

Problem Set 3

Due: February 25

Reading: Chapter 5.1–5.2, Chapter 6

Latest times for comments on different sections are indicated in the online tutor problem set TP.4.

Problem 1.

haha → In this problem you will prove a fact that may surprise you —or make you even more convinced that set theory is nonsense: the half-open unit interval is actually the *same size* as the nonnegative quadrant of the real plane!¹ Namely, there is a bijection from $(0, 1]$ to $[0, \infty)^2$.

(a) Describe a bijection from $(0, 1]$ to $[0, \infty)$.

Hint: $1/x$ almost works.

(b) An infinite sequence of the decimal digits $\{0, 1, \dots, 9\}$ will be called *long* if it has infinitely many occurrences of some digit other than 0. Let L be the set of all such long sequences. Describe a bijection from L to the half-open real interval $(0, 1]$.

Hint: Put a decimal point at the beginning of the sequence.

(c) Describe a surjective function from L to L^2 that involves alternating digits from two long sequences. a
Hint: The surjection need not be total.

(d) Prove the following lemma and use it to conclude that there is a bijection from L^2 to $(0, 1]^2$.

Lemma 1.1. *Let A and B be nonempty sets. If there is a bijection from A to B , then there is also a bijection from $A \times A$ to $B \times B$.*

(e) Conclude from the previous parts that there is a surjection from $(0, 1]$ and $(0, 1]^2$. Then appeal to the Schröder-Bernstein Theorem to show that there is actually a bijection from $(0, 1]$ and $(0, 1]^2$.

(f) Complete the proof that there is a bijection from $(0, 1]$ to $[0, \infty)^2$.

Problem 2.

A group of $n \geq 1$ people can be divided into teams, each containing either 4 or 7 people. What are all the possible values of n ? Use induction to prove that your answer is correct.

Problem 3.

Claim 3.2. *If a sequence of positive integers has sum $n \geq 1$, then the product of elements in the sequence is at most $3^{n/3}$.*

For example, the sequence 2, 2, 3, 4, 4, 7, has the sum:

$$2 + 2 + 3 + 4 + 4 + 7 = 22,$$

and sure enough, the product is:

$$2 \cdot 2 \cdot 3 \cdot 4 \cdot 4 \cdot 7 = 1344$$

$$\leq 3^{22/3}$$

$$\approx 3154.2, ; .$$

(a) Use strong induction to prove that $n \leq 3^{n/3}$ for every integer $n \geq 0$.

(b) Prove the claim by induction.

Hint: Use induction on the length of the sequence rather than on the value of the sum.

Problem 4.

A sequence of numbers is *weakly decreasing* when each number in the sequence is \geq the numbers after it. (This implies that a sequence of just one number is weakly decreasing.)

Here's a bogus proof of a very important true fact, every integer greater than 1 is a *product of a unique weakly decreasing sequence of primes* — a *pusp*, for short.

Explain what's bogus about the proof.

Lemma 4.3. Every integer greater than 1 is a pusp.

For example, $252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$

Bogus proof. We will prove Lemma 4.3 by strong induction, letting the induction hypothesis, $P(n)$, be n is a pusp.

So Lemma 4.3 will follow if we prove that $P(n)$ holds for all $n \geq 2$.

Base Case: ($n = 2$) $P(2)$ is true because 2 is prime, and so it is a length one product of primes, and this is obviously the only sequence of primes whose product can equal 2.

Inductive step: Suppose that $n \geq 2$ and that i is a pusp for every integer i where $2 \leq i < n + 1$. We must show that $P(n + 1)$ holds, namely, that $n + 1$ is also a pusp. We argue by cases:

If $n + 1$ is itself prime, then it is the product of a length one sequence consisting of itself. This sequence is unique, since by definition of prime, $n + 1$ has no other prime factors. So $n + 1$ is a pusp, that is $P(n + 1)$ holds in this case.

Otherwise, $n + 1$ is not prime, which by definition means $n + 1 = km$ for some integers k, m such that $2 \leq k, m < n + 1$. Now by the strong induction hypothesis, we know that k and m are pusps. It follows immediately that by merging the unique prime sequences for k and m , in sorted order, we get a unique weakly decreasing sequence of primes whose product equals $n + 1$. So $n + 1$ is a pusp, in this case as well.

So $P(n + 1)$ holds in any case, which completes the proof by strong induction that $P(n)$ holds for all $n \geq 2$.

Handwritten notes:

$n=2 \rightarrow 3 = 2 \cdot 1$

$n=3 \rightarrow 4 = 2 \cdot 2$

$n=4 \rightarrow 5 = 3 \cdot 2$

Can be more than 2 (regular int)

So recursive in

~~3 can not be $k \cdot m$~~

Oh is prime!

prime prime

not even right prime itself

Doing P-set 3

2/23

Not related but mod

↳ residue of $b \pmod{m}$

$\text{Mod}[m, n]$ is remainder $\frac{m}{n}$

That's what I thought

I don't get this problem at all!

A bit??

But thought need lot of discrete objects

b) What is this ∞ seq - ∞ deep

Oh can have recurrences

∞ set stuff is silly!

Did not practice at all

? What does a decimal point in front of seq do?

Writing same thing for everything!

c) ? Alternating digits ?

d) well what does it mean to multiply sets

- multiply each part in?

e) and in c) how can it be smaller?

②

f) Have abs no clue

Go to OH

1. Half-open unit interval

- unit interval $(0,1)$

- half open $(0,1]$

- open = ^{endpoints} not include $(0$

- closed = endpoint included $[0$

Non negative quadrant of real plane

$[0, \infty)^\infty$

a) Bij $[0,1] \rightarrow [0,\infty)^2$

Both are sets of infinite size, This means that they are both the same size so

$$|A| = |B|$$

A bij B

c) ~~L surj L^2~~

~~L surj L^2 means $\|L\| \geq \|L^2\|$~~

~~And this makes sense because $\|L^2\| = \|L\| \cdot \|L\|$~~

$$\|L\| \geq \|L\| \cdot \|L\|$$

$$\|L\|$$

$$1 \geq \|L\|$$

x a function that maps el from one set to another

$$\begin{array}{ccc} 1 & x^2 & 1 \\ 2 & \rightarrow & 4 \\ 3 & & 9 \end{array}$$

$f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ = bijection relation

$0, \infty$ case don't matter -excluded

$\frac{1}{x}$ works

$$\frac{1}{x} \neq 1$$

b) $999999 \rightarrow .999999$
 $\cdot 10^\infty$

$x \rightarrow .x$

c) $x_1, y_1, x_2, y_2, x_3, y_3 \rightarrow \cdot x_1, y_1, x_2$

$\overline{.9} \rightarrow \overline{.98}$
 $.8$

$\hookrightarrow \mathbb{I}$'s el of L

$(\overline{.9}, .8) \in L^2$

every $L^2 \rightarrow L$

2)

Proved bij $L \rightarrow [0,1]$

If know $A \leftrightarrow B$
 $A^2 \leftrightarrow B^2$ then by lemma

$$L \leftrightarrow [0,1]$$
$$L^2 \leftrightarrow [0,1]^2$$

Totally sep

Are of equal size

$$(a_i, a_j) \leftrightarrow (b_i, b_j)$$

Put all together

2. Strong induction

Look at 4Tve # 3

I don't know why I am doing sep sheet

? Circular conformation,

Is this even what supposed to or too basic?

3. This claim
Strong induction
Then normal ind

I would no normal ind

'This specific sequence', Oh no missed 1st part

$$n=2$$

$$1+1 \leq 3^{2/3}$$

$$2 \leq \approx 2.08$$

~~1~~

$$1+2 \leq 3$$

Am I simplifying what this is too much?
* know exponentiation rules

Now how to do by strong induction

Why would you want to do this?

Does proof by induction always use cases?

4. Weakly \downarrow if each $\# \geq \#$ after it

Bogus proof #3 hit on google is this P-set!

Every $\mathbb{Z} > 1$ is product of unique weakly decreasing
seq of prime

$$252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$$

? is that not ? 's

$$7 \cdot 3 \cdot 3 \cdot 2 \cdot 2$$

↑ can repeat $\# \geq$

See assignment sheet

~~$n=4$~~ ~~$5=$~~

$n=5$ $6 = 3 \cdot 2$

↑ ↑
P P

$n=6$ $7 = \text{prime}$

$n=7$ $8 = 4 \cdot 2$

↑ ↑ P

$2 \cdot 2$

↑ P ↑ P

Well fact is true

But proof is not

Where do proofs usually go south?

②

Somewhere from 1 step to another

i is psp - everything below $n+1$

- Unneeded

- will make things slow

But I don't think is problem

? Do you even use strong ind

- yeah use prior values

? Go from 2 to 3

? is prime

4

Don't know

4.

Math

Used seq ind - not string

Might be more than one k, m

252 is $4 \cdot 63$
or $36 \cdot 7$

both have $k =$

does not prove that they are $=$

Two list combine

Not unique weekly \downarrow set

Student's Solutions to Problem Set 3

Your name:	Michael Plasmeier			
Due date:	February 25			
Submission date:	2/25			
Circle your TA/LA:	Ali	Nick	Oscar	<u>Oshani</u>

Collaboration statement: Circle one of the two choices and provide all pertinent info.

1. I worked alone and only with course materials.
2. I collaborated on this assignment with:

got help from:¹

and referred to:²

Wolfcam MathWorld: Interval
WP: Prime

DO NOT WRITE BELOW THIS LINE

Problem	Score
1	5
2	4
3	6
4	3.5
Total	18.5

1/40

¹People other than course staff.

²Give citations to texts and material other than the Spring '11 course materials.

Need a function that maps from one set to another

$$(0, 1] \leftrightarrow [0, \infty)$$

$\frac{1}{x}$ does not work

So do $\frac{1}{x} - 1$

0	→	don't need to include
.01	→	100
.11	→	10
.11	→	9
1	→	$\frac{1}{1} = 1$

- 99
- 9
- 8
- 0

So do $\frac{1}{x} - 1$



b) ∞ seq of decimal digits $\{0, 1, \dots, 9\}$
 "Long" if has ∞ many occurrences of digit beside $0=L$
 Bij from L to $(0, 1]$

If the sets are both infinite, then they are
the same size.

*↪ You can't do this
 if A & B are
 infinite!*

So $|A| = |B|$
 A bij B

For example from $999999 \rightarrow .99999$

Which is $\cdot 10^\infty$

$x \rightarrow .x$

C) L^2 surj L

$x_1, y_1, x_2, y_2, x_3, y_3, \dots \rightarrow (x_1, y_1, x_2, y_2, x_3, y_3, \dots)$

$\begin{pmatrix} 9 \\ 8 \end{pmatrix} \rightarrow \overline{\begin{pmatrix} 9 \\ 8 \end{pmatrix}}$
↑ Is an element of L

Every
 $L^2 \rightarrow L$

$(\overline{9}, \overline{8})$ is an element of L^2

$$\|L^2\| \geq \|L\|$$

$$\|L^2\| = \|L\| \|L\|$$

$$\frac{\|L\| \|L\|}{\|L\|} \geq \frac{\|L\|}{\|L\|}$$

$$\|L\| \geq 1$$

d) A, B non empty sets

If A bi; B , then $A \circ A$ bi; $B \circ B$

A bi; B

means

$$|A| = |B|$$

square both sides

$$|A|^2 = |B|^2$$

$$|A^2| = |B^2|$$

A^2 bi; B^2

$A \circ A$ bi; $B \circ B$

Both are of the same size

$$(a_1, a_2, a_3, \dots) \leftrightarrow (b_1, b_2, b_3, \dots)$$

$$(a_i, a_j) \leftrightarrow (b_i, b_j)$$

e) Show that $(0,1] \text{ surj } (0,1]^2$

$$|(0,1]| \geq |(0,1]^2$$

Infinite sets have the same # of elements in each

So there is a bij between them

No they do not.

