So finding common divisors is useful for testing divisibility. The greatest common divisor of numerator and denominator reduces a fraction into its simplest form.

In general, common divisors help break problems apart.

> Written (a, b) or $\gcd(a, b)$, the greatest common divisor of a and b is the largest integer $d \geq 1$ that divides both a and b.

We'll discuss a total of two methods for finding the greatest common divisor. The first uses the prime factorization, and the second uses the divisibility form in the Euclidean algorithm. Later we'll extend the Euclidean algorithm to provide integer solutions x and y to equations $ax + by = c$.

The prime factorization method factors both a and b. Consider $a = 1400 = 2^3 \cdot 5^2 \cdot 7$ and $b = 1350 = 2 \cdot 3^3 \cdot 5^2$.

Lining up the factorizations and remembering that $x^0 = 1$, we have

$$a = 1400 = 2^3 \cdot 3^{\mathbf{0}} \cdot 5^{\mathbf{2}} \cdot 7^1, \text{ and}$$
$$b = 1350 = 2^{\mathbf{1}} \cdot 3^3 \cdot 5^{\mathbf{2}} \cdot 7^{\mathbf{0}}.$$

Now chose the least exponent for each factor. Then

$$d = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 = 50$$

is the greatest common divisor. For more than two integers, factor all the integers and find the least exponents across the corresponding factors in all of the factorizations.

For an example use, reduce a fraction $a/b = 1350/1400$ to its simplest form. To do so, divide the top and bottom by $d = 50$. Then $a/b = 1350/1400 = 27/28$.

Now we can state the requirement about divisibility given some factors:

> If two relatively prime integers a and b both divide c, then ab divides c.

Some other properties of the gcd:

- Because the gcd is positive, $(a, b) = (|a|, |b|)$.
- $(a, b) = (b, a)$
- If the gcd of two numbers is 1, or $(a, b) = 1$, then a and b are called **relatively prime**.

24.4 Least common multiple

Before the other method for finding the gcd, we consider one related quantity.

> The least common multiple, often written $\text{lcm}(a, b)$, is the least number $L \geq a$ and $L \geq b$ such that $a \mid L$ and $b \mid L$.

There are clear, every day uses. Think of increasing a recipe when you can only buy whole bags of some ingredient. You need to find the least common multiple

of the recipe's requirement and the bag's quantity. Or when you need to find the next day two different schedules intersect.

Again, you can work from the prime factorizations

$$a = 1400 = 2^{\mathbf{3}} \cdot 3^0 \cdot 5^{\mathbf{2}} \cdot 7^{\mathbf{1}}, \text{ and}$$
$$b = 1350 = 2^1 \cdot 3^{\mathbf{3}} \cdot 5^{\mathbf{2}} \cdot 7^0.$$

Now the least common multiple is the product of the *larger* exponents,

$$\operatorname{lcm}(a, b) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^1 = 37\,800.$$

And for more than two integers, take the maximum across all the exponents of corresponding factors.

Another relation for two integers a and b is that

$$\operatorname{lcm}(a, b) = \frac{ab}{d}.$$

So given $a = 1350$, $b = 1400$, and $d = 50$,

$$\operatorname{lcm}(1350, 1400) = \frac{1350 \cdot 1400}{50} = \frac{1\,890\,000}{50} = 37\,800.$$

This does not hold directly for more than two integers.

24.5 Euclidean GCD algorithm

Another method for computing the gcd of two integers a and b is due to Euclid. This often is called the first algorithm expressed as an abstract sequence of steps.

We start with the division form of b in terms of $a \neq 0$,

$$b = qa + r \text{ with } 0 \leq r < a.$$

Because $(a, b) = (|a|, |b|)$, we can assume both a and b are non-negative. And because $(a, b) = (b, a)$, we can assume $b \geq a$.

Let $d = (a, b)$. Last week we showed that if $d|a$ and $d|b$, then $d|ra + sb$ for any integers r and s. Then because $d|a$ and $d|b$, we have $d|b - qa$ or $d|r$. So we have that $d = (b, a)$ also divides r. Note that any number that divides a and r also divides b, so $d = (a, r)$.

Continuing, we can express a in terms of r as

$$a = q'r + r' \text{ with } 0 \leq r' < r.$$

Now $d|r'$ and $d = (r, r')$. Note that $r' < r < a$, so the problem keeps getting smaller! Eventually, some remainder will be zero. Then the *previous* remainder is the greatest common divisor.

1. Find q_0 and r_0 in $b = q_0 a + r_0$ with $0 \leq r_0 < a$.
2. If $r_0 = 0$, then $(a, b) = a$.
3. Let $r_{-1} = a$ to make the loop easier to express.
4. Then for $i = 1, \ldots$
   (a) Find q_i and r_i in $r_{i-2} = q_i r_{i-1} + r_i$ with $0 \leq r_i < r_{i-1}$.
   (b) If $r_i = 0$, then $(a, b) = r_{i-1}$ and quit.
   (c) Otherwise continue to the next i.

Consider calculating $(53, 77)$. Following the steps, we have

$$\begin{aligned} 77 &= 1 \cdot 53 + 24, \\ 53 &= 2 \cdot 24 + 5, \\ 24 &= 4 \cdot 5 + 4, \\ 5 &= 1 \cdot 4 + 1, \text{ and} \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

And thus $(53, 77) = 1$.

For another example, take $(128, 308)$. Then

$$\begin{aligned} 308 &= 2 \cdot 128 + 52, \\ 128 &= 2 \cdot 52 + 24, \\ 52 &= 2 \cdot 24 + 4, \text{ and} \\ 24 &= 6 \cdot 4 + 0. \end{aligned}$$

So $(128, 308) = 4$.

24.6 Linear Diophantine equations

Later in the semester, we will examine linear equations $ax + by = c$ over real numbers. But many every-day applications require integer solutions. We can use the Euclidean algorithm to find one integer solution to $ax + by = c$ or prove there are none. Then we can use the computed gcd to walk along the line to all integer solutions.

Say we need to solve $ax + by = c$ for integers a, b, and c to find **integer** solutions x and y.

Let $d = (a, b)$. Then, as before, $d \mid ax + by$ for all integers x and y. So $d \mid c$ for any solutions to exist. If $d \nmid c$, then there are **no integer solutions**. If a and b are relatively prime, then $(a, b) = 1$ and solutions exist for any integer c.

Consider solving $ax + by = d$. Because $d \mid c$, we can multiply solutions to $ax + by = d$ by c/d to obtain solutions of $ax + by = c$. To solve $ax + by = d$ we work backwards after using the Euclidean algorithm to compute $d = (a, b)$.

Say the algorithm required k steps, so $d = r_{k-1}$. Working backward one step,

$$\begin{aligned} d = r_{k-1} &= r_{k-3} - q_{k-1}r_{k-2} \\ &= r_3 - q_{k-1}(r_{k-4} - q_{k-2}r_{k-3}) \\ &= (1 + q_{k-1}q_{k-2})r_3 - q_{k-1}r_{k-4}. \end{aligned}$$

So $d = r_{k-1} = i \cdot r_{k-3} + j \cdot r_{k-4}$ where i and j are integers. Continuing, the gcd d can be expressed as an integer combination of each pair of remainders.

Returning to the example of $(77, 53)$,

$$\begin{aligned} 1 &= 5 - 1 \cdot 4, \\ &= 5 - 1 \cdot (24 - 5 \cdot 5) = 5 \cdot 5 - 1 \cdot 24 \\ &= 5 \cdot (53 - 2 \cdot 24) - 1 \cdot 24 = 5 \cdot 53 - 11 \cdot 24 \\ &= 5 \cdot 53 - 11 \cdot (77 - 1 \cdot 53) = 16 \cdot 53 - 11 \cdot 77. \end{aligned}$$

To solve $53x + 77y = 22$, we start with $53 \cdot 16 + 77 \cdot (-1) = 1$. Multiplying by 22,

$$53 \cdot (16 \cdot 22) + 77 \cdot (-1 \cdot 22) = 22,$$

and $x = 352$, $y = -22$ is one solution.

But if there is one solution, there are infinitely many! Remember that $d = (a, b)$, so a/d and b/d are integers. Given one solution $x = x_0$ and $y = y_0$, try substituting $x = x_0 + t \cdot (b/d)$ and $y = y_0 - t \cdot (a/d)$ for any integer t. Then

$$\begin{aligned} a(x_0 + t \cdot (b/d)) + b(x_0 - t \cdot (a/d)) &= ax_0 + bx_0 + t \cdot (ab/d)) + -t \cdot (ba/d)) \\ &= ax_0 + bx_0 = c. \end{aligned}$$

Actually, *all* integer solutions to $ax + by = c$ are of the form

$$x = x_0 + t \cdot (b/d), \quad \text{and} \quad y = y_0 - t \cdot (a/d),$$

where t is any integer, $d = (a, b)$, and x_0 and y_0 are a solution pair.

Another example, consider solving $12x + 25y = 331$. First we apply the Euclidian algorithm to compute $(12, 25) = 1$:

$$\begin{aligned} 25 &= 2 \cdot 12 + 1, \text{ and} \\ 12 &= 12 \cdot 1 + 0. \end{aligned}$$

Substituting back,

$$12 \cdot (-2) + 25 \cdot 1 = 1, \text{ and} 12 \cdot (-662) + 25 \cdot 331 = 331.$$

So we can generate any solution to $12x + 25y = 331$ with the equations

$$x = -662 + 25t \quad \text{and} \quad y = 331 - 12t.$$

Using these, we can find a "smaller" solution. Try making x non-negative with

$$\begin{aligned} -662 + 25t &\geq 0, \\ 25t &\geq 662, \text{ thus} \\ t &> 26. \end{aligned}$$

Substituting $t = 27$,

$$x = 13, \quad \text{and} \quad y = 7.$$

Interestingly enough, this must be the *only* non-negative solution. A larger t will force y negative, and a smaller t forces x negative. But the solution for $t = 26$ is still "small",

$$x = -12, \quad \text{and} \quad y = 19.$$

24.7 Homework

Practice is absolutely critical in this class.

