## **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! 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  $\{0, 1, ..., 9\}$  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  $n \ge 1$  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  $n \ge 1$ , 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:

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

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

<sup>&</sup>lt;sup>1</sup>The half open unit interval, (0, 1], is  $\{r \in \mathbb{R} \mid 0 < r \le 1\}$ . Similarly,  $[0, \infty) ::= \{r \in \mathbb{R} \mid r \ge 0\}$ .

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  $n \le 3^{n/3}$  for every integer  $n \ge 0$ .
- (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  $n \ge 2$ .

**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  $n \ge 2$  and that i is a pusp for every integer i where  $2 \le i < n + 1$ . 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  $2 \le k, m < n+1$ . 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  $n \ge 2$ .

all  $n \ge 2$ . Intl n=2 n=2 3=2 ol

The can not be known

Oh is prime! n=3  $\rightarrow 4=2.2$ (Prime Uprime) n=4  $\rightarrow 5=2.7$   $\leftarrow not$   $\rightarrow 0.00$   $\rightarrow 0.00$ 

Not related but mad

Lireside of b (mod m)

Mod [m, n] is remainder in

That's what I thought

I don't get this problem at all! A 60 (7) But thought need list of discrete objects b) What is this  $\infty$  seq  $-\infty$  deep Oh can have recurences \$ 50 staff is silly! Vid not practice at all What does a decimal point in tront of seq do? Woiling same thing for everything! () ? Alternating digits "

d) well what does it mean to multiply sets

e) and in c) flow can it be smaller.

- multiply each part in ?



1. Half-open unit interval - Unit interval (0,1) -half open (0,17 - open = not include (o - closed = endpoint included [ ... Non regitive quadrant of real plane  $\left(0,\infty\right)^{\alpha}$ a) Bij  $(0, 0) \rightarrow (0, \infty)^2$ Both are sets of infinite size, This means That they one both the same size so (A (=/B) A bij B

Listing L2

Listing L2 means  $|L| = |L|^2$ And this makes sense beause  $|L|^2 = |L|^6 |L|$   $|L| = |L|^6 |L|$   $|L| = |L|^6 |L|$   $|L| = |L|^6 |L|$ 

.

a a function that maps el from one set to another

1 2 3 4 3 PR = x<sup>2</sup> = bijection celation

0,00 case don't matter -excluded

11

999999 - , 999999

 $\begin{array}{c} () \times_{1} \times_{1} \times_{2} \times_{3} \times_{3} \rightarrow_{P} \times_{1} \times_{1} \times_{2} \end{array}$ 18 > 18 18 Lis el of L every 12 - 1

(19,18)-12

Proved by  $L \rightarrow (0,1)$ If know AGB AZEBZZTWA by lema L 0 [0,172 Totally Sep Are of equal 59 2e

 $(a_i,a_i) \hookrightarrow (b_i,b_i)$ 

APOT all together

2. Strong induction

Look at 4Tue # 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 indution Then normal ind I would no normal ind "This specific sequence", Oh ho missed let part n=2 1+1 4 32/3 2 6 2 7.08 1+2 6 3

Am I simplifying what this is too muchi.

Ahnow exponentian celes

Non how to be by strong induction why would you want to do this.

Does proof by induction always use cases?

4. Weally 1 if each # Z # after it Bagus proof #3 hit on google is this P-set! Every 271 is product of unique weally decreasing Sea of pine 252 = 7.2.3.3.7 ? is that not ? !! 7.3.3.212 Can cepeat # 7 See assignment sheet N=4 5= N=5 6=3.2n=6 7 - pine n=7 8=4.2 Well fact is true

But proof is hot Where do proofs usually go south?

Somewhere From 1 step to another 1 3 psp - everything below n+1 - Unneeded Will make things slow But I don't think is problem To Do you even use strong ind - year use prior values 7 60 from 2 to 3 Tis prime don't know

Vsed seg ind -not strong

Might be more than one lx, m

252 's 4063

or 36°7

both have be =

the list combine

Not vrigue weekly & set

# Student's Solutions to Problem Set 3

Your name:

Plasmeler

**Due date:** February 25

Submission date:

Circle your TA/LA:

Ali

Nick

Oscar

Oshani

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 Math World: Interval
WP: Prime

#### DO NOT WRITE BELOW THIS LINE

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

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

<sup>&</sup>lt;sup>1</sup>People other than course staff.

<sup>&</sup>lt;sup>2</sup>Give citations to texts and material other than the Spring '11 course materials.

(5)

low. Need a function that maps from one get to another

(0,1] ()[0,90)

Ix does not work

don't need to include

11 -) 10

1 > = 1

50 do \$ -1

50 do \$ -1

99

48

0

b) a sea of Lecimal Digits (0,1,1,93)
"Long" if has a many occurances of digit beside 0=1
Bi) from L to (0,17)

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

You can't do this SO |A| = |B|
if A & B are
infinite?

A by B

For example from 999999 - , 999999
Which is old

C) 12 svj L X, Y, X2 Y2 X3 Y3. ->, X, Y, X2 Y2 X3 Y3. ... 19 7 198
TIS an element of L EVELY 12 -> L (9,18) is an elevent of L2 129 ZL)

127 = 121 -

d) A,B non empty sets

If A bij B, then A.A bij B.B

A bij B mems |A| = |B|Square both sides  $|A|^2 = |B|^2$   $|A^2| = |B^2|$   $|A^2| = |B^2|$  $|A^2| = |B^2|$ 

Both are of the same size  $(a_1,a_2,a_3,\ldots) \hookrightarrow (b_1,b_2,b_3,\ldots)$   $(a_1,a_2) \hookrightarrow (b_1,b_2)$ 

E) Show that [0,1] suj (0,1]?

[0,1] Z [(0,1]?]

Intinite sets have the same # of elements in each

So there is a bij between them No they do not.