For example, \mathbb{Q} + \mathbb{R} are infinite but no bijection between them exists

So if $(0,1] \text{ surj } (0,1]^2$ and $(0,1]^2 \text{ surj } (0,1]$

Schröder-Bernstein Theorem

(c) Proof $(0, 1] \text{ bij } [0, \infty)^2$

Bring it all together

$$(0, 1] \leftrightarrow [0, \infty)$$

$$\text{by } \frac{1}{x} - 1$$

~~Proof by induction~~

~~The relationship $a \rightarrow b$ is $\frac{1}{x} - 1$~~

~~Base case~~

~~$x =$~~

~~not an integer~~

And two sets of infinite size are of the same size so a bijective function can be defined for them

Saving an infinite set keeps it the same size

Michael Plasmeier

P-Set 3

Oshani

Table 12

#2 Strong induction

4
see solution

First try first few value

$n=1$ x $1 \bmod 4 = 0$ OR $1 \bmod 7 = 0$

$n=2$ x $n \bmod 4 = 0$ OR $n \bmod 7 = 0$

$n=3$ x

$n=4$ ✓

$n=5$ x

$n=6$ x

$n=7$ ✓

$n=8$ ✓

Basically if multiple of 4 or 7 x also combination of them like

multiples of 4: 4, 8, 12, 16, 20, ...

multiples of 7: 7, 14, 21, 28

11, 15
18 - - -

Hypothesis $S(n)$ = multiples of 4 or 7 can be divided into teams of 4 or 7 players

$n \bmod 4 = 0$ OR $n \bmod 7 = 0$ x

there are more

~~also not induction~~

②.

Base cases

$n=4$ works

$S(4)$

$$4 \bmod 4 = 0 \quad \checkmark$$

$n=7$ works

$S(7)$

$$7 \bmod 7 = 0 \quad \checkmark$$

Inductive step

Strong hypothesis $S(n)$ for n divisible 4 or n divisible 7

By cases: 1. n 's divisible by 4

Assume works for n

$$n+4 \bmod 4 \stackrel{!}{=} 0$$

$$\begin{array}{r} n \bmod 4 = + 4 \bmod 4 \\ 0 \quad \quad + 0 = 0 \quad \checkmark \end{array}$$

Case 2: n 's divisible by 7

$$n+7 \bmod 7 \stackrel{!}{=} 0$$

$$\begin{array}{r} n \bmod 7 + 7 \bmod 7 \\ 0 + 0 = 0 \quad \checkmark \end{array}$$

③.

So it follows by strong induction that n divisible by 4 or 7 can be divided into teams each containing either 4 or 7 people

Michael Plasmeier

6 P-Set 3

Oshani

Table 12

3 Proof by strong induction for $n \geq 0$

$$S(n) ::= n \leq 3^{n/3}$$

Base case ($n=0$)

$$0 \leq 3^{0/3}$$

$$0 \leq 1$$

($n=1$)

$$1 \leq 3^{1/3}$$

$$1 \leq 1.44$$

($n=2$)

$$2 \leq 3^{2/3}$$

$$2 \leq 2.08$$

($n=3$)

$$3 \leq 3^{3/3}$$

$$3 = 3$$

($n=4$)

$$4 \leq 3^{4/3}$$

$$4 \leq 4.32$$

②

$$(n=5) \quad 5 \leq 3^{5/3}$$

$$5 \leq 6.24$$

(n=6)

$$6 \leq 3^{6/3}$$

$$6 \leq 9$$

Inductive Case

Assuming $s(0), s(1), s(2), \dots, s(n)$

Can get $s(n+1)$

$$n+1 \leq 3^{(n+1)/3}$$

$$n+1 \leq 3^{n/3 + 1/3}$$

$$n+1 \leq 3^{n/3} + 3^{1/3}$$

$$n+1 \leq 3^{n/3} + 1$$

-1

-1

$$n \leq 3^{n/3}$$

how do you know the inequality still holds when you make this substitution??

-2

Proved by induction

③

b) Proof by induction

$S(m) ::=$ If a sequence of positive integers has
sum $n \geq 1$ then product is at most $3^{n/3}$

$m = \#$ of integers in sequence

Base case ($m=1$)

$$1 \leq 3^{n/3}$$

$$1 \leq 3$$

$$1 \leq 2.444$$

But could also do

$$100 \leq 3^{100/3}$$

$$\approx 8 \cdot 10^{15}$$

So smaller values are better ...

Inductive case

Assume $S(m)$ is true for $m \geq 1$

④

So $S(m+1)$ should also be true

$$\underbrace{1 + 1 + 1 + \dots + 1}_m + 1$$

← are these 1 or 2?

$$\leq 3^{(m+1)/3}$$

$$\leq 3^{\frac{m}{3} + \frac{1}{3}}$$

$$\leq 3^{\frac{m}{3}} + 3^{\frac{1}{3}}$$

$$\leq 3^{m/3} + 1$$

If they're 1s, why?

If they're 2s, why are they all the same?

Need to be able to add any integers on the sequence.

Right idea, though.

-2

Thus if $S(m)$, then so is $S(m+1)$. Proved by induction

1. What is the purpose of the
 2. What is the purpose of the
 3. What is the purpose of the

4. What is the purpose of the
 5. What is the purpose of the

6. What is the purpose of the
 7. What is the purpose of the

8. What is the purpose of the

9. What is the purpose of the

10. What is the purpose of the

Michael Plasmeier

P-set 3

Oshani

Table 12

#4

∴ You do not need the step through all of the integers i each time you increase by 1
Would make calculation slower] ?

∴ There are multiple possible values for k, m

For example 252 could be $4 \cdot 63$

or $36 \cdot 7$

You never ~~prove which it is or~~ that they are equivalent, so it is not a unique set.

+73⁵

could be clearer;
see solutions!

Solutions to Problem Set 3

Reading: Chapter 5.1–5.2, Chapter 6

Latest times for comments on different sections are indicated in the online tutor problem set TP.4.

Problem 1.

In this problem you will prove a fact that may surprise you —or make you even more convinced that set theory is nonsense: the half-open unit interval is actually the *same size* as the nonnegative quadrant of the real plane!¹ Namely, there is a bijection from $(0, 1]$ to $[0, \infty)^2$.

(a) Describe a bijection from $(0, 1]$ to $[0, \infty)$.

Hint: $1/x$ almost works.

Solution. $f(x) ::= 1/x$ defines a bijection from $(0, 1]$ to $[1, \infty)$, so $g(x) ::= f(x) - 1$ does the job. ■

(b) An infinite sequence of the decimal digits $\{0, 1, \dots, 9\}$ will be called *long* if it has infinitely many occurrences of some digit other than 0. Let L be the set of all such long sequences. Describe a bijection from L to the half-open real interval $(0, 1]$.

Hint: Put a decimal point at the beginning of the sequence.

Solution. Putting a decimal point in front of a long sequence defines a bijection from L to $(0, 1]$. This follows because every real number in $(0, 1]$ has a unique long decimal expansion. Note that if we didn't exclude the non-long sequences, namely, those sequences ending with all zeroes, this wouldn't be a bijection. For example, the sequences $1000\dots$ and $099999\dots$ would both map to the same real number, namely, $1/10$. ■

(c) Describe a surjective function from L to L^2 that involves alternating digits from two long sequences. a
Hint: The surjection need not be total.

Solution. Given any long sequence $s = x_0, x_1, x_2, \dots$, let

$$h_0(s) ::= x_0, x_2, x_4, \dots$$


be the sequence of digits in even positions. Similarly, let

$$h_1(s) ::= x_1, x_3, x_5, \dots$$

be the sequence of digits in odd positions. Then h is a surjective function from L to L^2 , where

$$h(s) ::= \begin{cases} (h_1(s), h_2(s)), & \text{if } h_1(s) \in L \text{ and } h_2(s) \in L, \\ \text{undefined,} & \text{otherwise.} \end{cases} \quad (1)$$

(d) Prove the following lemma and use it to conclude that there is a bijection from L^2 to $(0, 1]^2$.

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer .

¹The half open unit interval, $(0, 1]$, is $\{r \in \mathbb{R} \mid 0 < r \leq 1\}$. Similarly, $[0, \infty) ::= \{r \in \mathbb{R} \mid r \geq 0\}$.

Lemma 1.1. Let A and B be nonempty sets. If there is a bijection from A to B , then there is also a bijection from $A \times A$ to $B \times B$.

Solution. Proof. Suppose $f : A \rightarrow B$ is a bijection. Let $g : A^2 \rightarrow B^2$ be the function defined by the rule $g(x, y) = (f(x), f(y))$. It is easy to show that g is a bijection:

- **g is total:** Since f is total, $f(a_1)$ and $f(a_2)$ exist $\forall a_1, a_2 \in A$ and so $g(a_1, a_2) = (f(a_1), f(a_2))$ also exists.
- **g is surjective:** Since f is surjective, for any $b_i \in B$ there exists $a_i \in A$ such that $b_i = f(a_i)$. So for any $(b_1, b_2) \in B^2$, there are is a pair $(a_1, a_2) \in A^2$ such that $g(a_1, a_2) ::= (f(a_1), f(a_2)) = (b_1, b_2)$. This shows that g is a surjection.
- **g is injective:**

$$\begin{aligned} g(a_1, a_2) = g(a_3, a_4) & \text{ iff } (f(a_1), f(a_2)) = (f(a_3), f(a_4)) && \text{(by def of } g\text{)} \\ & \text{ iff } f(a_1) = f(a_3) \text{ AND } f(a_2) = f(a_4) \\ & \text{ iff } a_1 = a_3 \text{ AND } a_2 = a_4 \text{ (since } f \text{ is injective)} \\ & (a_1, a_2) = (a_3, a_4), \end{aligned}$$

which confirms that g is injective. ■

Since it was shown in part (b) that there is a bijection from L , to $(0, 1]$, an immediate corollary of Lemma 1.1 is that there is a bijection from L^2 to $(0, 1]^2$. ■

(e) Conclude from the previous parts that there is a surjection from $(0, 1]$ and $(0, 1]^2$. Then appeal to the Schröder-Bernstein Theorem to show that there is actually a bijection from $(0, 1]$ and $(0, 1]^2$.

Solution. There is a bijection between $(0, 1]$ and L by part (b), a surjective function from L to L^2 and by part (c), and a bijection from L^2 to $(0, 1]^2$ by part (d). These jections compose to yield a surjection from $(0, 1]$ to $(0, 1]^2$.

Conversely, there is obviously a surjective function $f : (0, 1]^2 \rightarrow (0, 1]$, namely

$$f((x, y)) ::= x.$$

The Schröder-Bernstein Theorem now implies that there is a bijection from $(0, 1]$ to $(0, 1]^2$. ■

(f) Complete the proof that there is a bijection from $(0, 1]$ to $[0, \infty)^2$.

Solution. There is a bijection from $(0, 1]$ to $(0, 1]^2$ by part (e), and there is a bijection from $(0, 1]^2$ to $[0, \infty)^2$ by parts (a) and Lemma 1.1. These bijections compose to yield a bijection from $(0, 1]$ to $[0, \infty)^2$. ■

Problem 2.

A group of $n \geq 1$ people can be divided into teams, each containing either 4 or 7 people. What are all the possible values of n ? Use induction to prove that your answer is correct.