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

- Problem set 4.3, p264:
  - 6, 7, 13 (using any method, not the specified one), 15, 18, 25
- Compute the following using **both** the prime factorization method and the Euclidean algorithm:
  - $(720, 241)$
  - $(64, 336)$
  - $(-15, 75)$
- Compute the least common multiples:
  - $\text{lcm}(64, 336)$
  - $\text{lcm}(11, 17)$
  - $\text{lcm}(121, 187)$
  - $\text{lcm}(2025, 648)$
- Find **two** integer solutions to each of the following, or state why no solutions exist:
  - $64x + 336y = 32$

- $33x - 27y = 11$
- $31x - 27y = 11$

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 25

Solutions for eighth week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

25.1 Problem set 4.3

Problem 6 Every integer divides zero, so $(0, n) = n$ appears correct for $n > 0$. Indeed, $0 = 0 \cdot n$ and $n = 1 \cdot n$, so n divides both. The only point for discussion is in the *definition* of the greatest common divisor and divisibility. The text defines it in an obtuse way that disallows $(0, n) = n$.

Most mathematicians would allow $n \mid 0$ and $(0, n) = n$. Indeed, $n \mid 0$ for all n is stated on the *first page* of one of the most respected number theory textbooks[1]. So, alas, the "correct" response is to find out what standardized test uses which definition. This is yet another reason why standardized tests in higher mathematics are useless.

Problem 7 Again, by the text's definitions, this cannot be true. By most common mathematical definitions, $\text{lcm}(0, n) = 0$. This is another example where I'm interested in seeing how *you* state and defend your position.

Problem 13 • One method for finding both is to find the prime factorizations $18 = 2 \cdot 3^2$, $24 = 2^3 \cdot 3$, and $12 = 2^2 \cdot 3$. Then $(18, 24, 12) = 2 \cdot 3 = 6$ and $\text{lcm}(18, 24, 12) = 2^3 \cdot 3^2 = 72$.

[1] Hardy, G., & Wright, E. (1979). *An Introduction to the Theory of Numbers*. Oxford: Clarendon Press.

- Here $8 = 2^3$, $20 = 2^2 \cdot 5$, and $14 = 2 \cdot 7$. So $(8, 20, 14) = 2$ and $\text{lcm}(8, 20, 14) = 2^3 \cdot 5 \cdot 7 = 280$.
- Verify: $2 \cdot 280 = 560$, $8 \cdot 20 \cdot 14 = 2240$. So the two quantites are **not** equal. The product of the gcd and lcm only equals the product of the numbers when there are only two numbers involved or when no pairs of numbers **any** factors.

Problem 15

- $(24, 18) = 6$, and $(6, 12) = 6$. Also, $\text{lcm}(24, 18) = 72$ and $\text{lcm}(72, 12) = 72$. Both give the same result, as they must.
- $(8, 20) = 4$, $(4, 14) = 2$. $\text{lcm}(8, 20) = 40$, $\text{lcm}(40, 14) = 280$. Again, these agree.
- The gcd and lcm can be computed pairwise. That is, you can compute each over the first pair of numbers, then compute over that result and the next number, *etc.*

Problem 18

- Find the largest jump such that you can reach all the numbers when starting from zero.
- Take each number as a jump size. Find the first number where all the jumps land simultaneously.

Problem 25 This is looking for the least common multiple of 45 and 96. Think of it like the number line problem above. You mark a notch on each gear. Starting with that notch on zero, you roll each gear to generate the "jumps". You are looking for the point where they coincide. So $\text{lcm}(45, 96) = \text{lcm}(3 \cdot 15, 3 \cdot 32) = 3 \cdot 15 \cdot 32 = 1440$ teeth will go past. In terms of the *smaller* hear, this is $1440/45 =$ **32** revolutions.

25.2 Computing GCDs

Compute the following using **both** the prime factorization method and the Euclidean algorithm:

- $(720, 241)$
- $(64, 336)$
- $(-15, 75)$

Prime factorizations:

- 241 is prime. So $(720, 241) = 1$.
- $64 = 2^6$, $336 = 2^4 \cdot 3 \cdot 7$. $(64, 336) = 2^4 = 16$.
- $(-15, 75) = (15, 75)$. $15 = 3 \cdot 5$, $75 = 3 \cdot 5^2$, so $(-15, 75) = 15$.

Euclidean algorithm:

- $$\begin{aligned} 720 &= 2 \cdot 241 + 238, \\ 241 &= 1 \cdot 238 + 3, \\ 238 &= 79 \cdot 3 + \mathbf{1} \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

  So $(720, 241) = \mathbf{1}$.

- $$\begin{aligned} 336 &= 5 \cdot 64 + \mathbf{16}, \\ 64 &= 4 \cdot 16 + 0. \end{aligned}$$

  So $(336, 64) = 16$.

- $(-15, 75) = (15, 75)$:

  $$75 = 5 \cdot \mathbf{15} + 0.$$

  So $(-15, 75) = 15$.

25.3 Computing LCMs

Compute the least common multiples:

- $\text{lcm}(64, 336)$
- $\text{lcm}(11, 17)$
- $\text{lcm}(121, 187)$
- $\text{lcm}(2025, 648)$

- $\text{lcm}(64, 336) = 64 \cdot 336/(336, 64) = 1344$
- Both are prime, so $\text{lcm}(11, 17) = 11 \cdot 17 = 187$
- $\text{lcm}(121, 187) = \text{lcm}(11^2, 11 \cdot 17) = 11^2 \cdot 17 = 2057$
- $\text{lcm}(2025, 648) = \text{lcm}(3^3 \cdot 5^2, 2^3 \cdot 3^4) = 2^3 \cdot 3^4 \cdot 5^2 = 16200$

25.4 Linear Diophantine equations

Find **two** integer solutions to each of the following, or state why no solutions exist:

- $64x + 336y = 32$

  - $33x - 27y = 11$
  - $31x - 27y = 11$
- From a previous problem, we have that $336 = 64 \cdot 5 + 16$. Thus $336 \cdot 1 + 64 \cdot -5 = 16$ and $336 \cdot 2 + 64 \cdot -10 = 32$. So one solution is $\mathbf{x_0} = \mathbf{-10}$ and $\mathbf{y_0} = \mathbf{2}$. The general solution is $x = x_0 + t \cdot 336/(336, 64) = -10 + 21t$ and $y = y_0 - t \cdot 64/(336, 64) = 2 - 4t$ for any integer t. Another solution then is $\mathbf{x(1)} = \mathbf{-10 + 1 \cdot 21 = 11}$ and $\mathbf{y(1)} = \mathbf{2 - 4 \cdot 1 = -2}$.
- Here, $(33, 27) = (3 \cdot 11, 3^3) = 3$. Now $3 \nmid 11$, so there are **no solutions**.
- Now 31 is prime, so $(31, 27) = 1 \mid 11$ and there are solutions. Running through the Euclidean algorithm we see that

$$\begin{aligned} 31 &= 27 \cdot 1 + 4, \\ 27 &= 4 \cdot 6 + 3, \text{and} \\ 4 &= 3 \cdot 1 + 1. \end{aligned}$$

  Starting from the bottom and substituting for the previous remainder,

$$\begin{aligned} 4 + 3 \cdot (-1) &= 1, \\ 4 + (27 + 4 \cdot (-6)) \cdot -1 &= 27 \cdot (-1) + 4 \cdot 7 = 1, \\ 27 \cdot (-1) + (31 + 27 \cdot (-1)) \cdot 7 &= 31 \cdot 7 + 27 \cdot (-8) = 1. \end{aligned}$$

  We find that $31 \cdot 7 + 27 \cdot (-8) = 1$, so $31x - 27y = 11$ has an initial solution of $\mathbf{x_0} = \mathbf{7 \cdot 11 = 77}$ and $\mathbf{y_0} = \mathbf{-1 \cdot -8 \cdot 11 = 88}$.

  The general solutions have the form

$$\begin{aligned} x &= x_0 + t\frac{-27}{(31, 27)} = 77 - 27t, \text{ and} \\ y &= y_0 - t\frac{31}{(31, 27)} = 88 - 31t, \end{aligned}$$

  Another solution is given by $\mathbf{x(1)} = \mathbf{77 - 27 \cdot 1 = 50}$ and $\mathbf{y(1)} = \mathbf{88 - 31 \cdot 1 = 57}$.

Chapter 26

Notes for the ninth week: $ax + by = c$, fractions

Notes also available as PDF.

26.1 Linear Diophantine equations

In a few weeks, we will examine linear equations $ax + by = c$ over real numbers. But many every-day applications require integer solutions. We can use the Euclidean algorithm to find one integer solution to $ax + by = c$ or prove there are none. Then we can use the computed gcd to walk along the line to all integer solutions.

Some solvable problems:

> A 98 pound box contains 5 pound bags of sugar and 12 pound sacks of oranges. How many of each are in the box?

Or:

> Say you need a digital image in a 4 : 3 aspect ratio ($x : y$) that includes a 50 pixel border along each side. What sizes are possible for the inner image?

Consider the latter problem. Rephrasing algebraically,

$$\frac{4}{3} = \frac{x + 100}{y + 100}, \text{ or}$$
$$3x - 4y = 100.$$

We start by solving

$$3x - 4y = 1$$

and then multiplying the base solutions by 100. This case has one easy solution, $x = -1$ and $y = -1$, with $3 \cdot -1 - 4 \cdot -1 = -3 + 4 = 1$. Another solution is $x = 3$ and $y = 2$.