To crample, Q + R are infinite put no bijustion between them exists

So if (0,1] surj (0,1]? and (0,1]? Surj (0,1)

Schrö'der - Barnstein theorm

€) Proof (0,1] bij [0,∞)2 Bring it all together (0,17 (-) [0,50) by = -1 Ploot by indetition The relationship a -> 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 Savaing an infinite set beeps it the same size

P-Set 3 Michael Plasmoier Oshani Table 12 #2 Strong induction Leo Sollution First try first few valve n=1  $\times$  1 mod y=0 OR| mod 7 = 0 n=2 x n mod 4 = 0 OR n mod 7= 0 n=3 x n=4 / N=5 x N = 6 X n=7 / N = 8 V Basically it multiple of 4 or 7 x also combination multiples of 4; 4, 8, 12, 16, 20, ... Multiples of 7: 7, 14, 21, 28 Hypothsis S(n) ! = multiples of 4 or 7 can be divided into teams of 4 or 7 players M mod 4=0 OR n mod 7=0 x the

Base Cases N=4 Work 5(4) 4 mod 4 = 0 V n=7 works 5(7)7 mod 7 = 0 V Industry step Strong hypothesis B(n) for n divisiable 4 or n divisible 7 By casesilin's divisable by 4 Assume works for n n+4 mod 4 = 0 1 mod 4 + 4 mod 4 0 = () \ Case 2: n'is divisable by 7 1 + 7 mod 7 = 0 n mod 7 + 7 mod 7

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

6 P-Set 3 Michael Plasmeier Oshani Table 12 #3 Poof by Strong induction for nZO  $5(n) : |= n \leq 3^{n/3}$ Base case (n = 0) 0 4 30/3 0 = 1 (N=1)  $\leq 3^{1/3}$ 1 6 1.44  $(n=2)_{2} \leq 3^{2/3}$ (n=3)  $2 \le 2.08$  (n=3)  $3 \le 3^{3/3}$ 7=3 (n=4) 4£ 34/3

4 4 9,32

$$(n=5)$$
  $5 \le 3^{5/3}$   $5 \le 6.24$   $(n=6)$   $6 \le 3^{6/2}$   $6 \le 9$  Indulue (ase Assuming  $S(0), S(1), S(2), ..., S(n)$  (an get  $S(n+1)$ )

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

Proved by induction

b) Proof by Induction

S(m): = If a sequence of positive integers has

Sum n 7 1 then product is at most 3<sup>n/3</sup>

m = # of integers in sequence

Base case (m=1)

1 2 2<sup>n/3</sup>

1 \( \preceq \) 3 \( \frac{1}{2} \) \( \frac{1} \) \( \frac{1}{2} \) \( \frac{1}{2}

Bt could also do 100 \le 3 100/3 28.1015

So smaller values are better

Indutive case

Assume S(m) is true for m 21

So S(m+1) Should also be true

Let 1+1+1+1+1=2 are those 1 or 1? If they're 1s, why are they all the sine?

Mean to be allo be

.

Lephangh, along of 50 m 1 and one of 1 says all some all says and bear of bear of bear of head one of

P-501 3 Michael Plasmeier ()Shank Table 12 #4 " You do not need the step through all of the intergers it each time you increase by 1 ? Would make calculation slower There are multiple possible values for k, m For example 752 could be 4.63 0 < 36,07

In never prove which it is or that they are Equivilant, so it is not a unique set.

+735

could be cleaver; See solutions 1

# **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! 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  $\{0, 1, ..., 9\}$  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... and 099999... 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  $s = x_0, x_1, x_2, ...,$  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

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

<sup>&</sup>lt;sup>1</sup>The half open unit interval, (0, 1], is  $\{r \in \mathbb{R} \mid 0 < r \le 1\}$ . Similarly,  $[0, \infty) ::= \{r \in \mathbb{R} \mid r \ge 0\}$ .

**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  $f: A \to B$  is a bijection. Let  $g: A^2 \to B^2$  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  $(b_1, b_2)$  is  $B^2$ , 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:

$$g(a_1, a_2) = g(a_3, a_4)$$
 iff  $(f(a_1), f(a_2)) = (f(a_3), f(a_4))$  (by def of  $g$ )

iff  $f(a_1) = f(a_3)$  AND  $f(a_2) = f(a_4)$ 

iff  $a_1 = a_3$  AND  $a_2 = a_4$ (since  $f$  is injective)

 $(a_1, a_2) = (a_3, a_4)$ ,

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 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  $f:(0,1]^2 \to (0,1]$ , namely

$$f(\langle x, y \rangle) ::= x.$$

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  $n \ge 1$  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.

Ctoph /

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

$$4 = 4$$

$$7 = 7$$

$$8 = 4 + 4$$

$$11 = 4 + 7$$

$$12 = 4 + 4 + 4$$

$$14 = 7 + 7$$

$$15 = 4 + 4 + 7$$

$$16 = 4 + 4 + 4 + 4$$

$$18 = 4 + 7 + 7$$

$$19 = 4 + 4 + 4 + 7$$

$$20 = 4 + 4 + 4 + 4 + 4$$

$$21 = 7 + 7 + 7$$

and these are the only numbers  $\leq 21$  that can be divided into such teams. Now we claim that every group of n > 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  $n \ge 18$  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  $n \ge 21$ , we assume that  $P(18), P(19), \ldots, P(n)$  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  $n - 3 \ge 18$  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  $n \ge 18$ .

So all the possible values of *n* are 4, 7, 8, 11, 12, 14, 15, 16, and  $\geq$  18.

#### Problem 3.

**Claim 3.2.** If a sequence of positive integers has sum  $n \ge 1$ , 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  $n \le 3^{n/3}$  for every integer  $n \ge 0$ .