Study

Solution. We begin by observing that the following numbers of people can be divided into teams with 4 or 7 people per team:

$$\begin{aligned}
 4 &= 4 \\
 7 &= 7 \\
 8 &= 4 + 4 \\
 11 &= 4 + 7 \\
 12 &= 4 + 4 + 4 \\
 14 &= 7 + 7 \\
 15 &= 4 + 4 + 7 \\
 16 &= 4 + 4 + 4 + 4 \\
 18 &= 4 + 7 + 7 \\
 19 &= 4 + 4 + 4 + 7 \\
 20 &= 4 + 4 + 4 + 4 + 4 \\
 21 &= 7 + 7 + 7,
 \end{aligned}$$

and these are the only numbers ≤ 21 that can be divided into such teams. Now we claim that every group of $n \geq 18$ people can be divided into teams, each containing either 4 or 7 people.

Proof. The proof is by strong induction on n . Let $P(n)$ be the proposition that a group of $n \geq 18$ people can be divided into teams, with each containing either 4 or 7 people.

Base cases: As shown above $P(18)$, $P(19)$, $P(20)$, and $P(21)$ are true.

Inductive step: For all $n \geq 21$, we assume that $P(18)$, $P(19)$, \dots , $P(n)$ are true in order to prove that $P(n + 1)$ is true.

Since $n + 1 = (n - 3) + 4$, a team of 4 people can be removed from the set of $n + 1$ people, leaving $n - 3 \geq 18$ people. By induction hypothesis, the $n - 3$ people can be further divided into disjoint teams with 4 or 7 people. Since this divides the $n + 1$ people into teams with 4 or 7, we have shown that $P(n + 1)$ is true. It follows by strong induction that $P(n)$ holds for all $n \geq 18$.

So all the possible values of n are 4, 7, 8, 11, 12, 14, 15, 16, and ≥ 18 . ■

Problem 3.

Claim 3.2. *If a sequence of positive integers has sum $n \geq 1$, then the product of elements in the sequence is at most $3^{n/3}$.*

For example, the sequence 2, 2, 3, 4, 4, 7, has the sum:

$$2 + 2 + 3 + 4 + 4 + 7 = 22,$$

and sure enough, the product is:

$$\begin{aligned}
 2 \cdot 2 \cdot 3 \cdot 4 \cdot 4 \cdot 7 &= 1344 \\
 &\leq 3^{22/3} \\
 &\approx 3154.2, ;.
 \end{aligned}$$

(a) Use strong induction to prove that $n \leq 3^{n/3}$ for every integer $n \geq 0$.

Solution. The proof is by strong induction. Let $P(n)$ be the proposition that $n \leq 3^{n/3}$. First, we show that $P(0)$, $P(1)$, $P(2)$, $P(3)$, and $P(4)$ are true:

$$0^3 \leq 3^0 \rightarrow 0 \leq 3^{0/3}$$

$$1^3 \leq 3^1 \rightarrow 1 \leq 3^{1/3}$$

$$2^3 \leq 3^2 \rightarrow 2 \leq 3^{2/3}$$

$$3^3 \leq 3^3 \rightarrow 3 \leq 3^{3/3}$$

$$4^3 \leq 3^4 \rightarrow 4 \leq 3^{4/3}$$

Each implication follows by taking cube roots. Next, we show that $P(0), \dots, P(n)$ imply $P(n+1)$ for all $n \geq 4$. Thus, we assume that $P(0), \dots, P(n)$ are all true and reason as follows:

$$\begin{aligned} 3^{(n+1)/3} &= 3 \cdot 3^{(n-2)/3} \\ &\geq 3 \cdot (n-2) \\ &\geq n+1 \quad (\text{for all } n \geq 7/2) \end{aligned}$$

The first step is algebra. The second step uses our assumption $P(n-2)$. The third step is a linear inequality that holds for all $n \geq 7/2$. (This forced us to deal individually with the cases $P(3)$ and $P(4)$, above.) Therefore, $P(n+1)$ is true, and so $P(n)$ is true for all $n \geq 0$ by induction. ■

(b) Prove the claim by induction.

Hint: Use induction on the *length of the sequence* rather than on the value of the sum.

Solution. We use induction on the length of the sequence. Let $P(k)$ be the proposition that every sequence of k positive integers with sum n has product at most $3^{n/3}$. First, note that $P(1)$ is true by the preceding problem part.

Next, we must show that $P(k)$ implies $P(k+1)$ for all $k \geq 1$. So assume that $P(k)$ is true, and let x_1, \dots, x_{k+1} be a sequence of $k+1$ positive integers with sum n . Then we can reason as follows:

$$\begin{aligned} x_1 \cdot x_2 \cdots x_k \cdot x_{k+1} &\leq 3^{(n-x_{k+1})/3} \cdot x_{k+1} \\ &\leq 3^{(n-x_{k+1})/3} \cdot 3^{x_{k+1}/3} \\ &= 3^{n/3} \end{aligned}$$

The first step uses the assumption $P(k)$, the second uses the preceding problem part, and the last step is algebra. This shows that $P(k+1)$ is true, and so the claim holds by induction. ■

Problem 4.

A sequence of numbers is *weakly decreasing* when each number in the sequence is \geq the numbers after it. (This implies that a sequence of just one number is weakly decreasing.)

Here's a bogus proof of a very important true fact, every integer greater than 1 is a *product of a unique weakly decreasing sequence of primes* — a pusp, for short.

Explain what's bogus about the proof.

Lemma 4.3. *Every integer greater than 1 is a pusp.*

For example, $252 = 7 \cdot 3 \cdot 3 \cdot 2 \cdot 2$, and no other weakly decreasing sequence of primes will have a product equal to 252.

Bogus proof. We will prove Lemma 4.3 by strong induction, letting the induction hypothesis, $P(n)$, be

n is a pusp.

So Lemma 4.3 will follow if we prove that $P(n)$ holds for all $n \geq 2$.

Base Case ($n = 2$): $P(2)$ is true because 2 is prime, and so it is a length one product of primes, and this is obviously the only sequence of primes whose product can equal 2.

Inductive step: Suppose that $n \geq 2$ and that i is a pusp for every integer i where $2 \leq i < n + 1$. We must show that $P(n + 1)$ holds, namely, that $n + 1$ is also a pusp. We argue by cases:

If $n + 1$ is itself prime, then it is the product of a length one sequence consisting of itself. This sequence is unique, since by definition of prime, $n + 1$ has no other prime factors. So $n + 1$ is a pusp, that is $P(n + 1)$ holds in this case.

Otherwise, $n + 1$ is not prime, which by definition means $n + 1 = km$ for some integers k, m such that $2 \leq k, m < n + 1$. Now by the strong induction hypothesis, we know that k and m are pusps. It follows immediately that by merging the unique prime sequences for k and m , in sorted order, we get a unique weakly decreasing sequence of primes whose product equals $n + 1$. So $n + 1$ is a pusp, in this case as well.

So $P(n + 1)$ holds in any case, which completes the proof by strong induction that $P(n)$ holds for all $n \geq 2$. ■

Solution. The problem is that even if $n + 1 = km$ and k, m have unique factorizations, it is still possible that $n + 1 = ij$ for different i and j , producing a different weakly decreasing sequence of primes whose product is $n + 1$. ■

TP 4.7 Recursive Definitions

$$f(n) ::= 5n$$

Base $f(0) ::= 0$

Which recursive cases work?

1. $f(n+1) = 5(n+1)$

So recursive is build up

This would be

$$n=0$$

$$0$$

$$n=1$$

$$= 5(1+1)$$

$$= 10$$

not $5 \cdot 1$

Ne



②

$$2. f(n+1) = 5 f(n)$$

$$\begin{array}{l} n=0 \\ 0 \\ n=1 \\ \leftarrow 5 \\ n=2 \end{array}$$

No wrong philosophy

$$\begin{array}{l} n=0 \\ 0 \end{array}$$

$$n=1 = 5 \cdot 0 = 0$$

$$n=2 \neq \\ = 5 \cdot 0 = 0 \quad \checkmark$$

l. again

Not $f()$

So ans stands \checkmark

~~ⓧ~~

3

3. $f(n+1) = f(n+5)$

$n=0$

$n=1$

$f(n)$

und yet

$f(6) = f(10)$

...



4. $f(n+1) = f(n) + 5$

$n=0$

$n=1$

$0 + 5 = 5$

$n=2$

$5 + 5 = 10$

$n=3$

$10 + 5 = 15$

works



5. $f(n+1) = f(n) + f(1)$

$n=0$

$n=1$

und

$n=2$

$f(1) f(1)$

⊗ No



I am glad I figured it out

9
TP 4.8 Recursive String Set

W = set of strings

W^+ = set of another strings

Base if $w \in W$ then $w \in W^+$

Constructor if $w \in W$ and $x \in W^+$ then

$xw \in W^+$

↑
Concatenation


Part 1 Suppose $W = \{ab, abba, a\}$. What is in W^+ ?

↳ just all the concatenations

1. $ababba$
 ✓

2. $abba b$
 ✗

3. $babba$
 ✗

4. $aaaaaaaaab$
 ✓ 

5

Part 2

Suppose W is as Part 1

Which of the predicates satisfy both

a) $P(x)$ holds for all $x \in W^+$

b) $P(x)$ leads to an easy, direct proof when used as a structural induction to prove a

1. ~~head~~ $a \geq b$

✓

2. every prefix of x has $|a|=|b|$

x

3. " " " " " * $|a|=|b|+1$

x

4. $ax \in W^+$

✓

L_i starts with a

5. $xy \in W^+$ for all $y \in W^+$

L_i true

6. $wx \in W^+$ for all $w \in W$
' is a postfix?
sure

1456 (x)

14 (x)

146

A string is in W^+ iff it can be written as concat ≥ 1 strings of W . So 1, 3, 4, 5, 6 true for all $x \in W^+$

1, 4, 6 easy, direct proofs

5 not an easy, direct proof b/c base case of 5 is 6 which requires its own inductive proof thus 5 is Q and 6 is R

Once 6 proved, 5 does have easy proof:
 $(xy)^n \in W^+$ for all $y \in W^+$, assuming that $xz \in W^+$ for all $z \in W^+$



Structural Induction

To prove $P(x)$ holds for all x in recursively defined set R , prove

- $P(b)$ for each base case $b \in R$
- $P(c(x))$ for each constructor, c , assuming ind. hyp. $P(x)$



Albert R Meyer, February 25, 2011

7W.13



Matched Paren Strings M

Lemma: Every s in M has the same number of $]$'s and $[$'s.

Proof by structural induction on the definition of M



Albert R Meyer, February 25, 2011

lec 4F.14



Matched Paren Strings M

Lemma: Every s in M has the same number of $]$'s and $[$'s.

Let $EQ ::= \{\text{strings with same number of }] \text{ and } [\}$

Lemma (restated): $M \subseteq EQ$



Albert R Meyer, February 25, 2011

lec 4F.15



Structural Induction on M

Proof:

Ind. Hyp. $P(s) ::= (s \in EQ)$

Base case ($s = \lambda$):

λ has 0 $]$'s and 0 $[$'s,

so $P(\lambda)$ is true.

base case is OK



Albert R Meyer, February 25, 2011

lec 4F.17



Structural Induction on M

Constructor step: $s = [r]t$
can assume $P(r)$ and $P(t)$

$$\#] \text{ in } s = \#] \text{ in } r + \#] \text{ in } t + 1$$

$$\#[\text{ in } s = \#[\text{ in } r + \#[\text{ in } t + 1$$

$$\text{so } = = \text{by } P(r) = \text{by } P(t)$$

so $P(s)$ is true construct case is OK



Albert R Meyer, February 25, 2011

lec 4F.18



Structural Induction on M

so by struct. induct.

$$M \subseteq EQ$$

QED



Albert R Meyer, February 25, 2011

lec 4F.19



The 18.01 Functions, F18

The set F18 of functions on \mathbb{R} :
 $\text{Id}_{\mathbb{R}}$, constant functions, and $\sin x$
are in F18.

if $f, g \in \text{F18}$, then

- $f + g$, $f \cdot g$, e^f , (the constant e)
- the inverse, $f^{(-1)}$, of f , and
- $f \circ g$ (the composition of f and g)
are in F18.