In fact, there are infintely many solutions to $3x - 4y = 1$ given by

$$\begin{aligned} x &= -1 + 4t, \text{ and} \\ y &= -1 + 3t \end{aligned}$$

for any integer t. You can substitute these expressions into $3x - 4y$ to verify the result. Scaling the right-hand side by 100, solutions to $3x - 4y = 100$ are given by

$$\begin{aligned} x &= -100 + 4t, \text{ and} \\ y &= -100 + 3t. \end{aligned}$$

For $x > 0$ and $y > 0$, we need $t > 33$. So the first positive solutions are given by $t = 34, 35, \ldots$ and are

$$(x, y) \in \{\ldots, (36, 2), (40, 5), (44, 8), (48, 11), (52, 14), (56, 17), (60, 20), \ldots\}.$$

26.1.1 In general...

Say we need to solve $ax + by = c$ for integers a, b, and c to find **integer** solutions x and y. In general, equations over integers are called **Diophantine equations** after Diophantus of Alexandria (approx. 200AD-290AD). He was the first known to study these equations using algebra. The form $ax + b = c$ describes **linear Diophantine equations**.

Let $d = (a, b)$. Then, as before, $d \mid ax + by$ for all integers x and y. So $d \mid c$ for any solutions to exist. If $d \nmid c$, then there are **no integer solutions**. If a and b are relatively prime, then $(a, b) = 1$ and solutions exist for any integer c.

Consider solving $ax + by = d$. Because $d \mid c$, we can multiply solutions to $ax + by = d$ by c/d to obtain solutions of $ax + by = c$. To solve $ax + by = d$ we work backwards after using the Euclidean algorithm to compute $d = (a, b)$.

Say the algorithm required k steps, so $d = r_{k-1}$. Working backward one step,

$$\begin{aligned} d = r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} \\ &= r_3 - q_{k-1}(r_{k-4} - q_{k-2} r_{k-3}) \\ &= (1 + q_{k-1} q_{k-2}) r_3 - q_{k-1} r_{k-4}. \end{aligned}$$

So $d = r_{k-1} = i \cdot r_{k-3} + j \cdot r_{k-4}$ where i and j are integers. Continuing, the gcd d can be expressed as an integer combination of each pair of remainders.

Returning to the example of $(77, 53)$, we found

$$\begin{aligned} 77 &= 1 \cdot 53 + 24, \\ 53 &= 2 \cdot 24 + 5, \\ 24 &= 4 \cdot 5 + 4, \\ 5 &= 1 \cdot 4 + 1, \text{ and} \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Working from the second to the last,

$$\begin{aligned} 1 &= 5 - 1 \cdot 4, \\ &= 5 - 1 \cdot (24 - 5 \cdot 5) = 5 \cdot 5 - 1 \cdot 24 \\ &= 5 \cdot (53 - 2 \cdot 24) - 1 \cdot 24 = 5 \cdot 53 - 11 \cdot 24 \\ &= 5 \cdot 53 - 11 \cdot (77 - 1 \cdot 53) = 16 \cdot 53 - 11 \cdot 77. \end{aligned}$$

To solve $53x + 77y = 22$, we start with $53 \cdot 16 + 77 \cdot (-1) = 1$. Multiplying by 22,

$$53 \cdot (16 \cdot 22) + 77 \cdot (-1 \cdot 22) = 22,$$

and $x = 352$, $y = -22$ is one solution.

But if there is one solution, there are infinitely many! Remember that $d = (a, b)$, so a/d and b/d are integers. Given one solution $x = x_0$ and $y = y_0$, try substituting $x = x_0 + t \cdot (b/d)$ and $y = y_0 - t \cdot (a/d)$ for any integer t. Then

$$\begin{aligned} a(x_0 + t \cdot (b/d)) + b(x_0 - t \cdot (a/d)) &= ax_0 + bx_0 + t \cdot (ab/d)) + -t \cdot (ba/d)) \\ &= ax_0 + bx_0 = c. \end{aligned}$$

Actually, *all* integer solutions to $ax + by = c$ are of the form

$$x = x_0 + t \cdot (b/d), \quad \text{and} \quad y = y_0 - t \cdot (a/d),$$

where t is any integer, $d = (a, b)$, and x_0 and y_0 are a solution pair.

Another example, consider solving $12x + 25y = 331$. First we apply the Euclidian algorithm to compute $(12, 25) = 1$:

$$\begin{aligned} 25 &= 2 \cdot 12 + 1, \text{ and} \\ 12 &= 12 \cdot 1 + 0. \end{aligned}$$

Substituting back,

$$\begin{aligned} 12 \cdot (-2) + 25 \cdot 1 &= 1, \text{ and} \\ 12 \cdot (-662) + 25 \cdot 331 &= 331. \end{aligned}$$

So we can generate any solution to $12x + 25y = 331$ with the equations

$$x = -662 + 25t \quad \text{and} \quad y = 331 - 12t.$$

Using these, we can find a "smaller" solution. Try making x non-negative with

$$\begin{aligned} -662 + 25t &\geq 0, \\ 25t &\geq 662, \text{ thus} \\ t &> 26. \end{aligned}$$

Substituting $t = 27$,

$$x = 13, \quad \text{and} \quad y = 7.$$

Interestingly enough, this must be the *only* non-negative solution. A larger t will force y negative, and a smaller t forces x negative. But the solution for $t = 26$ is still "small",

$$x = -12, \quad \text{and} \quad y = 19.$$

26.1.2 The other example

Our other posed problem:

> A 98 pound box contains 5 pound bags of sugar and 12 pound sacks of oranges. How many of each are in the box?

So we need to solve $5x + 12y = 98$, and start with $5x + 12y = 1$.

Computing $(12, 5)$,

$$\begin{aligned} 12 &= 2 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1, \text{ and} \end{aligned}$$

$$2 = 2 \cdot 1 + 0.$$

So $(12, 5) = 1$. Because $1 \mid 98$, there are infinitely many integer solutions. We need to find the *non-negative* solutions from those.

For a base solution,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (12 - 2 \cdot 5) \\ &= 5 \cdot (5) + 12 \cdot (-2). \end{aligned}$$

So $x_0 = 5$ and $y_0 = -2$ solve $5x + 12y = 1$. Multiplying by 98,

$$x_0 = 490 \quad \text{and} \quad y_0 = -196$$

solve $5x + 12y = 98$.

To find all solutions,

$$x = 490 + 12t, \text{ and}$$
$$y = -196 - 5t.$$

To find *non-negative* solutions, first consider how to make y positive. Here $t = -40$ makes $y = 4$. Trying x, $x = 10$. So one solution is

$$x_+ = 10 \quad \text{and } y_+ = 5.$$

With $t = -39$, y is negative. And with $t = -41$, x is negative. So this is the **only** possible solution for the actual problem.

26.2 Into real numbers

We've used real numbers without much thought. For the next week and a half, we'll fill in a few details.

- Rational numbers
  - Arithmetic and comparisons
  - Decimal expansion (and other bases)
  - Percentages
- Irrational numbers
  - Show that non-rational real numbers exist
  - Square roots, cube roots, and other radicals
- Computing
  - Floating-point arithmetic (arithmetic with restricted rationals)

This week will cover topics in rational numbers and hence fractions. For some people, this will be old hat. For others, this is a continuing thorn in their sides.

This presentation will be a bit different than the text's more typical structure. I hope that this difference may help some who struggle with rationals and fractions by providing reasons for the rules.

26.2.1 Operator precedence

A quick aside on the order in which operations can be applied. Working with fractions stress operator precedence.

Operations generally don't pass through straight lines, whether horizontal for fractions or vertical for absolute value.

Parentheses force an order. Work from the inner outwards.

The general order of precedence between operations:

1. exponents, then
2. multiplication and division (which really are the same thing), then
3. addition, subtraction, and negation (again, these are the same thing).

Within a class, operations proceed from left to right.

Go through a parenthetical clause and compute every exponent, then every multiplication from left to right, and then every addition from left to right.

When in doubt, use parentheses when you write expressions.

26.3 Rational numbers

Rational numbers are ratios of integers. In a fraction $\frac{n}{d}$, n is the **numerator** and d is the **denominator**. The rational numbers form a set,

$$\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{J}, b \in \mathbb{J}, b \neq 0\},$$

where $\mathbb{J}$ is the set of all integers. Let $\mathbb{R}$ be the set of all real numbers, then $\mathbb{J} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. The integer on top, a, is the **numerator**; the integer on the bottom, b, is the **denominator**.

Note that this is a very formal construction. We just plop one integer atop another and call it a number. Amazing that it works.

Fractions represent ratios and proportions. When you state that 1 in 10 people are attractive to mosquitos[1], that's a rational number. We won't reach probability, where we learn to interpret these ratios correctly, but we will cover basic manipulations of rational numbers.

Two fun points:

- There are only as many rational numbers as there are non-negative integers (and hence integers)! Both sets are infinite, but you can construct a mapping from each non-negative integer to and from a corresponding fraction.
- Between any two real numbers of any sort, there is a rational number. The size of the separation does not matter! There always exists a rational number arbitrarily close to a given real. Consider taking a decimal/calculator expansion and chopping it off once it's close enough.

[1] `http://www.webmd.com/a-to-z-guides/features/are-you-mosquito-magnet`

26.4 Review of rational arithmetic

Rational arithmetic is based on integer arithmetic. The following properties will be inherited by multiplication and addition for rationals q, r, and s:

closure $q + r \in \mathbb{Q}$, $qr \in \mathbb{Q}$

commutative $q + r = r + q$, $qr = rq$,

associative $q + (r + s) = (q + r) + s$, $q(rs) = (qr)s$, and

distributive $q(r + s) = qr + qs$.

One homework question is to take the operation definitions below and verify some of these properties.

The following are somewhat formal definitions to show how to construct rationals along strict rules.

26.4.1 Multiplication and division

We start with multiplication and division. Let $a, b, k, x, y \in \mathbb{J}$, so all the variables are *integers*. We will extend these variables to run over the rational numbers shortly.