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

$$0^{3} \le 3^{0} \to 0 \le 3^{0/3}$$

$$1^{3} \le 3^{1} \to 1 \le 3^{1/3}$$

$$2^{3} \le 3^{2} \to 2 \le 3^{2/3}$$

$$3^{3} \le 3^{3} \to 3 \le 3^{3/3}$$

$$4^{3} \le 3^{4} \to 4 \le 3^{4/3}$$

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

$$3^{(n+1)/3} = 3 \cdot 3^{(n-2)/3}$$
  
 $\geq 3 \cdot (n-2)$   
 $\geq n+1$  (for all  $n \geq 7/2$ )

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  $n \ge 7/2$ . (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  $n \ge 0$  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  $k \ge 1$ . So assume that P(k) is true, and let  $x_1, \ldots, x_{k+1}$  be a sequence of k+1 positive integers with sum n. Then we can reason as follows:

$$x_1 \cdot x_2 \cdots x_k \cdot x_{k+1} \le 3^{(n-x_{k+1})/3} \cdot x_{k+1}$$

$$\le 3^{(n-x_{k+1})/3} \cdot 3^{x_{k+1}/3}$$

$$= 3^{n/3}$$

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.

Solutions to Problem Set 3 5

**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  $n \ge 2$ .

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  $n \ge 2$  and that i is a pusp for every integer i where  $2 \le i < n + 1$ . 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  $2 \le k, m < n + 1$ . 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.

# 6.042 Totac

# TP 4.7 Recusive Definitions

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

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

$$h=0$$

$$h=1$$

$$n=2$$

$$n=1 = 5.0 = 0$$
 $h=2$ 



3
$$3 \cdot f(n+1) = f(n+5)$$

$$h=0$$

$$h=1$$

$$f(ba(a))$$

$$and set$$

$$f(a) = f(b)$$

$$1 \cdot f(n+1) = f(n) + 5$$

$$n=0$$

$$n=1$$

$$0 + 5 = 5$$

$$n=2$$

$$5 + 5 = 10$$

$$n=3$$

$$10 + 5 = 15$$

$$Vorbs$$

$$5 \cdot f(n+1) = f(n) + f(1)$$

$$n=0$$

$$n=1$$

n=0 n=1 1 and n=2  $f(1) f(1) \otimes N_0$ 

Fan glad I figured it out TP4.8 Recrease String Set W= set of strings W+ = set of another strings i Base if WEW then WEWT Constructor if wtW and XEW+ ten XWE WT Conditionation Port | Sprose W= {ab, abba, a}. What is in W+? " just all the concatanations l a b abaloba 2. ab ba b 3. babba Vy. aaaaaaab

```
Part 2
   Sppose Wis as Part 1
   Which of the predicates sutisfy both
 a) P(x) holds for all x \in W^{+}
 b) P(x) leads to an easy direct proet when used
     as a stactual induction to prove a
l. basi a Z b
2. every prefix of x has |a| = |b|
 3. 11 11 11 * lal=16/+1
 V \alpha x \in W^{\dagger}
 5. xy EW+ for all yE W+
```

6. WX f Wt for all wf W (is a pootfix) see

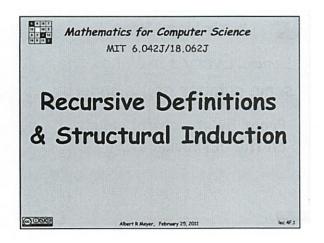
A string is W+ iff it can be writen as concat 2) strings of W. & 1,34,5,6 tre for all x & W+

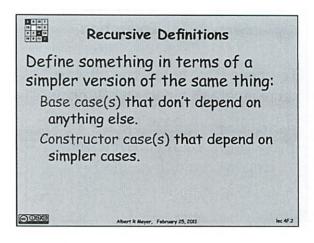
1,4,6 easy, direct prosts

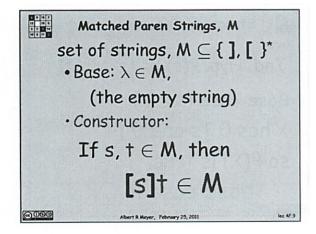
5 not an easy, direct proof b/c base case
of 5 ile le which requires its own indiction proof
thus 5 is Q and le is h

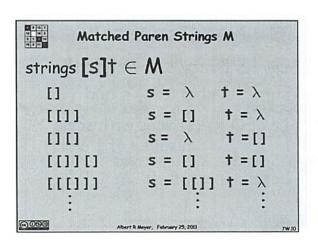
Once le proved, 5 does have easy proof;

(x yx) E W for all y E W f, asaming
that x 7 E W for all 2 E W f









```
not in M

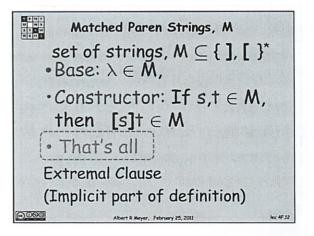
strings starting with ]

are not in M because

• \(\lambda\) does not start with ]

• [s]t does not start with ]

and everything in M arises in one of these two ways
```



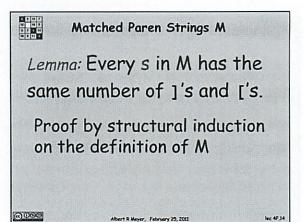
#### 0 0 7 0 0 1 1 1 2 W

# Structural Induction

To prove P(x) holds for all x in recursively defined set R, prove  $\cdot P(b)$  for each base case  $b \in R$   $\cdot P(c(x))$  for each constructor, c, assuming ind. hyp. P(x)

@000

Albert B Meuer February 25 201





### Matched Paren Strings M

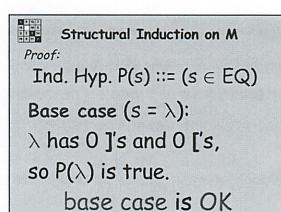
Lemma: Every s in M has the same number of ]'s and ['s.