Albert R Meyer, February 25, 2011

lec 4F.20



The 18.01 Functions, F18

Some functions in F18:

$$-x = (-1) \cdot x$$

$$\sqrt{x} = (x^2)^{(-1)} \text{ ---inverse}$$

$$\cos x = (1 - (\sin x \cdot \sin x))^{1/2}$$

$$\ln x = (e^x)^{(-1)}$$



Albert R Meyer, February 25, 2011

lec 4F.21



The 18.01 Functions, F18

Lemma.

F18 is closed under
taking derivatives:
if $f \in \text{F18}$, then $f' \in \text{F18}$

Class Problem



Albert R Meyer, February 25, 2011

lec 4F.22



Recursive function on M

Def. $\text{depth}(s)$ for $s \in M$

$$\text{depth}(\lambda) ::= 0$$

$$\text{depth}([s]t) ::=$$

$$\max\{1+d(s), d(t)\}$$



Albert R Meyer, February 25, 2011

7W.25



k^n — recursive function on \mathbb{N}

$$\text{expt}(k, 0) ::= 1$$

$$\text{expt}(k, n+1) ::= k \cdot \text{expt}(k, n)$$

--uses recursive def of \mathbb{N} :

- $0 \in \mathbb{N}$
- if $n \in \mathbb{N}$ then $n+1 \in \mathbb{N}$



Albert R Meyer, February 25, 2011

7W.27



Recursive Functions

summary:

f : Data \rightarrow Values

$f(b)$ def'd directly for base b

$f(\text{cnstr}(x))$ def'd using $f(x)$, x



Albert R Meyer, February 25, 2011

7W.28



positive powers of two

$$2 \in \text{PP2}$$

if $x, y \in \text{PP2}$, then $x \cdot y \in \text{PP2}$

$$2, 2 \cdot 2, 4 \cdot 2, 4 \cdot 4, 4 \cdot 8, \dots$$

$$2 \quad 4 \quad 8 \quad 16 \quad 32 \dots \in \text{PP2}$$



Albert R Meyer, February 25, 2011

7W.47



loggy function on PP2

$$\text{loggy}(2) ::= 1$$

$$\text{loggy}(x \cdot y) ::= x + \text{loggy}(y)$$

for $x, y \in \text{PP2}$

$$\text{loggy}(4) = \text{loggy}(2 \cdot 2) = 2 + 1 = 3$$

$$\begin{aligned} \text{loggy}(8) &= \text{loggy}(2 \cdot 4) = 2 + \text{loggy}(4) \\ &= 2 + 3 = 5 \end{aligned}$$

$$\begin{aligned} \text{loggy}(16) &= \text{loggy}(8 \cdot 2) = 8 + \text{loggy}(2) \\ &= 8 + 1 = 9 \end{aligned}$$



Albert R Meyer, February 25, 2011

7W.49



loggy function on PP2

$$\text{loggy}(16) = \text{loggy}(8 \cdot 2) = 9$$

WAIT A SEC!

$$\begin{aligned} \text{loggy}(16) &= \text{loggy}(2 \cdot 8) \\ &= 2 + \text{loggy}(8) = 2 + 5 \\ &= 7 \end{aligned}$$



Albert R Meyer, February 25, 2011

7W.50



ambiguous constructors

The Problem: more than one way to construct elements of PP2 from $\text{cnstrct}(x, y) = x \cdot y$

$$16 = \text{cnstrct}(8, 2) \text{ but also}$$

$$16 = \text{cnstrct}(2, 8)$$

ambiguous



Albert R Meyer, February 25, 2011

7W.51



Team Problems

Problems

1-3



Albert R Meyer, February 25, 2011

lec 4F.53

- Used to always have to program recursively in Scheme 1st year
- learn about structural induction
 - than can reject it

*Simpler version of the same thing

Base case - That don't depend on anything else

Constructor

For example matched Paren strings

$$M \subseteq \{ \rangle, [\} \text{ * set of finite strings of this}$$

Looking for bracket matches

* Ls set of strings where

$[[[\rangle \rangle \rangle]$ is example

Base $\lambda \in M$

- the empty string

- when you attach it to a string, it does not do anything

Constructor If $s, t \in M$, then

$$[s]t \in M$$

② Can be multiple constructor operations

Strings $[s]t \in M$

$$[] \quad s = \lambda \quad t = \lambda$$

$$[[]] \quad s = [] \quad t = \lambda$$

- now nested pairs of brackets

$$[] [] \quad s = \lambda \quad t = []$$

$$[[] [] \quad s = [] \quad t = []$$

⋮ ⇒ ⋮ ⋮

Not in M

Strings that start w/]

Not in M b/c λ does not start]

$[s]t$, ~~all~~ starts w/ [

So can only start w/ [

extrema clause everything in M arises w/ these two rules

3

Structural Induction

To prove $P(x)$ holds for all x in \mathcal{R} , ^{recursively defined} \downarrow prove

- $P(b)$ for each base case $b \in \mathcal{R}$

- $P(c(x))$ for each constructor c

Assuming induction hypothesis $P(x)$

Induction on # of times you apply rules

Lemma: Every string in M has some # $]$ and $[$'s

EQ := strings w/ same # $]$, $[$

Lemma: $M \subseteq EQ$
 ^{subset of}

Proof: Ind hyp $P(s) ::= (s \in EQ)$

- s must be base or constructed

Base case $s = \lambda$

λ has 0 $]$ and 0 $[$

True

Constructor $s = [r]t$

Can assume $P(r)$ and $P(t)$

④

$$\#] \text{ in } S = \boxed{\#] \text{ in } r} + \boxed{\#] \text{ in } t} + 1$$

$$\# [\text{ " " } = \# [\text{ " " } + \#] \text{ " " } + 1$$

$$= \text{By } P(r) \qquad = \text{By } P(t)$$

↑

So this is =

(I like this, makes sense)

Constructor case is Ok ✓

So by struct ind $M \subseteq EQ \quad \square$

F18 - 18.01 functions on \mathbb{Q}

- Id_r = identity functions

~~Def~~ ~~Constant~~ functions

- sin x

if $f, g \in F18$, then

Use operations to build what you want out of this

- $f+g$

- $f \cdot g$

- e^f ← the constant e

- the inverse $f^{(-1)}$ of f

(5)

- $f \circ g$ (the composition of f and g)

- ~~one~~ the most powerful

So how to get $-x$?

$$(-1) \cdot x$$

\sqrt{x} ?

$$(x^2)^{(-1)} \quad \text{-inverse}$$

$$\cos x \text{ ? } (1 - (\sin x \cdot \sin x))^{1/2}$$

- Since $\sin^2 + \cos^2 = 1$

$$\ln x \text{ ? } (e^x)^{(-1)}$$

Lemma: F18 is closed under taking deriv

If $f \in \text{F18}$, then $f' \in \text{F18}$

- don't have derivative operator

- can construct w/ chain rule

Define functions on them recursively

Def. $\text{depth}(s)$ for $s \in M$

Base $\text{depth}(\lambda) = 0$

Cons. $\text{depth}([s]t) = \max\{1 + d(s), d(t)\}$

(6) k^n - recursive function on \mathbb{N}

Base $\text{expt}(k, 0) := 1$

$$\text{Const } \text{expt}(k, n+1) = k \cdot \text{expt}(k, n)$$

- Uses ... (missed) (see slides #27)

Summary

f : Data \rightarrow Values

$f(b)$ base

$f(\text{const}(x))$ def'd using $f(x), x$

Problems Issues

$2 \in \text{PP2}$ \leftarrow positive power of 2

if $x, y \in \text{PP2}$, then $x \cdot y \in \text{PP2}$

$$2 \cdot 1 = 2$$

$$2 \cdot 2 = 4$$

$$4 \cdot 2 = 8$$

$$4 \cdot 4 = 16$$

$$4 \cdot 8 = 32 \in \text{PP2}$$

⑦

Loggy function on $\mathbb{P}\mathbb{P}2$

$$\text{loggy}(2) ::= 1$$

$$\text{loggy}(x \cdot y) ::= x + \text{loggy}(y) \text{ for } x, y \in \mathbb{P}\mathbb{P}2$$

$$\text{loggy}(4) = \text{loggy}(2 \cdot 2) = 2 + 1 = 3$$

$$\text{loggy}(8) = \text{loggy}(2 \cdot 4) = 2 + \text{loggy}(4) = 2 + 3 = 5$$

$$\text{loggy}(16) = \text{loggy}(8 \cdot 2) = 9$$

but ~~loggy~~

$$\text{also} = \text{loggy}(2 \cdot 8)$$

$$= 2 + \text{loggy}(8) = 2 + 5 = 7$$

↓ 2 diff values!

- Thought defining fn, but defining a relation

Should Prove by str. ind that fn

Be careful when more than one way to construct! ambiguous

So try to be unambiguous

In-Class Problems Week 4, Fri.

Problem 1.

The Elementary 18.01 Functions (F18's) are the set of functions of one real variable defined recursively as follows:

Base cases:

- The identity function, $\text{id}(x) ::= x$ is an F18,
- any constant function is an F18,
- the sine function is an F18,

Constructor cases:

If f, g are F18's, then so are

1. $f + g, fg, e^g$ (the constant e),
2. the inverse function $f^{(-1)}$,
3. the composition $f \circ g$.

(a) Prove that the function $1/x$ is an F18.

Warning: Don't confuse $1/x = x^{-1}$ with the inverse, $\text{id}^{(-1)}$ of the identity function $\text{id}(x)$. The inverse $\text{id}^{(-1)}$ is equal to id .

(b) Prove by Structural Induction on this definition that the Elementary 18.01 Functions are *closed under taking derivatives*. That is, show that if $f(x)$ is an F18, then so is $f' ::= df/dx$. (Just work out 2 or 3 of the most interesting constructor cases; you may skip the less interesting ones.)

Definition. Recursively define the set, RecMatch, of strings as follows:

- **Base case:** $\lambda \in \text{RecMatch}$.
- **Constructor case:** If $s, t \in \text{RecMatch}$, then

$$[s]t \in \text{RecMatch}.$$

Problem 2.

Let p be the string $[]$. A string of brackets is said to be *erasable* iff it can be reduced to the empty string by repeatedly erasing occurrences of p . For example, here's how to erase the string $[[[]][[]]]$:

$$[[[]][[]]] \rightarrow [[][]] \rightarrow [] \rightarrow \lambda.$$

Is this compressed or 1 step?

On the other hand the string $[[[]][[[[]]]]$ is not erasable because when we try to erase, we get stuck:

$$[[[]][[[[]]]] \rightarrow][[[]]] \rightarrow][[[]] \not\rightarrow$$

Let Erasable be the set of erasable strings of brackets. Let RecMatch be the recursive data type of strings of *matched* brackets given in Definition 7.1.1.

(a) Use structural induction to prove that

$$\text{RecMatch} \subseteq \text{Erasable}.$$

(b) Supply the missing parts of the following proof that

$$\text{Erasable} \subseteq \text{RecMatch}.$$

Proof. We prove by strong induction that every length- n string in Erasable is also in RecMatch. The induction hypothesis is

$$P(n) ::= \forall x \in \text{Erasable}. |x| = n \text{ IMPLIES } x \in \text{RecMatch}.$$

Base case:

What is the base case? Prove that P is true in this case.