The definition of **multiplying fractions**:

$$\frac{a}{b} \cdot \frac{x}{y} = \frac{ax}{by}.$$

As an example

$$\frac{3}{7} \cdot \frac{5}{2} = \frac{15}{14}.$$

The definition of a **relationship between division and fractions**:

$$a/b = a \cdot \frac{1}{b} = \frac{a}{b} \quad \text{so} \quad 8/2 = a \cdot \frac{1}{2} = \frac{8}{2}.$$

We need to be a little careful here. Integer division was defined only when $b \mid a$, so this expression formally only holds when $b \mid a$. We relax this restriction later to allow the variables to run over rational numbers.

An important consequence is that

$$a = \frac{a}{1}$$

for all a.

This leads to very useful technique, **expressing 1 as a fraction**:

$$1 = k/k = \frac{k}{k}$$

for any $k \neq 0$. Remember that in the divisibility form $k = 1 \cdot k + 0$, so $k \mid k$ and $k/k = 1$.

Next we show what the text calls "the fundamental property of rational numbers", which is not terribly fundamental. First we show that 1 is the **multiplicative identity for rationals** by using the fact that 1 is the multiplicative identity for integers,

$$\frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}.$$

Using this fact, we show that $\frac{a}{b} = \frac{ak}{bk}$ for any $k \neq 0$,

$$\frac{a}{b} = \frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{k}{k} = \frac{ak}{bk}.$$

Now we introduce **proper fractions**. A proper fraction is a rational $\frac{a}{b}$ where the numerator a and denominator b are relatively prime. That is $\gcd(a, b) = 1$ and they share no common factors. Every fraction is equal to some proper fraction. Given $\gcd(a, b) = d$, we can factor out the common divisor,

$$\frac{a}{b} = \frac{a' \cdot d}{b' \cdot d} = \frac{a'}{b'} \cdot \frac{d}{d} = \frac{a'}{b'}.$$

So for 15 and 35, $(15, 35) = 5$ and

$$\frac{15}{35} = \frac{3 \cdot 5}{7 \cdot 5} = \frac{3}{7}.$$

A fraction that is not proper is **improper**. An improper fraction is a redundant representation, and keeping fractions improper sometimes helps speed operations.

Every rational number with a non-zero numerator has a **multiplicative inverse**. This uses only the expression for 1 and the relationship between integer division and fractions. Using that $a/a = 1$ and commutativity of integer multiplication,

$$1 = (ab)/(ab) = \frac{ab}{ab} = \frac{ab}{ba} = \frac{a}{b} \cdot \frac{b}{a}.$$

So if $a \neq 0$, then $\frac{b}{a}$ is the multiplicative inverse of $\frac{a}{b}$. As an example,

$$\frac{3}{5} \cdot \frac{5}{3} = \frac{15}{15} = 1.$$

With a multiplicative inverse, we can define **division of rationals** analogously to the fractional form of division of integers,

$$\frac{a}{b} \Big/ \frac{x}{y} = \frac{a}{b} \cdot \frac{y}{x} = \frac{ay}{bx}.$$

For example,

$$\frac{3}{5} \Big/ \frac{5}{7} = \frac{3}{5} \cdot \frac{7}{5} = \frac{21}{25}.$$

26.4.2 Addition and subtraction

When adding rational numbers, you must ensure both ratios have the same denominators. This is the same as ensuring measurements are all in the same units; both numerators need measured by the same denominator.

The definition for **adding fractions**:

$$\frac{a}{b} + \frac{x}{y} = \frac{ay}{by} + \frac{bx}{by} = \frac{ay + bx}{by}.$$

Later we will use the least common multiple of b and y to work with a smaller initial denominator. So

$$\frac{1}{2} + \frac{1}{3} = \frac{3}{6} + \frac{2}{6} = \frac{5}{6}.$$

Rational numbers have additive identities:

$$\frac{a}{b} + \frac{0}{b} = \frac{a+0}{b} = \frac{a}{b}.$$

We prefer there to be only one additive identity. We can use the "fundamental property" above to prove that all additive identities are equal to $\frac{0}{1}$:

$$\frac{0}{b} = \frac{0 \cdot b}{1 \cdot b} = \frac{0}{1} \cdot \frac{b}{b} = \frac{0}{1} \cdot 1 = \frac{0}{1}.$$

Given that $1 \mid 0$, $\frac{0}{1} = 0/1 = 0$. So zero is the **additive identity** for rationals as well as integers.

Like integers, rationals have **additive inverses**:

$$\frac{a}{b} + \frac{-a}{b} = \frac{a + -a}{b} = \frac{0}{b} = 0.$$

Given the additive inverse exists, we can define the **negation** of a rational as

$$-\frac{a}{b} = \frac{-a}{b},$$

and then we define **subtraction** in terms of addition as

$$\frac{a}{b} - \frac{x}{y} = \frac{a}{b} + \frac{-x}{y} = \frac{ay - bx}{xy}.$$

So

$$\frac{1}{2} - \frac{1}{3} = \frac{3}{6} + \frac{-2}{6} = \frac{1}{6}.$$

26.4.3 Comparing fractions

We start with some high-level definitions and find the common product rule for comparing fractions.

First, a quick review of integer ordering. We say an integer is **negative** if it has a negative sign, *e.g.* -1. An integer is **positive** if it is neither zero nor negative, or equivalently if the integer is also a counting number. We start an ordering of the integers by saying that a positive $i > 0$, a negative $i < 0$, and $0 = 0$.

Then we can compare two integers i and j by their difference. There are three cases:

- If $i - j > 0$, then $i > j$.
- If $i - j < 0$, then $i < j$.
- Finally, if $i - j = 0$, then $i = j$.

This phrasing may help with the common confusion regarding comparisons and multiplication by negative numbers.

Consider two integers $3 < 5$. That $3 < 5$ implies $3 - 5 < 0$ (and we know it is -2). Now multiply both sides here by -1. If $3 - 5 < 0$, that implies $3 - 5$ is **negative**, and in turn $-1 \cdot (3 - 5) = 5 - 3 = 2$ is **positive**. *Thus multiplying both sides by -1 (and hence any negative number) requires reversing the comparison.* Here $-1 \cdot (3-5) = 5-3 > 0$. But by the distributive property, $-1 \cdot (3-5) = (-3)-(-5)$ as well, so $(-3) - (-5) > 0$ and $-3 > -5$.

Returning to rationals, the integers are a subset, so an order on the rationals should respect the same ordering on the integer subset.

A positive fraction is equal to some fraction where both the numerator and denominator are positive integers. So both the numerator and denominator must have the *same sign*,

$$\frac{3}{5}, \quad \text{or} \quad \frac{-3}{-5} = \frac{3}{5} \cdot \frac{-1}{-1} = \frac{3}{5}.$$

A negative fraction is equal to some fraction where the numerator is negative and the denominator is positive. Here the signs must be *opposite*,

$$\frac{-3}{5}, \quad \text{or} \quad \frac{3}{-5} = \frac{-3}{5} \cdot \frac{-1}{-1} = \frac{-3}{5}.$$

As we saw with the additive identity, a zero fraction is equal to the integer zero and has a zero numerator. The sign of zero does not matter in rational arithmetic (although it may in a computer's floating-point arithmetic).

Given two rationals r and q, r is strictly less than q, $r < q$, if $q - r$ is positive. Thus

$$\frac{q_n}{q_d} - \frac{r_n}{r_d} = \frac{q_n r_d - q_d r_n}{q_d r_d} > 0.$$

We can always move negative signs into the numerator, so we assume that q_d and r_d are positive. **But remember to convert the fraction into having a positive denominator!** Then the above relation

$$q_n r_d - q_d r_n > 0 \quad \text{or, equivalently,} \quad q_n r_d > q_d r_n.$$

So

$$\frac{q_n}{q_d} > \frac{r_n}{r_d} \quad \text{when} \quad q_n r_d > q_d r_n.$$

By symmetry, then we can compare two rational numbers by comparing appropriate products.

- If $q_n r_d > q_d r_n$, then $\frac{q_n}{q_d} > \frac{r_n}{r_d}$.
- If $q_n r_d < q_d r_n$, then $\frac{q_n}{q_d} < \frac{r_n}{r_d}$.
- If $q_n r_d = q_d r_n$, then $\frac{q_n}{q_d} = \frac{r_n}{r_d}$.

Consider comparing $\frac{1}{2}$ and $\frac{1}{3}$,

$$1 \cdot 3 > 1 \cdot 2 \Rightarrow \frac{1}{2} > \frac{1}{3}.$$

And for the negations $\frac{-1}{2}$ and $\frac{-1}{3}$,

$$-1 \cdot 3 < -1 \cdot 2 \Rightarrow \frac{-1}{2} < \frac{-1}{3}.$$

As an example of why you need to force the denominator to be positive, consider $\frac{1}{2}$ and $\frac{-1}{-3}$.

$$1 \cdot -3 < -1 \cdot 2 \not\Rightarrow \frac{1}{2} < \frac{1}{3}.$$

This is because we are in essence multiplying both sides by the product of their denominators. That product is negative, so we would have to flip the sign. It's just as easy to remember to make the denominator positive.

26.5 Complex fractions

So far, the numerator and denominator have been integers. We can loosen the definition slightly and allow **complex fractions** where the numerator and denominator are rational numbers. We extend the division definition to map complex fractions into fractions with integral numerators and denominators,

$$\frac{\frac{a}{b}}{\frac{x}{y}} = \frac{a}{b} / \frac{x}{y} = \frac{a}{b} \cdot \frac{y}{x} = \frac{ay}{bx}.$$

We could use this definition to show that all the arithmetic operations work as expected on complex fractions.

Working with complex fractions sometimes allows adding fractions without using a massive denominator.