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

Lemma (restated): M ⊆ EQ

@00

bert R Meyer, February 25, 2011



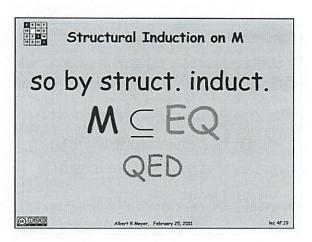
Structural Induction on M

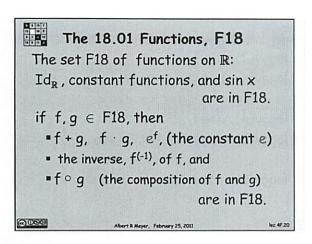
Constructor step:  $s = [r]^{\dagger}$ can assume P(r) and P(t)

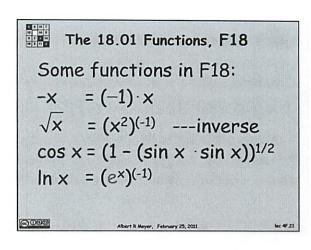
#] in s = # in r + # in t + 1#[ in s = #[ in r + #[ in t + 1so = = by P(r) = by P(t)

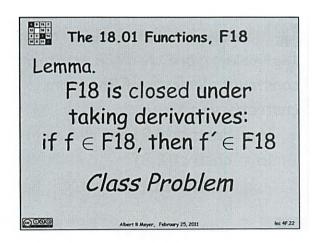
so P(s) is true constrct case is OK

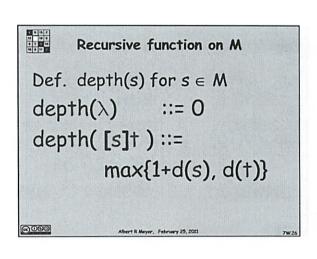
Abert R Mayer. February 25, 2011

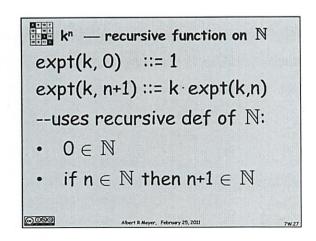


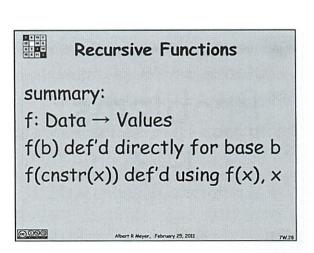


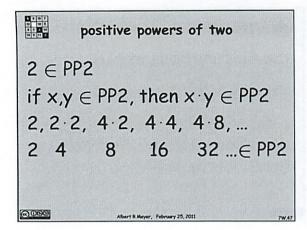


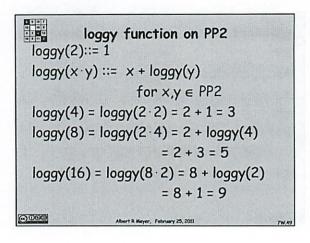


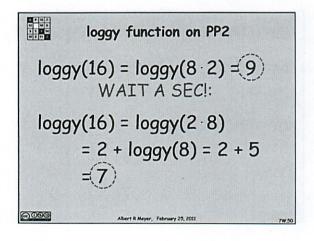


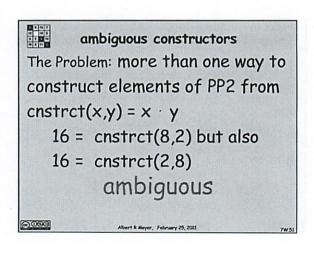


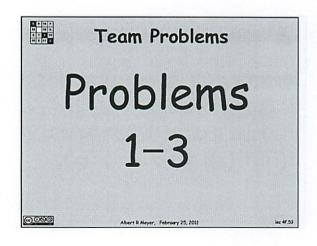












- Used to always have to program recursivly in Scheme 1st year -learn about structual induction - Than can reject it

#Simpler version of the same thing Base case - That don't depend me on anything else Constructor

For example matched paren strings MCGZL3\*Eset of finite strings

Looking for bracket matches Is set of strings where

LCC 777 & example

Base JEM The empty string - When you attach it to a string, it does not do anything Constructor If 5, t & M, then

[5/# EM

(an be multiple constitutor operations Strings 157+ EM  $S = \lambda$   $+ = \lambda$ C[77] s=L7  $t=\lambda$ - now nested pairs of brades [717 ([17][7] 5=[7] +=[7]Not in M Strings that start of 7 Not in M b/c I does not start 7 [57 t, all starts w/ C So can only start w/ [

extrema clause everything in M orises ul these two rules

Structural Induction recurry defined To prove P(x) holds for all x in R, prove - P(b) for each base case bE/1 - P(c(x)) for each constructor ( assuming induction hypothsis P(x) Induction on # of times you apply wells Lema: Every string in M has some # I and [ s Ea i = strings of same # 7, [ Lemmai MC EQ Proof! Ind hyp P(s): = (SER) -5 must be base or construted Base lase 5=2 I has O I and O I Constrution 6= [7]+ (an assume p(r) and P(t)

# ] in s= #7 in c | + | # 7 in + | + 1 50 This is = (I like this, makes sense) Constructor case is Oh V So by struct ind MC FQ 1-18 - 18.01 functions on ( - Id = identity functions

- Idr = identity functions

Description A- Constant functions
- Sin X

if fig & F18, then

Use operations to build what you want at of this

- f+g
- f · g

- ef - the constant e
- the inverse f(-1) of f

- fog the composition of E and q) - One the most powerful So how to get -x? (-1) · x VX (x2)(-1) -inverse (05 X [ ( ( - ( GIAX + GIA X ) ) 1/2 -Since sin2 + crs2 >1 ln x ? (e x x-1) Lemma: F18 is closed unter taking device IF f = F18, her f' = 18 -don't have derivitive operator - Can construct of chain rule Define Eunctions on them recursily