Inductive step: To prove $P(n + 1)$, suppose $|x| = n + 1$ and $x \in \text{Erasable}$. We need to show that $x \in \text{RecMatch}$.

Let's say that a string y is an *erase* of a string z iff y is the result of erasing a *single* occurrence of p in z .

Since $x \in \text{Erasable}$ and has positive length, there must be an erase, $y \in \text{Erasable}$, of x . So $|y| = n - 1 \geq 0$, and since $y \in \text{Erasable}$, we may assume by induction hypothesis that $y \in \text{RecMatch}$.

Now we argue by cases:

Case (y is the empty string):

Prove that $x \in \text{RecMatch}$ in this case.

Case ($y = [s]t$ for some strings $s, t \in \text{RecMatch}$): Now we argue by subcases.

- **Subcase (x is of the form $[s']t$ where s is an erase of s'):**

Since $s \in \text{RecMatch}$, it is erasable by part (b), which implies that $s' \in \text{Erasable}$. But $|s'| < |x|$, so by induction hypothesis, we may assume that $s' \in \text{RecMatch}$. This shows that x is the result of the constructor step of RecMatch, and therefore $x \in \text{RecMatch}$.

- **Subcase (x is of the form $[s]t'$ where t is an erase of t'):**

Prove that $x \in \text{RecMatch}$ in this subcase.

- **Subcase ($x = p[s]t$):**

Prove that $x \in \text{RecMatch}$ in this subcase.

The proofs of the remaining subcases are just like this last one. ~~List these remaining subcases.~~

This completes the proof by strong induction on n , so we conclude that $P(n)$ holds for all $n \in \mathbb{N}$. Therefore $x \in \text{RecMatch}$ for every string $x \in \text{Erasable}$. That is, $\text{Erasable} \subseteq \text{RecMatch}$. Combined with part (a), we conclude that

$$\text{Erasable} = \text{RecMatch}.$$

■

Explain why these work correction

Problem 3.

Here is a simple recursive definition of the set, E , of even integers:

Definition. Base case: $0 \in E$.

Constructor cases: If $n \in E$, then so are $n + 2$ and $-n$.

Provide similar simple recursive definitions of the following sets:

(a) The set $S ::= \{2^k 3^m 5^n \mid k, m, n \in \mathbb{N}\}$.

(b) The set $T ::= \{2^k 3^{2k+m} 5^{m+n} \mid k, m, n \in \mathbb{N}\}$.

(c) The set $L ::= \{(a, b) \in \mathbb{Z}^2 \mid 3 \mid (a - b)\}$.

Let L' be the set defined by the recursive definition you gave for L in the previous part. Now if you did it right, then $L' = L$, but maybe you made a mistake. So let's check that you got the definition right.

(d) Prove by structural induction on your definition of L' that

$$L' \subseteq L.$$

(e) Confirm that you got the definition right by proving that

$$L \subseteq L'.$$

(f) See if you can give an *unambiguous* recursive definition of L .

a) $\frac{1}{x}$

$$\sin(\sin^{-1}(x))^{-1}$$

Wk

$$\frac{d}{dx} [(e^x)^{-1}]$$

2. So essentially saying they match

I like \rightarrow to mean can't go further

So $\text{RecMatch} \subseteq \text{Erasable}$

$\text{Erasable} \subseteq \text{RecMatch}$

So $\text{RecMatch} \stackrel{=}{=} \text{Erasable}$

3. Base QEE

Const ~~2^k~~, $2^k \cdot 3^m \cdot 5^n$

where $k, m, n \in \mathbb{N}$

- but that is too simplistic

(2)

2b - For empty string Base case

Are 0 and 0 so =

Nothing to erase - so fully erased

1a Used b to get a , but now need to get a

b. Show that already have deriv of basic functions

So can make deriv of anything - like $f \circ g$
Product rule, chain rule, etc

Identity function $y = x$
- w $f(x) = x$

$\frac{d}{dx} f(x) = 1$ a constant which we have

~~sin~~ $\cos x = (1 - (\sin x + \sin x))^{1/2}$

$\frac{d}{dx} \sin x = \cos x = \sin(x + \frac{1}{2})$

Proves base cases:

No prove that anything we make w/ constructors will work

3

$$\frac{d}{dx} x^{-1} = -x^{-2}$$

$$= -x^{-1} \cdot x^{-1}$$

but do we have that as a constructor?

Pay attention to - power and inverse!
'So above may not hold

Our Board

1a) $x \rightarrow e^x \rightarrow \ln x \rightarrow -\ln x$ *only works pos*

$$e^{-\ln x} = \frac{1}{x}$$

1b) Base cases

$$f(x) = x, f'(x) = 1$$

$$f(x) = c, f'(x) = 0$$

$$f(x) = \sin x, f'(x) = \cos(x) = \sin\left(\frac{\pi}{2} - x\right)$$

Inductive

Given $F(x), F'(x)$

$$f'(x) = \frac{dx}{dy} = \frac{1}{\frac{dy}{dx}} = \frac{1}{f'(f^{-1}(x))}$$

(4)

Given part a, if $f'(x)$, $f^{-1}(x)$ are FIBs

FIBs, $\frac{1}{f'(f^{-1}(x))}$ is in FIB

Given ~~h(x) = f(g(x))~~ $h(x) = f(g(x))$

$$h'(x) = f'(g(x))g'(x)$$

multiplication and composition of FIB

↳ $f'(x)$ in FIB

Meyer: Not showing using the constructor functions

$h = f \circ g$ was given

- express it in that way

So Given $h(x) = f \circ g$

$$h'(x) = f' \circ g \circ g'(x) \text{ \textit{no variables!}}$$

Getting too caught up in Calculus
focus on the rules of the game

Solutions to In-Class Problems Week 4, Fri.

Problem 1.

The Elementary 18.01 Functions (F18's) are the set of functions of one real variable defined recursively as follows:

Base cases:

- The identity function, $\text{id}(x) ::= x$ is an F18,
- any constant function is an F18,
- the sine function is an F18,

Constructor cases:

If f, g are F18's, then so are

1. $f + g, fg, e^g$ (the constant e),
2. the inverse function $f^{(-1)}$,
3. the composition $f \circ g$.

(a) Prove that the function $1/x$ is an F18.

Warning: Don't confuse $1/x = x^{-1}$ with the inverse, $\text{id}^{(-1)}$ of the identity function $\text{id}(x)$. The inverse $\text{id}^{(-1)}$ is equal to id .

Solution. $\log x$ is the inverse of e^x so $\log x \in \text{F18}$. Therefore so is $c \cdot \log x$ for any constant c , and hence $e^{c \log x} = x^c \in \text{F18}$. Now let $c = -1$ to get $x^{-1} = 1/x \in \text{F18}$.¹ ■

(b) Prove by Structural Induction on this definition that the Elementary 18.01 Functions are *closed under taking derivatives*. That is, show that if $f(x)$ is an F18, then so is $f' ::= df/dx$. (Just work out 2 or 3 of the most interesting constructor cases; you may skip the less interesting ones.)

Solution. Proof. By Structural Induction on def of $f \in \text{F18}$. The induction hypothesis is the above statement to be shown.

Base Cases: We want to show that the derivatives of all the base case functions are in F18.

This is easy: for example, $d \text{id}(x)/dx = 1$ is a constant function, and so is in F18. Similarly, $d \sin(x)/dx = \cos(x)$ which is also in F18 since $\cos(x) = \sin(x + \pi/2) \in \text{F18}$ by rules for constant functions, the identity function, sum, and composition with sine.

This proves that the induction hypothesis holds in the Base cases.

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer .

¹There's a little problem here: since $\log x$ is not real-valued for $x \leq 0$, the function $f(x) ::= 1/x$ constructed in this way is only defined for $x > 0$. To get an F18 equal to $1/x$ defined for all $x \neq 0$, use $(x/|x|) \cdot f(|x|)$, where $|x| = \sqrt{x^2}$.

Constructor Cases: $(f^{(-1)})$. Assume $f, df/dx \in \text{F18}$ to prove $d f^{(-1)}(x)/dx \in \text{F18}$. Letting $y = f(x)$, so $x = f^{(-1)}(y)$, we know from Leibniz's rule in calculus that

$$df^{(-1)}(y)/dy = dx/dy = \frac{1}{dy/dx}. \quad (1)$$

For example,

$$d \sin^{(-1)}(y)/dy = 1/(d \sin(x)/dx) = 1/\cos(x) = 1/\cos(\sin^{(-1)}(y)).$$

Stated as in (1), this rule is easy to remember, but can easily be misleading because of the variable switching between x and y . It's more clearly stated using variable-free notation:

$$(f^{(-1)})' = (1/f') \circ f^{(-1)}. \quad (2)$$

Now, since $f' \in \text{F18}$ (by assumption), so is $1/f'$ (by part (a)) and $f^{(-1)}$ (by constructor rule 2.), and therefore so is their composition (by rule 3). Hence the righthand side of equation (2) defines a function in F18.

Constructor Case: $(f \circ g)$. Assume $f, g, df/dx, dg/dx \in \text{F18}$ to prove $d(f \circ g)(x)/dx \in \text{F18}$.

The Chain Rule states that

$$\frac{d(f(g(x)))}{dx} = \frac{df(g)}{dg} \cdot \frac{dg}{dx}.$$

Stated more clearly in variable-free notation, this is

$$(f \circ g)' = (f' \circ g) \cdot g'.$$

The righthand side of this equation defines a function in F18 by constructor rules 3. and 1.

The other Constructor cases are similar, so we conclude that the induction hypothesis holds in all Constructor cases.

This completes the proof by structural induction that the statement holds for all $f \in \text{F18}$. ■

Definition. Recursively define the set, RecMatch, of strings as follows:

- **Base case:** $\lambda \in \text{RecMatch}$.
- **Constructor case:** If $s, t \in \text{RecMatch}$, then

$$[s]t \in \text{RecMatch}.$$

Problem 2.

Let p be the string $[]$. A string of brackets is said to be *erasable* iff it can be reduced to the empty string by repeatedly erasing occurrences of p . For example, here's how to erase the string $[[[[]]]]$:

$$[[[[]]]] \rightarrow [[]] \rightarrow [] \rightarrow \lambda.$$

On the other hand the string $[] [[[[]]]]$ is not erasable because when we try to erase, we get stuck:

$$[] [[[[]]]] \rightarrow] [[[]] \rightarrow] [[] \not\rightarrow$$

Let Erasable be the set of erasable strings of brackets. Let RecMatch be the recursive data type of strings of *matched* brackets given in Definition ??.

(a) Use structural induction to prove that

$$\text{RecMatch} \subseteq \text{Erasable}.$$

Solution. Proof. We prove by structural induction on the definition of RecMatch that the predicate

$$P(x) ::= x \in \text{Erasable}$$

is true for all $x \in \text{RecMatch}$.

Base case ($x = \lambda$): The empty string is erasable by definition of Erasable—it can be reduced to itself by erasing the substring $[]$ 0 times.

Constructor case ($x = [s]t$ for $s, t \in \text{RecMatch}$): By structural induction hypothesis, we may assume that $s, t \in \text{Erasable}$. So to erase x , erase s and then erase t to be left with the substring $[]$, and one more erasure leads to the empty string.

This completes the proof by structural induction, so we conclude that

$$\forall x. x \in \text{RecMatch} \text{ IMPLIES } x \in \text{Erasable}$$

which by definition means that $\text{RecMatch} \subseteq \text{Erasable}$. ■

(b) Supply the missing parts of the following proof that

$$\text{Erasable} \subseteq \text{RecMatch}.$$

Proof. We prove by strong induction that every length- n string in Erasable is also in RecMatch. The induction hypothesis is

$$P(n) ::= \forall x \in \text{Erasable}. |x| = n \text{ IMPLIES } x \in \text{RecMatch}.$$

Base case:

What is the base case? Prove that P is true in this case.