Let L be the least common multiple of b and y. Then $b \mid L$ and $y \mid L$, so L/b and L/y are integers. We can manipulate the addition definition slightly by introducing L,

$$\begin{aligned}
\frac{a}{b} + \frac{x}{y} &= \frac{\frac{a}{b}}{1} + \frac{\frac{x}{y}}{1} = \frac{a \cdot \frac{1}{b}}{1} + \frac{x \cdot \frac{1}{y}}{1} \\
&= \frac{L}{L} \cdot \left(\frac{a \cdot \frac{1}{b}}{1} + \frac{x \cdot \frac{1}{y}}{1} \right) \\
&= \frac{a \cdot \frac{L}{b}}{L} + \frac{x \cdot \frac{L}{y}}{L} \\
&= \frac{a(L/b)}{L} + \frac{x(L/y)}{L} \\
&= \frac{a(L/b) + x(L/y)}{L}.
\end{aligned}$$

With $75 = \operatorname{lcm}(15, 25)$,

$$\frac{7}{15} + \frac{8}{25} = \frac{7 \cdot 3 + 8 \cdot 5}{75} = \frac{61}{75}.$$

Quite often there is less work in reducing the result into proper form if you use the least common multiple as the denominator.

26.6 Homework

Practice is absolutely critical in this class.

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

- **Repeated, because I didn't cover the material last week:** Find **two** integer solutions to each of the following, or state why no solutions exist:
  - $64x + 336y = 32$
  - $33x - 27y = 11$
  - $31x - 27y = 11$
- Problem set 6.1 (p354)
  - 2, 6, 11, 12
  - 32

- Problem set 6.2 (p375)
  - 6, 18, 13, 25
- Problem set 6.3 (p389)
  - 2
  - 8, 9
  - 12

Note that you *may* email homework. However, I don't use Microsoft^{TM} products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 27

Solutions for ninth week's assignments

Also available as PDF.

Note: These are my approaches to these problems. There are many ways to tackle each.

27.1 Diophantine equations

See the previous week's solutions.

27.2 Problem set 6.1

Problem 2 I'm not going to draw this, but it should be fairly straight-forward. This was more an exercise in something handy for elementary classes.

Problem 6

- $\frac{20}{60} = \frac{1}{3}$
- $\frac{30}{60} = \frac{1}{2}$
- $\frac{5}{7}$
- $\frac{25}{100} = \frac{1}{4}$
- $\frac{25}{100} = \frac{1}{4}$
- $\frac{3}{12} = \frac{1}{4}$
- $\frac{2}{3}$

- $\frac{3}{4}$ (A quart is made of *quart*ers... There are four cups in a *quart*. Cooking is a source of bizarre but traditional units.)

Problem 11
- $\frac{4}{5} = \frac{6\cdot 4}{6\cdot 5} = \frac{24}{30}$
- $\frac{6}{9} = \frac{3\cdot 2}{3\cdot 3} = \frac{2}{3}$
- $\frac{-7}{25} = \frac{20\cdot -7}{20\cdot 25} = \frac{-140}{500}$
- $\frac{18}{3} = \frac{3\cdot 6}{3\cdot 1} = \frac{6}{1} = \frac{-1\cdot 6}{-1\cdot 1} = \frac{-6}{-1}$

Problem 12
- $\frac{18}{42} = \frac{6\cdot 3}{6\cdot 7} = \frac{3}{7}$.
- Here $(18, 49) = 1$ and $(5, 14) = 1$, so both are in lowest common terms. That form is unique, and these fractions differ, so these **fractions cannot be equal**. Following the text's method, you want to compare $\frac{2\cdot 18}{2\cdot 49} = \frac{36}{98}$ and $\frac{7\cdot 5}{7\cdot 14} = \frac{35}{98}$, because $\text{lcm}(49, 14) = 98$.
- $\frac{9}{25} = \frac{20\cdot 9}{20\cdot 25} = \frac{180}{500} \neq \frac{140}{500}$.
- $\frac{24}{144} = \frac{2}{12} = \frac{1}{6}$, $\frac{32}{96} = \frac{1}{3} = \frac{2}{6}$. **These are not equal.**

Problem 32 Yes, this is a general property. But you need to provide some examples.

27.3 Problem set 6.2

Problem 6
- $\frac{5}{7}$
- $\frac{10}{5} = 2$
- $\frac{20}{24} = \frac{5}{6}$
- $\frac{56}{65}$
- $\frac{76}{60} = \frac{19}{15}$
- $\frac{100}{200} = \frac{1}{2}$
- $\frac{-31}{100}$
- $\frac{321}{450} = \frac{107}{150}$

Problem 18
- 1
- $\frac{1}{4}$
- 1

Problem 13
- $3 \cdot \frac{5}{2} = \frac{15}{2}$
- $\frac{2}{3} \cdot \frac{3}{2} = 1$
- $\frac{3}{4} \cdot 2 = \frac{3}{2}$

Problem 25 For each, you proceed by solving the row, column, or diagonal that has only one open spot. Repeating suffices to fill the squares.

$\frac{1}{2}$	$\frac{1}{12}$	$\mathbf{\frac{5}{12}}$
$\frac{1}{4}$	$\mathbf{\frac{1}{3}}$	$\mathbf{\frac{5}{12}}$
$\mathbf{\frac{1}{4}}$	$\mathbf{\frac{7}{12}}$	$\mathbf{\frac{1}{6}}$

$\mathbf{\frac{8}{15}}$	$\mathbf{\frac{1}{5}}$	$\mathbf{\frac{4}{15}}$
$\mathbf{\frac{1}{15}}$	$\frac{1}{3}$	$\frac{3}{5}$
$\mathbf{\frac{2}{5}}$	$\mathbf{\frac{7}{15}}$	$\frac{2}{15}$

27.4 Problem set 6.3

Problem 2

- Reassociate to add the first two terms with the common denominator of 5 first.
- Commute the terms in the parenthesis and reassociate to add terms with common denominator of 4 first.
- Use the distributive property to pull out the $\frac{2}{3}$, then add the eighths.
- Commute and reassociate to multiply $\frac{3}{4} \cdot \frac{4}{3} = 1$ first.

Problem 8

- $\frac{2}{3} \cdot \frac{4}{7} + \frac{2}{3} \cdot \frac{3}{7} = \frac{2}{3} \cdot (\frac{4}{7} + \frac{3}{7}) = \frac{2}{3} \cdot 1 = \frac{2}{3}$
- $\frac{4}{5} \cdot \frac{2}{3} - \frac{3}{10} \cdot \frac{2}{3} = (\frac{4}{5} - \frac{3}{10}) \cdot \frac{2}{3} = \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$
- $\frac{4}{7} \cdot \frac{3}{2} - \frac{4}{7} \cdot \frac{6}{4} = \frac{4}{7} \cdot (\frac{3}{2} - \frac{6}{4}) = \frac{4}{7} \cdot 0 = 0$
- $(\frac{4}{7} \cdot \frac{2}{5})/\frac{2}{7} = \frac{4 \cdot 2}{7 \cdot 5} \cdot \frac{7}{2} = \frac{4}{5}$

Problem 9

- adding fractions with a common denominator
- multiplying fractions
- distributing multiplication over addition
- adding fractions with a common denominator
- multiplying fractions

Problem 12

- First subtraction of 32, then multiplication by the inverse of $\frac{9}{5}$.
Celsius	-40	-20	0	10	20	45	100
Fahrenheit	-40	-13	32	50	68	104	212

- As seen in the table above, both agree at -40. If $-F = C$, then $-F = \frac{5}{9}(F - 32)$, $\frac{-9}{5}F = F - 32$, $32 = \frac{14}{5}F$, $F = \frac{80}{7} \approx 11$.

Chapter 28

Notes for the tenth week: Irrationals and decimals

Notes also available as PDF.

- exponents, roots, and irrationals
- decimals and percentages
- floating-point arithmetic

exponents, roots, and irrationals

- exponents, rules, etc.
- extending to negative exponents: rationals
- extending to rational exponents leads to roots
- roots to/from exponents

28.1 Real numbers

We won't *define* the real numbers. That requires more time than we can allow here. We will simply use the reals, denoted $\mathbb{R}$, as more than the rationals. This was the state of affairs until around 1872 when Richard Dedekind finally discovered a way to construct real numbers formally.

So the reals fit into our system of sets on the very top,

$$\text{natural numbers } \subsetneq \text{ whole numbers } \subsetneq \mathbb{J} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}.$$

Look up the term "Dedekind cut" for more on actually defining real numbers.

28.2 Exponents and roots

We will cover:

- definition for positive integer exponents,
- rules,
- zero exponents,
- negative exponents, and
- rational exponents and roots.