Define Eunctions on them recursity

Def. depth(s) for sEM

Base depth (L) = 0

Lons. depth (Ls) + max (1+d(s),d(+))

(6)

k" - recursive function on N

Bar expt (k,0):=1

Const expt (k, n+1) = k · expt (k,n)

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

Summary

fi Nata -> Values

f(b) base

f(const(x)) def'd using f(x), x

Predictions Issues

2 & PP2 & Positive power of 2

It x, y & PP2, ten xoy & PP2

20 = 2
2.2 4

4.2 8

4.8 32 EPP2

oggy function on PPZ loggy (2) := 1 loggy (x·y) := x rloggy(y) for x, y t PPZ loggy (4) = loggy (2·2) = 2 + 1=3 10997 (8) = loggy (2.4) = 2 + loggy (4) = 2+3=5 loggy (la) = logggy (8 12) = but delygon 12 lift values! also = (0994 (2.8) = 2+loggy(8) #2.5 = > - Thought Letining for, but defining a relation

Shall Prove by stru. ind that En

Be careful when more than one may to construct! ambigious 60 try to be enambiging

# 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, 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,  $id^{(-1)}$  of the identity function id(x). The inverse  $id^{(-1)}$  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 [[[]][]][]:

For example, here's how to erase the string [[[]][]][]:

$$\begin{bmatrix}
[[[]]] \\
[]
\end{bmatrix}
\end{bmatrix}$$
Is this compressed of life [[]][]] is not erasable because when we try to erase, we get stuck:

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

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.

Correction

(a) Use structural induction to prove that

RecMatch  $\subseteq$  Erasable.

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

Erasable  $\subseteq$  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  $|y| = n - 1 \ge 0$ , 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  $x \in \mathbf{RecMatch}$  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 ∈ RecMatch, it is erasable by part (b), which implies that s' ∈ Erasable. But |s'| < |x|, so by induction hypothesis, we may assume that s' ∈ RecMatch. This shows that x is the result of the constructor step of RecMatch, and therefore x ∈ 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 ∈ 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, Erasable  $\subseteq \text{RecMatch}$ . Combined with part (a), we conclude that

Erasable = 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  $S ::= \{2^k 3^m 5^n \mid k, m, n \in \mathbb{N}\}.$
- **(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) +

Sin (sin(x)))-1

W

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

2. So essentally saying they match

I like As to mean can't go furter

So Rect Match C Erasable

Erasable C Rect Metch

So Rect Metch & Erasable

3. Base QEE

Const 20th, 2x. 3m. 5n

Where L, m, n EN
- but that is too simplistic

26 - For empty string Base case Are O [ and 07 50 = Nothing to crase -so Fully erased la Vsed b to get a, but now need to get a b. Show that already have dein of basic Funding So (an make deriv of anything - like tog Product rule, chain rule, otc Identity function y=x -W f(x) = x $\frac{d}{dx}$  f(x) = 1 a constant which we have (05 x ( | -(Sinx a 5(nx)) 42  $\frac{d}{dx} \sin x = \cos x = \sin (x + \frac{1}{2})$ Proves base cases Wo prove that anything we make uf constructors will vork

$$\int_{0}^{\infty} dx x^{-1} = -x^{-2}$$

$$= -x^{-1} \cdot x^{-1}$$
but do we have that as a construtor?

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

Our board la) x + ex -) ln x + -ln x & only works pos e-hx = + 16) Base Cases f(x) = (f(x) = 0) $f(x) = \sin x, f'(x) = \cos(x) = \sin\left(\frac{x}{2} - x\right).$ Indulie Given F(x), F (x)  $f'(x) = \frac{dx}{dy} = \frac{1}{dx} = \frac{1}{f'(f'(x))}$ 

Given part a, if f'(x), f (x) are F185 f(8s, f(f'(x)) is in f18 Given MANDER h(x) = f(g(x))h'(x) = f'(g(x))g'(x)multiplication and composition of F18 4 f'(x) in F18 Myer: Not storing voing the constructor functions h=fog has given - express it in that way 50 Given h(x) = f'og hi(x) = f'og , glyn e no variables. betting too caught up in Calulous tocus on the rules of the gare

# 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, 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,  $id^{(-1)}$  of the identity function id(x). The inverse  $id^{(-1)}$  is equal to id.

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

(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  $f \in F18$ . 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,  $d \operatorname{id}(x)/dx = 1$  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.

<sup>&</sup>lt;sup>1</sup>There's a little problem here: since  $\log x$  is not real-valued for  $x \le 0$ , 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  $x \ne 0$ , use  $(x/|x|) \cdot f(|x|)$ , where  $|x| = \sqrt{x^2}$ .

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

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

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

Now, since  $f' \in F18$  (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  $f, g, df/dx, dg/dx \in F18$  to prove  $d(f \circ g)(x)/dx \in F18$ .

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  $f \in F18$ .

**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:

$$[]][[[[[]]] \rightarrow ][[[]] \rightarrow ][[] \rightarrow$$

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

RecMatch  $\subseteq$  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

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

which by definition means that RecMatch  $\subseteq$  Erasable.

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

Erasable  $\subseteq$  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  $|y| = n - 1 \ge 0$ , 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  $x \in \mathbf{RecMatch}$  in this case.