Solution. The base case is ($n = 0$). Now $P(0)$ is true because the empty string is the only string of length 0, and it is in RecMatch by the base case of Definition ?? of RecMatch. ■

Inductive step: To prove $P(n + 1)$, suppose $|x| = n + 1$ and $x \in \text{Erasable}$. We need to show that $x \in \text{RecMatch}$.

Let's say that a string y is an *erase* of a string z iff y is the result of erasing a *single* occurrence of p in z .

Since $x \in \text{Erasable}$ and has positive length, there must be an erase, $y \in \text{Erasable}$, of x . So $|y| = n - 1 \geq 0$, and since $y \in \text{Erasable}$, we may assume by induction hypothesis that $y \in \text{RecMatch}$.

Now we argue by cases:

Case (y is the empty string):

Prove that $x \in \text{RecMatch}$ in this case.

Solution. In this case $x = p \in \text{RecMatch}$. ■

Case ($y = [s]t$ for some strings $s, t \in \text{RecMatch}$): Now we argue by subcases.

- **Subcase** (x is of the form $[s']t$ where s is an erase of s'):

Since $s \in \text{RecMatch}$, it is erasable by part (b), which implies that $s' \in \text{Erasable}$. But $|s'| < |x|$, so by induction hypothesis, we may assume that $s' \in \text{RecMatch}$. This shows that x is the result of the constructor step of RecMatch , and therefore $x \in \text{RecMatch}$.

- **Subcase** (x is of the form $[s]t'$ where t is an erase of t'):

Prove that $x \in \text{RecMatch}$ in this subcase.

Solution. The proof is essentially identical to the previous case, with t, t' in place of s, s' :

Now t is erasable by part (b), so $t' \in \text{Erasable}$. But $|t'| < |x|$, so by induction hypothesis, we may assume that $t' \in \text{RecMatch}$. This proves that x is the result of the constructor step of RecMatch and therefore $x \in \text{RecMatch}$. ■

- **Subcase** ($x = p[s]t$):

Prove that $x \in \text{RecMatch}$ in this subcase.

Solution. Let $t' ::= [s]t$ and s' be the empty string. Then $x = [s']t'$. But we know $s', t' \in \text{RecMatch}$, which implies that $x \in \text{RecMatch}$ because it is the result the RecMatch constructor step applied to s', t' . ■

Are there any remaining subcases? If so list those. If not, explain why the above cases are sufficient.

Solution.

There are no other subcases.

One could argue that the following are subcases.

1. **case** ($x = [ps]t$),
2. **case** ($x = [sp]t$),
3. **case** ($x = [s]pt$),
4. **case** ($x = [s]tp$).

But subcases 1 and 2 are analogous to the case where x is of the form $[s']t$ where s is an erase of s' . Similarly, subcases 3 and 4 are analogous to the case where x is of the form $[s]t'$ where t is an erase of t' . ■

This completes the proof by strong induction on n , so we conclude that $P(n)$ holds for all $n \in \mathbb{N}$. Therefore $x \in \text{RecMatch}$ for every string $x \in \text{Erasable}$. That is, $\text{Erasable} \subseteq \text{RecMatch}$. Combined with part (a), we conclude that

$$\text{Erasable} = \text{RecMatch}.$$

■

Problem 3.

Here is a simple recursive definition of the set, E , of even integers:

Definition. Base case: $0 \in E$.

Constructor cases: If $n \in E$, then so are $n + 2$ and $-n$.

Provide similar simple recursive definitions of the following sets:

(a) The set $S ::= \{2^k 3^m 5^n \mid k, m, n \in \mathbb{N}\}$.

Solution. We can define the set S recursively as follows:

- $1 \in S$
- If $n \in S$, then $2n$, $3n$, and $5n$ are in S .

■

(b) The set $T ::= \{2^k 3^{2k+m} 5^{m+n} \mid k, m, n \in \mathbb{N}\}$.

Solution. We can define the set T recursively as follows:

- $1 \in T$
- If $n \in T$, then $18n$, $15n$, and $5n$ are in T .

■

(c) The set $L ::= \{(a, b) \in \mathbb{Z}^2 \mid 3 \mid (a - b)\}$.

Solution. We can define a set $L' = L$ recursively as follows:

- $(0, 0), (1, 1), (2, 2) \in L'$
- If $(a, b) \in L'$, then $(a + 3, b), (a - 3, b), (a, b + 3),$ and $(a, b - 3)$ are in L' .

Lots of other definitions are also possible.

■

Let L' be the set defined by the recursive definition you gave for L in the previous part. Now if you did it right, then $L' = L$, but maybe you made a mistake. So let's check that you got the definition right.

(d) Prove by structural induction on your definition of L' that

$$L' \subseteq L.$$

Solution. For the L' defined above, a straightforward structural induction shows that if $(c, d) \in L'$, then $(c, d) \in L$. Namely, each of the base cases in the definition of L' are in L since $3 \mid 0$. For the constructor cases, we may assume $(a, b) \in L$, that is $3 \mid (a - b)$, and must prove that $(a \pm 3, b) \in L$ and $(a, b \pm 3) \in L$. In the first case, we must show that $3 \mid ((a \pm 3) - b)$. But this follows immediately because $((a \pm 3) - b) = (a - b) \pm 3$ and 3 divides both $(a - b)$ and 3. The other constructor case $(a, b \pm 3)$ follows in exactly the same way. So we conclude by structural induction on the definition of L' that $L' \subseteq L$.

■

(e) Confirm that you got the definition right by proving that

$$L \subseteq L'.$$

Solution. Conversely, we must show that $L \subseteq L'$. So suppose $(c, d) \in L$, that is, $3 \mid (c - d)$. This means that $c = r + 3k$ and $d = r + 3j$ for some $r \in \{0, 1, 2\}$ and $j, k \in \mathbb{Z}$. Then starting from base case $(r, r) \in L'$, we can apply the $(a \pm 3, b)$ constructor rule $|k|$ times to conclude that $(\bar{c}, r) \in L'$, and then apply the $(a, b \pm 3)$ rule $|j|$ times to conclude that $(c, d) \in L'$. This implies that $L \subseteq L'$, which completes the proof that $L = L'$. ■

(f) See if you can give an *unambiguous* recursive definition of L .

Solution. This is tricky. Here is an attempt:

base cases: $(0, 0), (1, 1), (2, 2), (-1, -1), (-2, -2), (-3, -3), (1, -2), (2, -1), (-1, 2), (-2, 1) \in L$.


Now the idea is to constrain the constructors so the two coordinates have absolute values that increase differing by at most 1, then one coordinate only can continue to grow in absolute value. Let


$$\text{Sg}(x) ::= \begin{cases} 1 & \text{if } x \geq 0, \\ -1 & \text{if } x < 0. \end{cases}$$


constructors: if $(a, b) \in L'$, then

- if $||a| - |b|| \leq 1$, then $(a + 3\text{Sg}(a), b + 3\text{Sg}(b)), (a + 3\text{Sg}(a), b), (a, b + 3\text{Sg}(b)) \in L'$,
- if $|a| > |b| + 1$, then $(a + 3\text{Sg}(a), b) \in L'$,
- if $|b| > |a| + 1$, then $(a, b + 3\text{Sg}(b)) \in L'$.


■



Mathematics for Computer Science
 MIT 6.042J/18.062J
**Intro to
 Number Theory:
 Divisibility, GCD's**


 Albert R Meyer February 28, 2011 lec 5M.1


Arithmetic Assumptions

assume usual rules for $+, \cdot, -$:
 $a(b+c) = ab + ac$, $ab = ba$,
 $(ab)c = a(bc)$, $a - a = 0$,
 $a + 0 = a$, $a+1 > a$, ...



 Albert R Meyer February 28, 2011 lec 5M.2



The Division Theorem

For $b > 0$ and any a , have
 $q = \text{quotient}(a,b)$
 $r = \text{remainder}(a,b)$


\exists unique numbers q, r such that
 $a = qb + r$ and $0 \leq r < b$.


Take this for granted too!


 Albert R Meyer February 28, 2011 lec 5M.3


Divisibility


c divides a ($c|a$) iff
 $a = k \cdot c$ for some k
 $5|15$ because $15 = 3 \cdot 5$
 $n|0$ because $0 = 0 \cdot n$



 Albert R Meyer February 28, 2011 lec 5M.4


Simple Divisibility Facts


- $c|a$ implies $c|(sa)$


$[a=k'c$ implies
 $(sa) = \frac{(sk')c}{k}$


 Albert R Meyer February 28, 2011 lec 5M.5


Simple Divisibility Facts


- $c|a$ implies $c|(sa)$
- if $c|a$ and $c|b$ then
 $c|(a+b)$
 [if $a=k_1c$, $b=k_2c$ then
 $a+b = (k_1+k_2)c$]



 Albert R Meyer February 28, 2011 lec 5M.6

 **Simple Divisibility Facts**


c a common divisor of a, b


- if $c|a$ and $c|b$ then $c|(sa+tb)$
integer linear combination of a and b

 Albert R Meyer February 28, 2011 lec. 5M.7

 **Common Divisors**


Common divisors of a & b divide integer linear combinations of a & b .


 Albert R Meyer February 28, 2011 lec. 5M.9

 **GCD**

$\text{gcd}(a, b) ::=$ the *greatest* common divisor of a and b


$\text{gcd}(10, 12) = 2$
 $\text{gcd}(13, 12) = 1$
 $\text{gcd}(17, 17) = 17$
 $\text{gcd}(0, n) = n$ for $n > 0$


 Albert R Meyer February 28, 2011 lec. 5M.10

 **GCD Remainder Lemma**


Lemma: for $b \neq 0$
 $\text{gcd}(a, b) = \text{gcd}(b, \text{rem}(a, b))$


Proof: $a = qb + r$
 any divisor of these 3 terms, divides all 3.

 Albert R Meyer February 28, 2011 lec. 5W.12


 **Euclidean Algorithm**
 as a State Machine:

States ::= $\mathbb{N} \times \mathbb{N}$
 start ::= (a, b)
 state transitions defined by
 $(x, y) \rightarrow (y, \text{rem}(x, y))$
 for $y \neq 0$

 Albert R Meyer February 28, 2011 lec. 5W.13

 **GCD correctness**

Example: $\text{GCD}(662, 414)$
 $= \text{GCD}(414, 248)$ since $\text{rem}(662, 414) = 248$
 $= \text{GCD}(248, 166)$ since $\text{rem}(414, 248) = 166$
 $= \text{GCD}(166, 82)$ since $\text{rem}(248, 166) = 82$
 $= \text{GCD}(82, 2)$ since $\text{rem}(166, 82) = 2$
 $= \text{GCD}(2, 0)$ since $\text{rem}(82, 2) = 0$
 return value: 2

 Albert R Meyer February 28, 2011 lec. 5W.15



GCD correctness

By Lemma, $\text{gcd}(x,y)$ is constant.
so preserved invariant is
 $P((x,y)) ::= [\text{gcd}(a,b) = \text{gcd}(x,y)]$

$P(\text{start})$ is trivially true:
 $(\text{gcd}(a,b) = \text{gcd}(a,b))$



GCD partial correctness

at termination

$$x = \text{gcd}(a,b)$$

Proof: at termination, $y = 0$, so
 $x = \text{gcd}(x,0) = \underbrace{\text{gcd}(x,y)}_{\text{preserved invariant}} = \text{gcd}(a,b)$



GCD Termination

y halves or smaller at
each step
reaches minimum in \leq
 $\log_2 b$
transitions



GCD is a linear combination

Theorem:

$\text{gcd}(a,b)$ is an integer
linear combination of
 a and b .