28.2.1 Positive exponents

We've already used positive exponents when discussing the digit representation of numbers:

$$\begin{aligned} 10 &= 10 && = 10^1 \\ 100 &= 10 \cdot 10 && = 10^2 \\ 1000 &= 10 \cdot 10 \cdot 10 && = 10^3 \\ 10000 &= 10 \cdot 10 \cdot 10 \cdot 10 && = 10^4 \\ \vdots & \quad \vdots & & \vdots \end{aligned}$$

In general, for any number (integer, rational, or real), the number raised to an integer exponent is defined as:

$$\begin{aligned} a^1 &= a, \\ a^2 &= a \cdot a, \\ a^3 &= a \cdot a \cdot a, \\ &\vdots \\ a^k &= \overbrace{a \cdot a \cdot a \cdot \ldots \cdot a}^{k}. \end{aligned}$$

For example,

$$\begin{aligned} 2^3 &= 8, \text{ and} \\ \left(\frac{2}{3}\right)^2 &= \frac{4}{9}. \end{aligned}$$

Negative numbers have signs that bounce around:

$$\begin{aligned}(-5)^1 &= -5,\\ (-5)^2 &= 25,\\ (-5)^3 &= -125, \text{ and}\\ (-5)^4 &= 625.\end{aligned}$$

With the symbolic definition, we can show other properties of exponentiation:

$$\begin{aligned}(ab)^3 &= (ab)\cdot(ab)\cdot(ab)\\ &= (a\cdot a\cdot a)\cdot(b\cdot b\cdot b) \text{ (by commutativity and associativity)}\\ &= a^3\cdot b^3.\end{aligned}$$

In general,

$$(ab)^k = a^k b^k.$$

For example,

$$1000 = 10^3 = (2\cdot 5)^3 = 2^3\cdot 5^3 = 8\cdot 125.$$

Or when multiplying numbers raised to powers, we have that exponents add as in

$$\begin{aligned}a^k\cdot a^m &= \overbrace{a\cdot\ldots\cdot a}^{k}\cdot\overbrace{a\cdot\ldots\cdot a}^{m}\\ &= \overbrace{a\cdot\cdots\cdot a}^{k+m}\\ &= a^{k+m}.\end{aligned}$$

For example,

$$10^2\cdot 10^3 = 100\cdot 1000 = 100000 = 10^5.$$

And numbers raised to powers multiple times multiply exponents as in

$$(a^k)^m = \overbrace{a^k\cdot a^k\cdot a^k\cdot\ldots\cdot a^k}^{m} = a^{km}.$$

For example,

$$100^2 = (10^2)^2 = 10^4 = 10000.$$

28.2.2 Zero exponent

Consider the following relationship between integer exponents and division:

$$\begin{aligned}a^3 &= a^4/a,\\ a^2 &= a^3/a, \text{ and}\\ a^1 &= a^2/a.\end{aligned}$$

Reasoning *inductively*, we suspect that

$$a^0 = a^1/a = 1.$$

Using the rule above for adding exponents along with the additive identity property that $k + 0 = k$, we can *deduce* that

$$a^k = a^{k+0} = a^k \cdot a^0.$$

So for any $a \neq 0$,

$$a^0 = 1 \quad \text{when } a \neq 0.$$

Why can't we define this for $a = 0$? $0^k = 0$ for any integer $k > 0$. So $0 = 0^k = 0^k \cdot 0^0$ does not help to define 0^0; we're left with $0 = 0 \cdot 0^0$. Because $0 \cdot x = 0$ for any x, 0^0 can be anything.

Examples:

$$\begin{aligned} 5^0 &= 1 \\ (-73)^0 &= 1 \\ 0^0 &\text{ is undefined} \ldots \end{aligned}$$

28.2.3 Negative exponents

Continuing *inductively* for $a \neq 0$,

$$\begin{aligned} a^0 &= 1, \\ a^{-1} &= a^0/a = \frac{1}{a}, \text{ and} \\ a^{-2} &= a^{-1}/a = \frac{1}{a} \cdot \frac{1}{a} = \frac{1}{a^2}. \end{aligned}$$

Again, we can use the fact that exponents add to derive this *deductively*:

$$1 = a^0 = a^{k+-k} = a^k \cdot a^{-k},$$

and so a^{-k} is the multiplicative inverse of a^k, and we previously showed that to be $\frac{1}{a^k}$. We have shown that

$$a^{-k} = \frac{1}{a^k}$$

for all $a \neq 0$.

For example:

$$2^{-2} = \frac{1}{2^2} = \frac{1}{4}$$

is the inverse of

$$2^2 = 4.$$

Also,

$$\begin{aligned}\left(\frac{2}{3}\right)^{-1} &= \frac{1}{\frac{2}{3}} \\ &= \frac{3}{2}\end{aligned}$$

is the multiplicative inverse of

$$\frac{2}{3}.$$

And

$$\begin{aligned}\left(\frac{2}{3}\right)^{-2} &= \frac{1}{(\frac{2}{3})^2} \\ &= \frac{1}{\frac{4}{9}} \\ &= \frac{9}{4}\end{aligned}$$

is the multiplicative inverse of

$$\left(\frac{2}{3}\right)^{2} = \frac{2}{3}.$$

28.2.4 Rational exponents and roots

So we've played with division and exponents. Consider now reasoning *inductively* using the multiplication rule for exponents:

$$\begin{aligned}a^4 &= (a^2)^2, \\ a^2 &= (a^1)^2, \text{ and so} \\ a^1 &= (a^{\frac{1}{2}})^2.\end{aligned}$$

We call $a^{\frac{1}{2}}$ the square root of a and write $\sqrt{a}$.

But $\sqrt{a}$ is only defined some of the time. Over integers, there clearly is no integer b such that $b^2 = 2$, so $\sqrt{2}$ is not defined **over the integers** and fractional exponents are **not closed** over integers.

Also, the product of two negative numbers is positive, and the product of two positive numbers is positive, so there is no real number whose square is negative. Hence for real a,

$$\sqrt{a} \text{ is undefined for } a < 0.$$

Remember that $(-b)^2 = (-1)^2 \cdot b^2 = b^2$, so the square root may be either positive or negative!

$$\begin{aligned} 2^2 &= 4, \\ (-2)^2 &= 4, \text{ hence} \\ \sqrt{4} &= \pm 2. \end{aligned}$$

In most circumstances, $\sqrt{a}$ means the positive root, often called the **principal square root**. When you hit a square-root key or apply a square root in a spreadsheet, you get the principal square root.

Other rationals provide other roots:

$$a^1 = (a^{\frac{1}{3}})^3$$

is the cube root,

$$\sqrt[3]{a} = a^{\frac{1}{3}}.$$

Here, though, $(-a)^3 = (-1)^3 \cdot a^3 = -(a^3)$, and there is no worry about the sign of the cube root.

Using $(a^k)^m = a^{km}$, we also have

$$a^{\frac{2}{3}} = \sqrt[3]{a^2} = (\sqrt[3]{a})^2$$

The exponential operator can be defined on more than just the rationals, but we won't go there. However, remember that I mentioned the rationals are *dense* in the reals. There is a rational number close

28.2.5 Irrational numbers

There are more reals than rationals. This is a very non-obvious statement. To justify it, we will

- prove that $\sqrt{2}$ is not rational, and
- generalize that proof to other roots.

Remember the table to show that there are as many integers as rationals? You cannot construct one for the reals. I might show that someday. It's shockingly simple but still a mind-bender. But for now, a few simple examples suffice to make the point.

Theorem: The number $\sqrt{2}$ is not rational.

Proof. Suppose $\sqrt{2}$ were a rational number. Then

$$\sqrt{2} = \frac{a}{b}$$

for some integers a and b. We will show that any such a and b, two must divide both and so $(a, b) \geq 2$. Previously, we explained that any fraction can be reduced to have $(a, b) = 1$. Proving that $(a, b) \geq 2$ shows that we *cannot* write $\sqrt{2}$ as a fraction.

Now if $\sqrt{2} = \frac{a}{b}$, then $2 = \frac{a^2}{b^2}$ and $2b^2 = a^2$. Because $2 \mid 2b^2$, we also know that $2 \mid a^2$. In turn, $2 \mid a^2$ and 2 being prime imply that $2 \mid a$ and thus $a = 2q$ for some integer q.

With $a = 2q$, $a^2 = 4q^2$. And with $a^2 = 2b^2$, $2b^2 = 4q^2$ or $b^2 = 2q^2$. Now $2 \mid b$ as well as $2 \mid a$, so $(a, b) \geq 2$. □

Theorem: Suppose x and n are positive integers and that $\sqrt[n]{x}$ is rational. Then $\sqrt[n]{x}$ is an integer.

Proof. Because $\sqrt[n]{a}$ is rational and positive, there are positive integers a and b such that

$$\sqrt[n]{x} = \frac{a}{b}.$$

We can assume further that the fraction is in lowest terms, so $(a, b) = 1$. Now we show that $b = 1$.

As in the previous proof, $\sqrt[n]{x} = \frac{a}{b}$ implies that $x \cdot b^n = a^n$.

If $b \geq 1$, there is a prime p that divides b. And as before, $p \mid b$ implies $p \mid a$, contradicting the assumption that $(a, b) = 1$. Thus $b = 1$ and $\sqrt[n]{x}$ is an integer. □

With decimal expansions, we will see that rational numbers have repeating expansions. Irrational numbers have decimal expansions that never repeat. There are some fascinating properties of the expansions

Irrational numbers come in two kinds, **algebraic** and **transcendental**. We won't go into the difference in detail, but numbers like $\sqrt{2}$ are algebraic, and numbers like π and e are transcendental.

28.3 Decimal expansions and percentages

Remember positional notation:

$$1\,234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0.$$

Given negative exponents, we can expand to the right of 10^0. General English notation uses a **decimal point** to separate the integer portion of the number from the rest.

So with the same notation,

$$1\,234.567 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0 \\ +5 \cdot 10^{-1} + 6 \cdot 10^{-2} + 7 \cdot 10^{-3}.$$

Operations work in exactly the same digit-by-digit manner as before. When any position goes over 9, a factor of 10 **carries** into the next higher power of 10. If any digit becomes negative, a factor of 10 is **borrowed** frrom the next higher power of 10.

Other languages use a comma to separate the integer from the rest and also use a period to mark off powers of three on the other side, for example

$$1,234.567 = 1.234,567.$$

You may see this if you play with "locales" in various software packages. Obviously, this can lead to massive confusion among travellers. (A price of 1.234 is **not** less than 2 but rather greater than 1000.)

Typical international mathematical and science publications use a period to separate the integer and use a space to break groups of three:

$$1,234.567 = 1\,234.567.$$

28.3.1 Representing rationals with decimals

What is the part to the right of the decimal point? It often is called the **fractional part** of the number, giving away that it is a representation of a fraction.

Here we consider the decimal representation of rational numbers $\frac{1}{a}$ for different integers a. We will see that the expansions fall into two categories:

1. some **terminate** after a few digits, leaving the rest zero; and
2. some **repeat** a trailing section of digits.