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

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

- Subcase (x is of the form [s']t where s is an erase of s'):
   Since s ∈ RecMatch, it is erasable by part (b), which implies that s' ∈ Erasable. But |s'| < |x|, so by induction hypothesis, we may assume that s' ∈ RecMatch. This shows that x is the result of the constructor step of RecMatch, and therefore x ∈ RecMatch.</li>
- Subcase (x is of the form [s]t' where t is an erase of t'):
   Prove that x ∈ 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 ∈ 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, Erasable  $\subseteq \text{RecMatch}$ . Combined with part (a), we conclude that

Erasable = 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 ∈ T
- If  $n \in S$ , 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 the 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  $(c,r) \in L'$ , 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: 
$$(0,0), (1,1), (2,2), (-1,-1), (-2,-2), (-3,-3)(1,-2), (2,-1), (-1,2), (-2,1) \in L$$

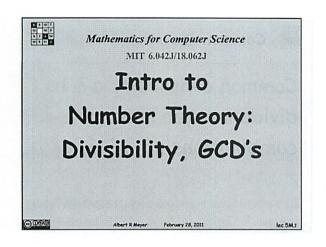
Now the idea is to constrain the constructors so the two coordinates have absolute values that increase differing by at most 1, then one coordinate only can continue to grow in absolute value. Let

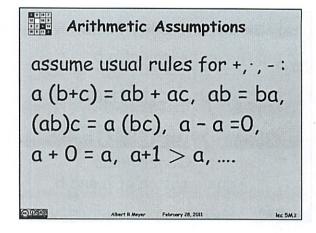
$$Sg(x) ::= \begin{cases} 1 \text{ if } x \ge 0, \\ -1 \text{ if } x < 0. \end{cases}$$

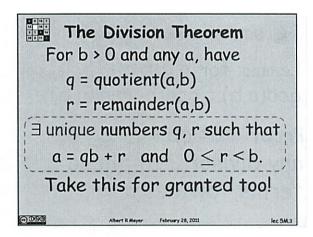
**constructors**: if  $(a, b) \in L'$ , then

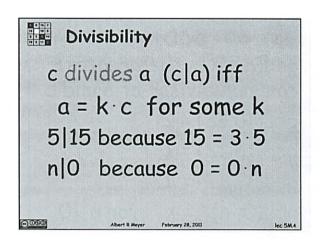
- if  $||a| |b|| \le 1$ , then  $(a + 3\operatorname{Sg}(a), b + 3\operatorname{Sg}(b)), (a + 3\operatorname{Sg}(a), b), (a, b + 3\operatorname{Sg}(b)) \in L'$ ,
- if |a| > |b| + 1, then  $(a + 3Sg(a), b) \in L'$ ,
- if |b| > |a| + 1, then  $(a, b + 3Sg(b)) \in L'$ .

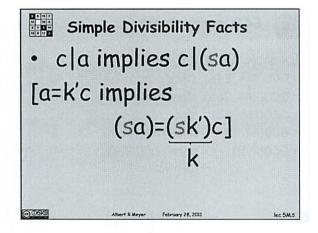


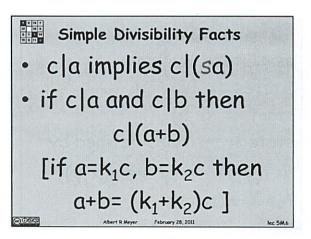


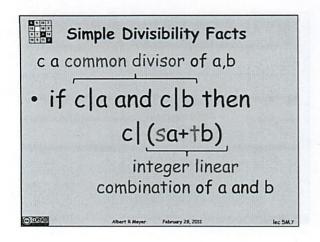


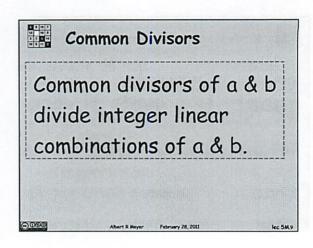


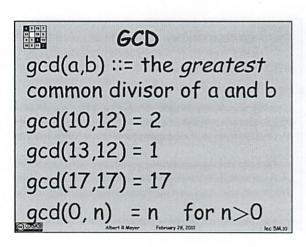


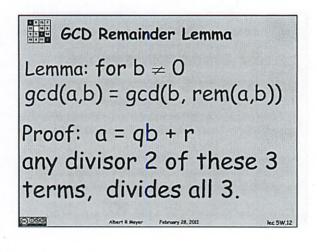


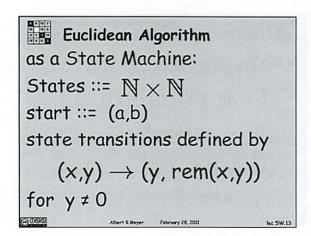


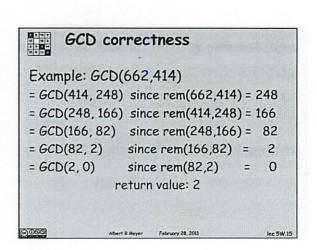










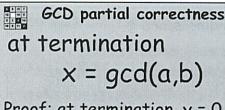




# GCD correctness

By Lemma, gcd(x,y) is constant. so preserved invariant is P((x,y)) ::= [qcd(a,b) = qcd(x,y)]

P(start) is trivially true: (qcd(a,b) = qcd(a,b))



Proof: at termination, y = 0, so x = gcd(x,0) = gcd(x,y) = gcd(a,b)preserved invariant



# GCD Termination

y halves or smaller at each step reaches minimum in < log2 b transitions

# GCD is a linear combination

# Theorem:

gcd(a,b) is an integer linear combination of a and b.



# 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

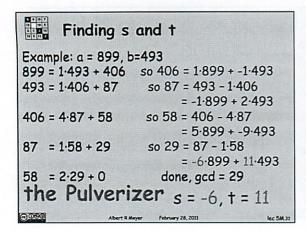
899 = 1.493 + 406 so 406 = 1.899 + -1.493

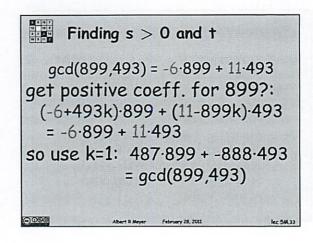
493 = 1.406 + 87 so 87 = 493 - 1·406 = -1.899 + 2.493

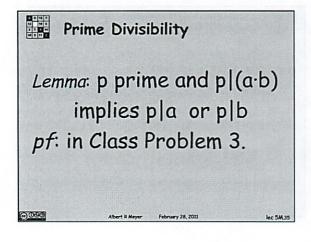
406 = 4.87 + 58 so 58 = 406 - 4·87 = 5.899 + -9.493