$\text{gcd}(a,b) = sa+tb$

Proof: Show how to find
coefficients s,t .

Method: apply Euclidean
algorithm, finding
coefficients as you go.



Finding s and t

Example: $a = 899, b = 493$

$$899 = 1 \cdot 493 + 406 \quad \text{so } 406 = 1 \cdot 899 + -1 \cdot 493$$


$$493 = 1 \cdot 406 + 87 \quad \text{so } 87 = 493 - 1 \cdot 406$$
$$= -1 \cdot 899 + 2 \cdot 493$$

$$406 = 4 \cdot 87 + 58 \quad \text{so } 58 = 406 - 4 \cdot 87$$
$$= 5 \cdot 899 + -9 \cdot 493$$

$$87 = 1 \cdot 58 + 29 \quad \text{so } 29 = 87 - 1 \cdot 58$$
$$= -6 \cdot 899 + 11 \cdot 493$$

$$58 = 2 \cdot 29 + 0 \quad \text{done, gcd} = 29$$



 **Finding s and t**

Example: $a = 899, b = 493$

$$899 = 1 \cdot 493 + 406 \quad \text{so } 406 = 1 \cdot 899 + -1 \cdot 493$$


$$493 = 1 \cdot 406 + 87 \quad \text{so } 87 = 493 - 1 \cdot 406$$


$$406 = 4 \cdot 87 + 58 \quad \text{so } 58 = 406 - 4 \cdot 87$$

$$87 = 1 \cdot 58 + 29 \quad \text{so } 29 = 87 - 1 \cdot 58$$

$$58 = 2 \cdot 29 + 0 \quad \text{done, gcd} = 29$$

the Pulverizer $s = -6, t = 11$

 Albert R Meyer February 28, 2011 lec. 5M.31

 **Finding $s > 0$ and t**

$$\text{gcd}(899, 493) = -6 \cdot 899 + 11 \cdot 493$$


get positive coeff. for 899?:


$$(-6 + 493k) \cdot 899 + (11 - 899k) \cdot 493$$

$$= -6 \cdot 899 + 11 \cdot 493$$

so use $k=1$: $487 \cdot 899 + -888 \cdot 493$


$$= \text{gcd}(899, 493)$$


 Albert R Meyer February 28, 2011 lec. 5M.33

 **Prime Divisibility**

Lemma: p prime and $p | (a \cdot b)$
implies $p | a$ or $p | b$


pf: in Class Problem 3.


 Albert R Meyer February 28, 2011 lec. 5M.35

 **Prime Divisibility**


Cor: If p is prime, and
 $p | a_1 \cdot a_2 \cdot \dots \cdot a_m$
then $p | a_i$ for some i .


pf: By induction on m .

 Albert R Meyer February 28, 2011 lec. 5M.36


 **Fundamental Thm. of Arithmetic**

Every integer > 1
factors uniquely into a
weakly increasing
sequence of primes

 Albert R Meyer February 28, 2011 lec. 5M.38

 **Unique Prime Factorization**

Every integer $n > 1$ has a
unique factorization into
primes: $p_0 \cdot p_1 \cdot \dots \cdot p_k = n$
with $p_0 \leq p_1 \leq \dots \leq p_k$

 Albert R Meyer February 28, 2011 lec. 5M.39



Unique Prime Factorization

Fundamental Theorem of Arithmetic

Example:

$$61394323221 = \\ 3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$$



Albert R Meyer

February 28, 2011

lec 5M.40



Unique Prime Factorization

pf: suppose not. choose smallest $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \leq p_2 \leq \cdots \leq p_k$$

$$q_1 \leq q_2 \leq \cdots \leq q_m$$

can assume $q_1 < p_1$

so $q_1 \neq \text{any } p_i$



Albert R Meyer

February 28, 2011

lec 5M.41



Unique Prime Factorization

Pf. but $q_1 | n$ & $n = p_1 \cdot p_2 \cdots p_k$
 so $q_1 | p_i$ for some i by Cor,
 contradicting that p_i is
 prime QED



Albert R Meyer

February 28, 2011

lec 5M.42



Team Problems

Problems

1–3



Albert R Meyer

February 28, 2011

lec 5M.49

(10 min late)

GCD

Factoring is hard

Lemma to find GCD

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

Proof: $a = qb + r$

Have same divisor

So same GCD

So can change # into smaller #s

Euclidean Algorithm as SM

States = $N \times N$

Start = (a, b)

Transitions $(x, y) \rightarrow (y, \text{rem}(x, y))$

repeat, repeat, etc

$\gcd(n, 0) = n$

Invariant - new # has the same GCD

$$P((x, y)) ::= [\gcd(a, b) = \gcd(x, y)]$$

②

P(start) trivially true

then true for anything you can get to

at termination $y=0$

$$x = \gcd(x, 0) = \gcd(x, y) = \gcd(a, b)$$

reaches min $i \leq 2 \log_2 b$ transitions

Theorem $\gcd(a, b)$ is an integer linear combo of a, b

$$\gcd(a, b) = sa + tb$$

? show how to find the coefficients s, t

Pulverizer

Start $a = 899$ $b = 493$

$$899 = \underset{\substack{\uparrow \\ \text{quotient}}}{1} \cdot \underset{\substack{\uparrow \\ \text{divisor}}}{493} + \underset{\substack{\uparrow \\ \text{remainder}}}{406}$$

$$493 = 1 \cdot 406 + 87$$

$$406 = 4 \cdot 87 + 58$$

$$87 = 1 \cdot 58 + 29$$

$$58 = 2 \cdot 29 + 0$$

$$\gcd = 29$$

$$\text{so } 406 = 1 \cdot 899 - 1 \cdot 493$$

$$87 = 493 - 1 \cdot 406 \\ = -1 \cdot 899 + 2 \cdot 493 \quad \text{back substitute}$$

$$58 = 406 - 4 \cdot 87 \\ = \cancel{5 \cdot 899} - 9 \cdot 493$$

$$29 = 87 - 1 \cdot 58 \\ = -6 \cdot 899 + 11 \cdot 493$$

$$\boxed{s = -6 \quad t = 11}$$

Keep info from 2 stages back

③

one is always \oplus and one is always \ominus

Get + coeff for $899'$

$$(-6 + 493k) \cdot 899 + (11 - 899k) \dots$$

... (missed info, see slide 34)

Prime Divisibility

Lemma: p prime and $p | (a \cdot b) \Rightarrow p | a$ or $p | b$

L) in class, problem 3

P-Set - had to ~~prove~~ divide by a prime

Corollary: If p is prime and $p | a_1 \cdot a_2 \cdot \dots \cdot a_n$
... (missed)

Get Unique Factorization Theorem / Fund. Theorem of Algebra

- can do weakly increasing ~~set~~ or decreasing
Unique factorization of primes

...

If there is any, there is a smallest one

...

$$a_1 < p_1$$

(4)

q is a divisor of n

So ~~q_1~~ $q_1 | n$ and $n = p_1 p_2 \dots p_k$

So $q_1 | p_i$ for some i by corollary

In-Class Problems Week 5, Mon.

Problem 1.

A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.¹

Problem 2. (a) Use the Pulverizer to find integers x, y such that

$$x \cdot 50 + y \cdot 21 = \gcd(50, 21).$$

(b) Now find integers x', y' with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \gcd(50, 21)$$

Problem 3.

For nonzero integers, a, b , prove the following properties of divisibility and GCD'S. (You may use the fact that $\gcd(a, b)$ is an integer linear combination of a and b . You may *not* appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

- (a) Every common divisor of a and b divides $\gcd(a, b)$.
- (b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- (c) If $p \mid ab$ for some prime, p , then $p \mid a$ or $p \mid b$.
- (d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

↑ Prof - read sols for #3
Very important

¹Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: *every* even perfect number is of this form (for a simple proof see <http://primes.utm.edu/notes/proofs/EvenPerfect.html>). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.

Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned} \gcd(259, 70) &= \gcd(70, 49) && \text{since } \text{rem}(259, 70) = 49 \\ &= \gcd(49, 21) && \text{since } \text{rem}(70, 49) = 21 \\ &= \gcd(21, 7) && \text{since } \text{rem}(49, 21) = 7 \\ &= \gcd(7, 0) && \text{since } \text{rem}(21, 7) = 0 \\ &= 7. \end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$= x - q \cdot y$
259	70	49	$= 259 - 3 \cdot 70$
70	49	21	$= 70 - 1 \cdot 49$
			$= 70 - 1 \cdot (259 - 3 \cdot 70)$
			$= -1 \cdot 259 + 4 \cdot 70$
49	21	7	$= 49 - 2 \cdot 21$
			$= (259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$= \boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0	

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b , which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

In Class Problems

2/28

1, So this was in the book

10 does not work

1, 2, 5, 10

$$1 + 2 + 5 = 8 \otimes$$

When is prime? - only then

What is k ? - just a #

$$k=0$$

~~$$2^1(2^0 - 1)$$~~

• First test $2^0 - 1 = 0 \otimes$

$$k=1$$

$$2^1 - 1 = 1 \otimes \otimes \text{ Not prime by convention}$$

$$k=2$$

~~$$2^2 - 1 = 3 \checkmark \text{ prime}$$~~

$$2^1(3) = 6 \otimes \text{ Not prime}$$

but that is ^{not} what we are looking for
looking for perfectness

1, 2, 3, 6

$$1 + 2 + 3 \textcircled{1}$$

②

But how does this work generally?
What patterns are there in prime, in perfect
| our board)

$2^{k-1}(2^k-1)$ has following factors besides itself

a) Those that are divided by the prime 2^k-1

b) Those that are not, but are instead powers of 2

These correspond to

a) $(2^k-1)(1) + (2^k-1)(2) + (2^k-1)(4) + \dots + (2^k-1)(2^{k-2})$

b) $1, 2, 4, \dots, 2^{k-2}$

Summing (a) we get

$$(2^k-1) \sum_{n=0}^{k-2} 2^n$$

$$= (2^k-1) (2^{k-1}-1)$$

never show

2^{k-1} is prime

- show that those are the only divisors

Summing (b) we get

$$\sum_{n=0}^{k-1} 2^n = 2^k - 1$$

So sum of the factors of $2^{k-1}(2^k-1)$ besides itself is

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

$$= (2^{k-1})(2^k-1)$$

③

2 on board)

Pulverizer $x(0) = 50$ $y(0) = 21$

x	y	r = x - qy	
50	21	8 = 50 - (2 * 21)	
21	8	5 = 21 - (2 * 8)	= 5 * 21 - 2 * 50
8	5	3 = 8 - 5	= 3 * 50 - 7 * 21
5	3	2 = 5 - 3	= 12 * 21 - 5 * 50
3	2	1 = 3 - 2	= 8 * 50 - 19 * 21
2	1	0	gcd = 1

$$\text{gcd}(50, 21) = 1 = \underset{p_5}{8} \cdot 50 - \underset{p_+}{19} \cdot 21$$

Not the shortest way to do

b) $8 \cdot 50 - 19 \cdot 21 = 1$, so $-8 \cdot 50 + 19 \cdot 21 = -1$

$$5 \cdot 50 = 250$$

$$12 \cdot 21 = 252$$

$$12 \cdot 21 - 5 \cdot 50 = 2$$

$$-8 \cdot 50 + 19 \cdot 21 = 5 \cdot 50 + 12 \cdot 21 = -1 + 2 = 1$$

$$-13 \cdot 50 + 31 \cdot 21 = 1 = \text{gcd}(50, 21)$$

$$\begin{cases} x' = -13 \\ y' = 31 \end{cases}$$

(4)

2b editor

~~SWT~~

$$8.50 - 19.21 = 1$$

$$\begin{array}{r} -21.50 \\ \quad \quad \quad \cancel{19.21} \\ \quad \quad \quad +21.50 \end{array}$$

$$-13.50 + 31.21 = 1$$

So this is switching which is -

Can keep doing to find ∞ combos

- ⊖ - one side gets more ⊖
- ⊕ - other side gets more ⊕

3.