For rational numbers, these are the only two possibilities.

We can find the decimal expansions by long division.

Two simple examples that terminate:

$$\begin{array}{r} 0.5 \\ 2 \overline{)\ 1.0} \\ -1.0 \end{array} \qquad\qquad \begin{array}{r} 0.2 \\ 5 \overline{)\ 1.0} \\ -1.0 \end{array}$$

Note that $2 \mid 10$ and $5 \mid 10$, so both expansions terminate immediately with $\frac{1}{2} = .5$ and $\frac{1}{5} = .2$.

Actually, all fractions with a denominator consisting of powers of 2 and five have terminating expansions. For example,

$$\begin{aligned}\frac{1}{2^2} &= \frac{1}{4} = 0.25,\\ \frac{1}{5^3} &= \frac{1}{125} = 0.008, \text{ and}\\ \frac{1}{2\cdot 5^2} &= \frac{1}{50} = 0.02.\end{aligned}$$

What if the denominator a in $\frac{1}{a}$ does not divide 10, or $a \nmid 10$? Then the expansion does not terminate, but it does **repeat**. If the denominator has no factors of 2 or 5, it repeats immediately.

Examples of repeating decimal expansions:

$$\begin{array}{r|l} & 0.33\ldots \\ \hline 3 & 1.000 \\ & -.9 \\ & \ .10 \\ & -\ \ 9 \\ & \ \ \ 10 \end{array} \qquad \begin{array}{r|l} & 0.1428571\ldots \\ \hline 7 & 1.00000000 \\ & -.7 \\ & \ \ 30 \\ & -28 \\ & \ \ \ 20 \\ & -\ 14 \\ & \ \ \ 60 \\ & -\ \ 56 \\ & \ \ \ 40 \\ & -\ \ 35 \\ & \ \ \ 50 \\ & -\ \ 49 \\ & \ \ \ 10 \\ & -\ \ \ 7 \\ & \ \ \ 3 \end{array}$$

We write these with a bar over the repeating portion, as in

$$\begin{aligned}\frac{1}{3} &= 0.\overline{3}, \text{ and}\\ \frac{1}{7} &= 0.\overline{142857}.\end{aligned}$$

We say that $0.\overline{3}$ has a **period** of 1 and $0.\overline{142857}$ has a period of 6.

We could write $0.2 = 0.2\overline{0}$, but generally we say that this **terminates** once we reach the repeting zeros.

If the denominator a contains factors of 2 or 5, the repeating portion occurs a number of places after the decimal. For example, consider $\frac{1}{6} = \frac{1}{2\cdot 3}$ and $\frac{1}{45} = \frac{1}{5\cdot 9}$:

$$\begin{array}{r} 0.166\ldots \\ 6\,\overline{)\,1.0000} \\ -.6 \\ 40 \\ -36 \\ 40 \end{array} \qquad \begin{array}{r} 0.022\ldots \\ 45\,\overline{)\,1.0000} \\ -.90 \\ 100 \\ -90 \\ 10 \end{array}$$

So the decimal representations are

$$\frac{1}{6} = 0.1\overline{6}, \text{ and}$$
$$\frac{1}{45} = 0.0\overline{2}.$$

The hard way to determine the period of a repeating fraction

Note that for all non-negative integer k,

$$\begin{aligned} 10^k &\equiv 0 \pmod 2, \\ 10^k &\equiv 0 \pmod 5, \text{ and} \\ 10^k &\equiv 1 \pmod 3. \end{aligned}$$

These tell us that the expansions have periods of 0, 0, and 1.

For seven,

$$\begin{aligned} 10^0 &\equiv 1 \pmod 7, \\ 10^1 &\equiv 3 \pmod 7, \\ 10^2 &\equiv 2 \pmod 7, \\ 10^3 &\equiv 6 \pmod 7, \\ 10^4 &\equiv 4 \pmod 7, \\ 10^5 &\equiv 5 \pmod 7, \text{ and} \\ 10^6 &\equiv 1 \pmod 7, \end{aligned}$$

so the period is of length 7.

For 45,

$$\begin{aligned} 10^0 &\equiv 1 \pmod{45}, \\ 10^1 &\equiv 10 \pmod{45}, \text{ and} \\ 10^2 &\equiv 10 \pmod{45}. \end{aligned}$$

This is a little more complicated, but the pattern shows that there is one initial digit before hitting a repeating pattern, exactly like the expansion $\frac{1}{45} = 0.0\overline{2}$.

In each case, we are looking for the **order** of 10 modulo the denominator. Finding an integer with a large order modulo another integer is a building block in RSA encryption used in SSL (the `https` prefix in URLs).

28.3.2 The repeating decimal expansion may not be unique!

One common stumbling block for people is that the repeating decimal expansion is not unique.

Let

$$n = 0.\overline{9} = 0.9999\overline{9}.$$

Then multiplying n by 10 shifts the decimal over one but does not alter the pattern, so

$$10n = 9.\overline{9} = 9.9999\overline{9}.$$

Given

$$10n = 9.\overline{9}, \text{ and}$$
$$n = 0.\overline{9},$$

we can subtract n from the former.

$$9n = 9.\overline{9} - 0.\overline{9} = 9.$$

With $9n = 9$, we know $n = 1$. Thus $1 = 0.\overline{9}$!

This is a consequence of sums over infinite sequences, a very interesting and useful topic for another course. But this technique is useful for proving that rationals have repeating expansions.

28.3.3 Rationals have terminating or repeating expansions

Theorem: A decimal expansion that repeats (or terminates) represents a rational number.

Proof. Let n be the number represented by a repeating decimal expansion. Without loss of generality, assume that $n > 0$ and that the integer portion is zero. Now let that expansion have d initial digits and then a period of length p. Here we let a terminating decimal be represented by trailing 0 digits with a period of 1.

For example, let $d = 4$ and $p = 5$. Then n looks like

$$n = 0\,.\,d_1d_2d_3d_4\overline{p_1p_2p_3p_4p_5}.$$

Then $10^d n$ leaves the repeating portion to the right of the decimal. Following our example $d = 4$ and $p = 5$,

$$10^4 n = d_1d_2d_3d_4\,.\,\overline{p_1p_2p_3p_4p_5}.$$

Because it repeats, $10^{d+p}n$ has the same pattern to the right of the decimal. In our running example,

$$10^{4+5}n = d_1d_2d_3d_4p_1p_2p_3p_4p_5\,.\,\overline{p_1p_2p_3p_4p_5}.$$

So $10^{d+p}n - 10^d n$ has zeros to the right of the decimal and is an integer k. In our example,

$$k = 10^{4+5}n - 10^4 n = d_1d_2d_3d_4p_1p_2p_3p_4p_5 - d_1d_2d_3d_4.$$

We assumed $n > 0$, so the difference above is a positive integer. The fractional parts cancel out.

Now $n = \frac{k}{10^{d+p}-10^d}$ is one integer over another and thus is rational. □

Theorem: All rational numbers have repeating or terminating decimal expansions.

Proof. This is a very different style of proof, using what we have called the **pidgeonhole principle**. Without loss of generality, assume the rational number of interest is of the form $\frac{1}{d}$ for some positive integer d.

At each step in long division, there are only d possible remainers. If some remainder is 0, the expansion terminates.

If no remainder is 0, then there are only $d-1$ possible remainders that appear. If the expansion is taken to length d, some remainder must appear twice. Because of the long division procedure, equal remainders leave equal sub-problems, and thus the expansion repeats. □

28.3.4 Therefore, irrationals have non-repeating expansions.

So we know that any repeating or terminating decimal expansion represents a rational, and that all rationals have terminating or repeating decimal expansions.

Thus, we have the following:
Corollary: A number is rational if and only if it has a repeating decimal expansion.

So if there is no repeating portion, the number is *irrational*. One example,

$$0.101001000100001\cdots,$$

has an increasing number of zero digits between each one digit. This number is irrational.

It's beyond our scope to prove that π is irrational, but it is. Thus the digits of π do not repeat.

28.3.5 Percentages as rationals and decimals

Percentage comes from *per centile*, or part per 100. So a direct numerical equivalent to 85% is

$$85\% = \frac{85}{100} = .85.$$

We can expand fractions to include decimals in the numerator and denominator. The decimals are just rationals in another form, and we already explored "complex fractions" with rational numerators and denominators.

So we can express decimal percentages,

$$85.75\% = \frac{85.75}{100} = .8575.$$

Everything else "just works". To convert a fraction into a percentage, there are two routes. One is to convert the denominator into 100:

$$\frac{1}{2} = \frac{50}{100} = 50\%.$$

Another is to produce the decimal expansion and then multiply that by 100:

$$\frac{1}{7} = 0.\overline{142857} = 14.2857\overline{142857}\%.$$

Converting a percentage into a proper fraction required dropping the percentage into the numerator and then manipulating it appropriately:

$$85.75\% = \frac{85.75}{100} = \frac{\frac{8575}{100}}{100} = \frac{8575}{10000} = \frac{343}{400}.$$

28.4 Fixed and floating-point arithmetic

So far we have considered *infinite* expansions, ones that are not limited to a set number of digits. Computers (and calculators) cannot store infinite expansions that do not repeat, and those that do require more overhead than they are worth.

Instead, computers **round** infinite results to have at most a fixed number of **significant digits**. Operations on these limited representations incur some **round-off error**, leading to a tension between computing speed and the precision of computed results. One important fact to bear in mind is that **precision does not imply accuracy**. The following is a very precise but completely in-accurate statement:

> The moon is made of Camembert cheese.

First we'll cover different rounding rules from the perspective of **fixed-point arithmetic**, or arithmetic using a set number of digits to the right of the decimal plce. Then we'll explain **floating-point arithmetic** where the decimal point "floats" through a fixed number of significant digits.