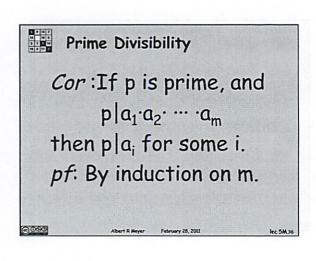
87 = 1.58 + 29 so 29 = 87 - 1.58

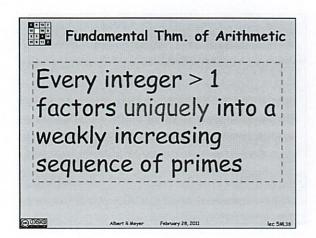
= -6.899 + 11.493 58 = 2.29 + 0 done, gcd = 29

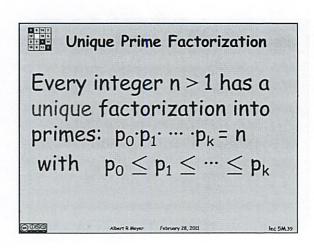










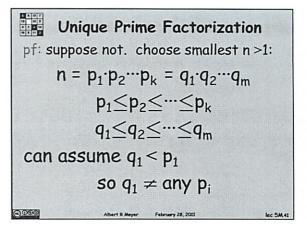




# Unique Prime Factorization

Fundamental Theorem of Arithmetic Example:

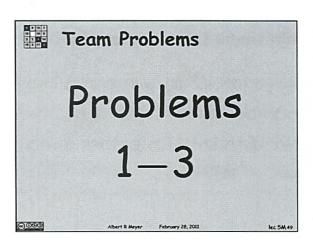
61394323221 = 3.3.3.7.11.11.37.37.37.53





# Unique Prime Factorization

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



(10 min late) (C) Factoring is hard Lemma to find GCD Gcd(a,b) = gcd(b, rem(a,b))Proof: a=qb+r Have same Vivisor 50 same 60 So can change # into smaller #5 Euclidean Algorithm as SM States = NNN Start = (a, b) Transitions (x, x) -) (y, rem (x,y)) repeat, repeat, etc G(D(n,0) = nInvarient - new # hat The same GCD P((x,y)) := [gcd(a,b) = gcd(x,y)]

P(start) trivally tree then true for anything you can get to at termination y=0 x = gcd(x, 0) = gcd(x, y) = gcd(a, b)reaches min in & 2 log 2 b transitions Theorem gcd(a,b) is an integer linear combo of a,b gcd(a,b) = sa + tb I show how to find the coefficients s,t Pulverizer Start a = 899 b=443 899 = 1 .493 + 406 avoient Justice Tremander Se 406=1.899-1.493 493=1=406+87 87 = 493 - 10406. back shotiste 406 = 4.87 + 58 =-1.899 + 2.493 87 = 1.58+29 57 = 406 - 4.87= 400 - 1.8 / Heep into = 800 - 1.8 / Heep into = 87 - 1.00 - 9.493 fram 2 Shages Shuch 58 - 2.29 + 0 gal = 29 29 = 87 - 1.58 = -6.899 + 11.4935 = -6 + = 11

3)
One is always & and one is always &

Oct + coeff for 899'

(-6 + 493 kl. 899 + (11 - -849 kl) - ...

(missed info, see slide 34)

Prime Divisibility Lemmai P Prime and plant) of pla or plant L) in class problem 3 P-Set - had to prome divide by a prime Correlary: It p is prime and pla, az am (missed) bet Unique Factorization Theory/ End. Theory of Alegba - Can do wealthy increasing to or decreasing Unique factorization of primes

If there is any there is a smallest one

a, Lp

9 is a divisor of n

So the 91 ln and n = p. p2 ··· ph

So Orlp: for some! by corellary

## 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.

**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 - and sols For #3 Very important

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

<sup>&</sup>lt;sup>1</sup>Euclid 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:

$$gcd(a, b) = gcd(b, rem(a, b))$$

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

$$gcd(259, 70) = gcd(70, 49)$$
 since  $rem(259, 70) = 49$   
 $= gcd(49, 21)$  since  $rem(70, 49) = 21$   
 $= gcd(21, 7)$  since  $rem(49, 21) = 7$   
 $= gcd(7, 0)$  since  $rem(21, 7) = 0$   
 $= 7$ .

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:

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  $\operatorname{rem}(x, y)$ , 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

1, So This was in the book 10 does not work 1,2,5,10 1+2+5=8 8 When is prime? - only then What is Ki - just a # K>1) 2-1/20-11 · First test 20-1 = 0 (x) k=1 21-1 = 1 & & Not prime by convention k=2 22-1=3  $\sqrt{prime}$ 2'(3) = 6 & Not prime but that is not what we are looking for looking for perfectness 1,2,3,6

1,2,3,6 1+2+3 0

But how does this work generally? What patterns are there in prime in pertect lour board) 2K+ (2K4) has following factors besides itself a) Those that are divided by the prime 2 "-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, ..., 2 k-2 Never show Symming (a) he get 2k-1 is pane - Show that those are (2h-1) \(\frac{k-7}{2}\) 2h = (2h-1) (\frac{k-1}{2}) The only divisors Suming (b) we get 2 n=2k-1 2h-1 (2h-1) besides itself is So summ of the factors of - (2 mm) (2 m-1 - 1+1) # =(2 hd) (2 hm)

2 our board)

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

Not the shortest way to do

$$\frac{8.50 - 19.21 = 1.50 - 8.50 + 19.21 = -1}{5.50 = 250}$$

$$\frac{-8.50 + 19.21 = -1}{12.21 = 2502}$$

$$\frac{-13.50 + 48.31.21 = 1 = 9cd(50,21)}{|x'=-13|}$$

$$\frac{-13.50 + 4831.21 = 1 = 9cd (50,21)}{|X'=-13|}$$

26 ealsors

SAFRAS

8.50 #-19.21 =1

-21.50 **ABO** +21.50

-13.500 + 31.21 = 1

So this is switching which is -

Can keep doing to Find a combos

0 - One side gets more

- Other side gets more (F)

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.