Solutions to In-Class Problems Week 5, Mon.

Problem 1.

A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.¹

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, 2, 4, \dots, 2^{k-1}, \quad (1)$$

and

$$1 \cdot (2^k - 1), 2 \cdot (2^k - 1), 4 \cdot (2^k - 1), \dots, 2^{k-2} \cdot (2^k - 1). \quad (2)$$

The sequence (1) sums to $2^k - 1$ (using the formula for a geometric series,² and likewise the sequence (2) sums to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect. ■

Problem 2. (a) Let $m = 2^9 5^{24} 11^7 17^{12}$ and $n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2$. What is the $\gcd(m, n)$? What is the *least common multiple*, $\text{lcm}(m, n)$, of m and n ? Verify that


$$\gcd(m, n) \cdot \text{lcm}(m, n) = mn. \quad (3)$$

Solution.

$$\begin{aligned} g &= 2^3 11^7 17^9, \\ l &= 2^9 5^{24} 7^{22} 11^{211} 13^1 17^{12} 19^2 \\ gl &= 2^{12} 5^{24} 7^{22} 11^{218} 13^1 17^{21} 19^2 = mn \end{aligned}$$

(b) Describe in general how to find the $\gcd(m, n)$ and $\text{lcm}(m, n)$ from the prime factorizations of m and n . Conclude that equation (3) holds for all positive integers m, n .

Solution. The divisors of m correspond to subsequences of the weakly increasing sequence of primes in the factorization of m , and likewise for n . So the factorization $\gcd(m, n)$ is the largest common subsequence of the two factorizations. This can be calculated by taking all the primes that appear in both factorizations raised to the *minimum* of the powers of that prime in each factorization.

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer.

¹Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: *every* even perfect number is of this form (for a simple proof see <http://primes.utm.edu/notes/proofs/EvenPerfect.html>). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.

²It's fun to notice the "computer science" proof that (1) sums to $2^k - 1$. The binary representation of 2^j is a 10^j , so the sum is represented by 1^k . This what you get by subtracting 1 from 2^k which is the binary representation of 2^k .

Likewise, the factorization of $\text{lcm}(m, n)$ is the shortest sequence that has the factorizations of m and n as subsequences. So the factorization of $\text{lcm}(m, n)$ can be calculated by taking all the primes that appear in either factorization raised to the *maximum* of the powers of that prime in each factorization.

So in the factorization of $\text{gcd}(m, n) \cdot \text{lcm}(m, n)$ each prime appears raised to a power equal to the sum of its powers in the factorizations of m and n , which is precisely its power in the factorization of mn . ■

Problem 3. (a) Use the Pulverizer to find integers x, y such that

$$x \cdot 50 + y \cdot 21 = \text{gcd}(50, 21).$$

Solution. Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x, y) = x - q \cdot y$
50	21	$8 = 50 - 2 \cdot 21$
21	8	$5 = 21 - 2 \cdot 8$ $= 21 - 2 \cdot (50 - 2 \cdot 21)$ $= -2 \cdot 50 + 5 \cdot 21$
8	5	$3 = 8 - 1 \cdot 5$ $= (50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$ $= 3 \cdot 50 - 7 \cdot 21$
5	3	$2 = 5 - 1 \cdot 3$ $= (-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$ $= -5 \cdot 50 + 12 \cdot 21$
3	2	$1 = 3 - 1 \cdot 2$ $= (3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$ $= \boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0

(b) Now find integers x', y' with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \text{gcd}(50, 21)$$

Solution. since $(x, y) = (8, -19)$ works, so does $(8 - 21n, -19 + 50n)$ for any $n \in \mathbb{Z}$, so letting $n = 1$, we have

$$-13 \cdot 50 + 31 \cdot 21 = 1$$

Problem 4.

For nonzero integers, a, b , prove the following properties of divisibility and GCD'S. (You may use the fact that $\text{gcd}(a, b)$ is an integer linear combination of a and b . You may *not* appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

(a) Every common divisor of a and b divides $\text{gcd}(a, b)$.

Solution. For some s and t , $\text{gcd}(a, b) = sa + tb$. Let c be a common divisor of a and b . Since $c \mid a$ and $c \mid b$, we have $a = kc, b = k'c$ so

$$sa + tb = skc + tk'c = c(sk + tk')$$

so $c \mid sa + tb$. ■

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Solution. Since $\gcd(a, b) = 1$, we have $sa + tb = 1$ for some s, t . Multiplying by c , we have

$$sac + tbc = c$$

but a divides the second term of the sum since $a \mid bc$, and it obviously divides the first term, and therefore it divides the sum, which equals c . ■

(c) If $p \mid ab$ for some prime, p , then $p \mid a$ or $p \mid b$.

Solution. If p does not divide a , then since p is prime, $\gcd(p, a) = 1$. By part (b), we conclude that $p \mid b$. ■

(d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

Solution. Since $\gcd(a, b)$ is positive and an integer linear common of a and b , we have

$$m \leq \gcd(a, b).$$

On the other hand, since m is a linear combination of a and b , every common factor of a and b divides m . So in particular, $\gcd(a, b) \mid m$, which implies

$$\gcd(a, b) \leq m.$$

■

Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned} \gcd(259, 70) &= \gcd(70, 49) && \text{since } \text{rem}(259, 70) = 49 \\ &= \gcd(49, 21) && \text{since } \text{rem}(70, 49) = 21 \\ &= \gcd(21, 7) && \text{since } \text{rem}(49, 21) = 7 \\ &= \gcd(7, 0) && \text{since } \text{rem}(21, 7) = 0 \\ &= 7. \end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$= x - q \cdot y$
259	70	49	$= 259 - 3 \cdot 70$
70	49	21	$= 70 - 1 \cdot 49$
			$= 70 - 1 \cdot (259 - 3 \cdot 70)$
			$= -1 \cdot 259 + 4 \cdot 70$
49	21	7	$= 49 - 2 \cdot 21$
			$= (259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$= \boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0	

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b , which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

	x	y	remainder r
	259	70	$259 - 3 \cdot 70 = 49$
	70	21	$70 - 3 \cdot 21 = 7$
	49	7	$49 - 7 \cdot 7 = 0$
	259	70	$259 - 11 \cdot 70 = 29$
	70	21	$70 - 3 \cdot 21 = 7$
	29	7	$29 - 4 \cdot 7 = 1$

Week 3 + 4

Sets + Relations

Set Theory

Russell's Paradox

Infinity

Induction

SM: Invariants

Recursive

bad at

comfortable w/

Is reviewing book helpful?

Or do problems

- scan book

$$|A| \geq |B| \quad \text{surj}$$

$$|A| \leq |B| \quad \text{inj}$$

$$|A| = |B| \quad \text{bij}$$

$$|A| > |B| \quad \text{strict}$$

Cheat sheet!

- was on last cheat sheet

② Have not practiced Recursive at all
Last part though!

How to study?

- Rewrite answers
- just read answers

- read qu + think ←

- try to do on own

Not much time so might be best

Problems are variants off the book

Its what format the sol is / How to start

To prove invariant

Prove that eq always holds

$$P(r, s, a) \rightarrow (r', s', a')$$

$$\text{That is } r's' + a' = xy$$

Go through each transition case

Show invariant

$$\begin{aligned} r's' + a' &= 2r + \frac{s}{2} + a \\ &= rs + a \quad \checkmark \\ &= xy \end{aligned}$$

Prove both - so invariant

$$B_{ij} = \text{same} \quad \# \quad |A| = |B|$$

$$L^2 \quad h(s) = \begin{cases} (h_1(s), h_2(s)) & \text{if } h_1(s) \in L \text{ and } h_2(s) \in L \\ \text{end} & \text{otherwise} \end{cases}$$

(can take 3) to make inductive cases

$$\text{Identity } f(x) = x \quad \forall x \in M$$

↑ domain + co domain

$f(n+1) = (n+1) \cdot fac(n)$ for $n \geq 0$

Fib $Fib(0) = 0$

$Fib(1) = 1$

$Fib(n) = Fib(n-1) + Fib(n-2)$

Mapping Rules

- 1. $|A| \geq |B|$ A surj B
- 2. $|A| \leq |B|$ A inj B
- 3. $|A| = |B|$ A-bij B
- 4. $|A| > |B|$ A strict B

Bij ∞

$e(b)_i = a_0$

$e(a)_i = a_{i+1}$ for $n \in \mathbb{N}$

$e(a)_i = a$ for $a \in A - \{b, a_0, \dots\}$

Replacement A formula ϕ of set theory

defines the graph of a \in^n

$\forall x, y, z. [\phi(x, y) \text{ and } \phi(x, z)] \rightarrow$

The image of any set S under that \in^n is also a set t .

$\forall s \exists t \forall y [\exists x, \phi(x, y) \text{ iff } y \in t]$

Foundation There can not be an ∞ seq

$\dots \in x_n \in \dots \in x_1 \in x_0$ of sets

where each one is member of previous.

member-minimal $(m, x) = \{m \in x \text{ and } \forall y \in x, y \notin m\}$

So $\forall x, x \neq \emptyset \rightarrow \exists m$ member-minimal (m, x)

Choice Given a set S , whose members are non empty sets, no 2 of which have any elm in common, there is set C , consisting of one el from each set in S .

Induction $P()$ = predicate

If $P(0)$

$P(n) \rightarrow P(n+1)$ for $\forall n \in \mathbb{N}$

$\forall n \in \mathbb{N} P(n)$ for $\forall n \in \mathbb{N}$

Invariant Principle

If the preserved invariant of a gm is true for the start state, then it is true for all reachable states

Strong Induction $P()$ = predicate

If $P(0)$

for all $n \in \mathbb{N}, P(0), P(1), \dots, P(n)$ together

then $P(n)$ is true for all $n \in \mathbb{N} \rightarrow P(n+1)$

Recursive - construct new data els from previous ones

Structural induction - w/ constructor

$\langle 1, \leq 0, \leq 1, \leq 1, \leq 2 \dots \rangle$

Concatination

Expression parsing

Structural Induction $P()$ Predicate, Q = data type

If $P(b)$ is true for each base case el $b \in R$

for all 2 argument constructors C

$[P(r) \text{ and } P(s) \rightarrow P(C(r, s))]$ for all $r, s \in R$

then $P(c)$ is true for all $c \in R$

Russell's Paradox

$W = \{S \mid S \notin S\}$

So $S \in W$ iff $S \notin S$

for every S

Cont: $W \in W$ iff $W \notin W$

So W not a set - can't be a member of itself

ZFC

Extensionality, 2 sets = if same members
 $(\forall z, (z \in x \text{ iff } z \in y)) \rightarrow x = y$

Pairing For 2 sets x, y there is a set $\{x, y\}$ w/ x, y as only eles

$\forall x, y \exists v \forall z [z \in v \text{ iff } (z = x \text{ or } z = y)]$

Union union of z 's is also a set

$\forall z, \exists v \forall x (\exists y, x \in y \text{ AND } y \in z) \text{ iff } x \in v$

Infinity There is an ∞ set. A nonempty set x , such that for any set $y \in x$ the set $\{y\}$ is also a member of x .

Power Set All subsets form another set.

$\forall x, \exists p \forall u, u \subseteq x \text{ iff } u \in p$