We will not cover the errors in floating-point operations, but we will cover the errors that come from typical binary representation of decimal data.

The points you need to take away from this are the following:

- Using a limited number of digits (or bits) to represent real numbers leads to some inherent, representationall error.
- Representing every-day decimal quantities in binary also incurs some representational error.

Despite the doom-like points above, floating-point arithmetic often provides results that are accurate enough. We won't be able to cover why this is, but the high-level reasons include:

- using far more digits of precision than initially appear necessary, and
- carrying intermediate results to even higher precision.

28.4.1 Rounding rules

Generally, computer arithmetic can be modelled as computing the **exact** result and then rounding that exact result into an economical representation.

truncation or rounding to zero With this rounding method, digits beyond the stored digits are simply dropped.

rounding half-way away from zero This is the text's method of "round half up". A number is rounded to the nearest representable number. In the half-way case, where the digits beyond the number of digits stored are $5000\cdots$, the number is rounded upwards.

rounding half-way to even This is the **preferred** method for rounding in general. A number is rounded to the nearest representable number. In the half-way case, where the digits beyond the number of digits stored are $5000\cdots$, the number is rounded so the final stored digit is **even**.

There are more rounding methods, but these suffice for our discussion. Rounding rules are hugely important in banking and finance, and there are quite a few versions required by different regulations and laws.

Examples of each rounding method above, rounding to two places after the decimal point:

initial number	truncate	round half up	round to nearest even
$\frac{1}{3} = 0.\overline{3}$	0.33	0.33	0.33
$\frac{1}{7} = 0.\overline{142857}$	0.14	0.14	0.14
0.444	0.44	0.44	0.44
0.445	0.44	0.45	0.44
0.4451	0.44	0.45	0.45
0.446	0.44	0.45	0.45
0.455	0.44	0.46	0.46

Rounding error is the absolute difference between the exact number and the rounded, stored representation. In the table above, the rounding error in representing $\frac{1}{3}$ is $|\frac{1}{3} - 0.33| = |\frac{1}{3} - \frac{33}{100}| = |\frac{100}{300} - \frac{99}{300}| = \frac{1}{300} = 0.00\overline{3}$. Note that here the rounding error is 1% of the exact result. That error is large because we use only two digits.

Note that you cannot round in stages. Consider round-to-nearest-even applied to 0.99455 and rounding to two places after the point:

Incorrect	Correct
0.99455	0.99455
0.9946	
0.995	
1.00	0.99

28.4.2 Floating-point representation

Consider repeatedly dividing by 10 in fixed-point arithmetic that carries two digits beyond the decimal:

$$1 \div 10 = 0.10,$$
$$0.1 \div 10 = 0.01,$$
$$0.01 \div 10 = 0.00.$$

So $(\,(\,1 \div 10\,) \div 10\,) \div 10$ evaluates to 0! This phenomenon is called **underflow**, where a number grows too small to be represented. A similar phenomenon, **overflow**, occurs when a number becomes too large to be represented. Computer arithmetics differ on how they handle over- and underflow, but generally overflow produces an ∞ symbol and underflow produces 0.

Floating-point arithmetic compensates for this by carrying a fixed number of **significant** digits rather than a fixed number of fractional digits. The position

of the decimal place is carried in an **explicit, integer exponent**. This allows floating-point numbers to store a wider range and actually makes analysis of the round-off error easier.

In floating-point arithmetic,

$$\begin{aligned} 1 \div 10 &= 1.000 \cdot 10^{0}, \\ 0.1 \div 10 &= 1.000 \cdot 10^{-1}, \\ 0.01 \div 101.000 &\cdot 10^{-2}, \\ &\vdots \end{aligned}$$

This continues until we run out of representable range for the integer exponents. We leave the details of floating-point underflow for another day (if you're unlucky).

28.4.3 Binary fractional parts

Just as integers can be converted to other bases, fractional parts can be converted as well.

Each position to the right of the point (no longer the *decimal* point) corresponds to a power of the base. For binary, the typical computer representation,

$$\begin{aligned} \frac{1}{2} &= 2^{-1} = 0.1_2 = 0.5, \\ \frac{1}{4} &= 2^{-2} = 0.01_2 = 0.25, \\ \frac{1}{8} &= 2^{-3} = 0.001_2 = 0.125. \end{aligned}$$

So a binary fractional part can be expanded with powers of two:

$$0.1101_2 = \frac{1}{2^1} + \frac{1}{2^2} + \frac{0}{2^3} + \frac{1}{2^4} = 0.8125.$$

To find a binary expansion, we need to carry out long division in base 2. I won't ask you to do that.

The important part to recognize is that finite *decimal* expansions may have infinite, repeating *binary* expansions! Remember that in decimal, $2 \mid 10$ and $5 \mid 10$, so negative powers of 2 and 5 have terminating decimal expansions. In binary, only $2 \mid 2$, so only powers of 2 have terminating binary expansions.

Numbers you expect to be exact are not. Consider 0.1. Its binary expansion is

$$0.1 = 0.\overline{00011}_2.$$

A five-bit fixed-point representation would use

$$0.1 \approx 0.00011_2.$$

The error in representing this with a five-digit fixed-point representation is 0.00625, or over 6%.

In a five-bit floating-point representation,

$$0.1 \approx 1.1001_2 \cdot 2^{-4}.$$

The error here is less than 0.0024, or less than 0.24%. You can see what floating-point gains here.

Ultimately, though, in a limited binary fractional representation, adding ten dimes does not equal one dollar! This is why often programs slanted towards finance (*e.g.* spreadsheets) use a form of decimal arithmetic. On current common hardware, decimal arithmetic is implemented in software rather than hardware and is orders of magnitude slower than binary arithmetic.

28.5 Homework

Practice is absolutely critical in this class.

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

- Problem set 7.1 (p421):
  - 1, 2, 3, 4
  - 14
  - 25
  - 28
- Problem set 7.2 (p433):
  - 4
  - 5 (I won't get a chance to cover this, but scientific notation is a good exercise in positional notation and rounding.)
  - 9
- Problem set 7.4 (p457);
  - 2, 3, 4
  - 18
- On rounding and floating point arithmetic:

- Round each of the following to the nearest tenth (one place after the decimal) using **round to nearest even**, **round to zero (truncation)**, and **round half-up**:
  - 86.548
  - 86.554
  - 86.55
- Compute the following quantities with a computer or a calculator. **Write what type of computer/calculator you used and the software package if it's a computer.** Compute it as shown. Do not simplify the expression before computing it, and do not re-enter the intermediate results into the calculator or computer program. Also compute the expressions that do not include 10^{16} by hand exactly. There should be a difference between the exact result and the displayed result in some of these cases. Remember to work from the innermost parentheses outward.
  - $(\overbrace{0.1+0.1+0.1+0.1+0.1+0.1+0.1+0.1+0.1+0.1}^{10\text{ times}})-1$
  - $(\overbrace{(0.1+0.1+0.1+0.1+0.1+0.1+0.1+0.1+0.1+0.1}^{10\text{ times}})-1)\times 10^{16}$, where 10^{16} often is entered as 1e16. If the result overflows (signals an error) on various calculators, replace 10^{16} by 10^8 in this and later portions.
  - $(((2\div 3)-1)\times 3)+1$
  - $((((2\div 3)-1)\times 3)+1)\times 10^{16}$
  - $(((6\div 7)-1)\times 7)+1$
  - $((((6\div 7)-1)\times 7)+1)\times 10^{16}$

  The object of this first part is to demonstrate round-off error. The first to problems, adding 0.1 repeatedly, may see no error if the device calculates in decimal. The latter four parts should see some error regardless of the base used.
- Now copy down the number displayed by the first calculation in each of the following. Re-enter it as x in the second calculation.
  - $1\div 3$, then $1\div 3-x$ where x is the number displayed.
  - If you have a calculator or program with π, π, then $\pi-x$ where x is the number displayed.

  The object here is to see that the number displayed often is not the number the computer or calculator has stored.

Note that you *may* email homework. However, I don't use Microsoft™ products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.

Chapter 29

Second exam and solutions

Available as PDF.

Chapter 30

Third exam, *due 1 December*

Available as PDF. Remember, this is due on **1 December, 2008**.

Chapter 31

Third exam solutions

Available as PDF.

Chapter 32

Final exam

Available as PDF. As a warning, there are typos.

Part IV

Resources

Chapter 33

Math Lab

See the Math Lab Information Sheet for details.

Room 209 of the J. F. Hicks Memorial Library. Tutoring and additional material.
Run by Prof. Charlotte Ingram.

Chapter 34

On-line

As with all things, question the provenance of on-line resources before relying upon them. This list is not comprehensive and does not provide endorsements; this list is just a starting point.

34.1 Educational Standards

- Virginia DOE Standards of Learning resources for mathematics
- National Council of Teachers of Mathematics standards

34.2 General mathematics education resources

Encyclopedia:

- Planet Math
- Wolfram Mathworld

Texts:

- Wikibooks
- George Cain's list of online mathematics textbooks
- Alex Stef(?)'s list of texts

Education and Coursework:

- The Math Forum
- Internet School Library Media Center Mathematics Resources K-12

- Math Archive's K-12 Teaching Materials
- Mathematics Association of America's professional development resources
- Elementary?: Maths is Fun (British, obviously)
- Late high school through graduate: Webcast@Berkeley, MIT Open CourseWare
- Everyday items: SIAM's Math Matters! publications
- others...

34.3 Useful software and applications

This list is for future reference. Each item has a somewhat steep learning curve that is outside our scope. These may not be immediately useful for this course, but they can be useful for playing with ideas quickly.

Exploratory and programming environments:

- Linear algebra: Octave
- Statistics: R
- Geometry: Geomview
- Algebra: Maxima, YACAS, others...
- Spreadsheet: OpenOffice, SIAG, others... Note: spreadsheets often are made notorious for their poor quality arithmetic.