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

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

and

$$1 \cdot (2^k - 1), \quad 2 \cdot (2^k - 1), \quad 4 \cdot (2^k - 1), \quad \dots, \quad 2^{k-2} \cdot (2^k - 1).$$
 (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*, lcm(m, n), of m and n? Verify that

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

Solution.

$$g = 2^{3}11^{7}17^{9},$$

$$l = 2^{9}5^{24}7^{22}11^{211}13^{1}17^{12}19^{2}$$

$$gl = 2^{12}5^{24}7^{22}11^{218}13^{1}17^{21}19^{2} = mn$$

(b) Describe in general how to find the gcd(m, n) and 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.

<sup>&</sup>lt;sup>1</sup>Euclid 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.

<sup>&</sup>lt;sup>2</sup>It's fun to notice the "computer science" proof that (1) sums to  $2^k - 1$ . The binary 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 by  $10^k$  which is the binary representation of  $2^k$ .

Likewise, the factorization of lcm(m,n) is the shortest sequence that has the factorizations of m and n as subsequences. So the factorization of 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  $gcd(m, n) \cdot lcm(m, n)$  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

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

**Solution.** Here is the table produced by the Pulverizer:

x	y	rem(x, y)	1	[2] [1] [2] [2] [2] [2] [2] [2] [2] [2] [2] [2
		$\operatorname{rem}(x, y)$	=	$x-q\cdot y$
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	=	$8-1\cdot 5$
			199	$(50-2\cdot 21)-1\cdot (-2\cdot 50+5\cdot 21)$
			=	$3 \cdot 50 - 7 \cdot 21$
5	3	2	=	$5-1\cdot 3$
			=	$(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$
			118	$-5 \cdot 50 + 12 \cdot 21$
3	2	1		$3-1\cdot 2$
			=	$(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$
			_	8.50 - 19.21
2	1	0		

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

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

**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 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).

**Solution.** For some s and t, 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:

$$gcd(a, b) = gcd(b, rem(a, b))$$

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

$$gcd(259, 70) = gcd(70, 49)$$
 since  $rem(259, 70) = 49$   
 $= gcd(49, 21)$  since  $rem(70, 49) = 21$   
 $= gcd(21, 7)$  since  $rem(49, 21) = 7$   
 $= gcd(7, 0)$  since  $rem(21, 7) = 0$   
 $= 7$ .

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	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	=	$49 - 2 \cdot 21$
			=	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			=	$3 \cdot 259 - 11 \cdot 70$
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  $\operatorname{rem}(x,y)$ , 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.

```
Week 3 + 4

Sets + Relations

Set Theory.

Russell's Paradox

Intinity

Induction

SM: Invarients
```

Recursing

bad at

comfortable w/

Is reviewing book helpful?

Or do problems
- scan book

| A| = |B| suri
| A| = |B| bij
| A| 7 |B| stict

Cheat Sheet!
- was on last cheet sheet

Have not practice & Recruisive at al Last part though! Mar to Study ? - (ewrite answers - just read anywers - read qu t think \_ -try to do or own Not much time so might be best Problems are valients eff the book Its what format the sol is / How to start To pore invarient Prove that eq always holds P(c,s,a) > (c',s',a) That is ('s'+ a'=xy Go though each transion case Show invarient = (5 ta 0 Prove both - so invarient Bij = Same # |A| = |B|  $L^{2} h(s) = ((h_{1}(s), h_{2}(o)) ; f hi(s) \in L \text{ and } h_{1}(s) \notin L$ Und otherwise

(an take 3) to make indutive cases

Identity f(x) = X X pm EM
7 domain + co domain

Factorial f(0)=1

Fib Fid (0)-0

Fib(1) = 1

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

6.042 Cled Sheet Z

Replacement A formula pot set thoory defines the graph of a En Vx, y, ₹. [p(x, x) and p(x, 2)]> The image of any set sunder that Y= 3 is also a set t. 457 A! (KIX) O(XI) IE AESA Foundation There can not be an on seq ... Exat "EX, Exo of sets

where each one is member of previous. Member-mining (max) = [mtx and tx x,x4/2] 50 ∀x, x≠Ø → Jm member minnel (m,x) (hoice Given a set s, whose members

OLE non empty sets, no 2 of which have any elm in common, then is set co

Consisting of one el from each set ins.

Induction P() = predicate

IF P(0)

P(N-) P(n+1) for FrEN

then PM) for AmeN

Formaliant Principle If the preserved invallent of a gm is the for the start state, then it is true to all reachable states

Strong Location P() - predicate

If P(0)

to all nEN, P(6), P(1), Lu, P(n) together

Then P(n) is the for all men -> P(n+1)

Recursive -construct new data els from previous ones

Structural induction - w/ constructor

4,60,61,61,27777

Concatnation Expression polling

Studual Induction P() predicate, Qidata type If P(B) is the for each base case el b & R

for all 2 organent constructors C

[P(r) and P(s) -) P(c(1,4) for all 1,5 & R then Mc) is the for all rER

1. AZBASYB 2. |A| = (B) A injB 3. A = B A - by B 4. 1A 7 B A strut B

Mapping Rules

Bij an e(16) = a0 e(an) : = ant for n EN e(a) i = a for a EA - {b po, }

Russell's Paradox W:1= 66/5#53

50 SEW IH 545 for every 5

Cont. WEW IFF W #W

So V not a set-can't be a melanger of itself

ZFC

Extensionality, 2 sets - it same members (45, (3Ex IFF 3EY)) -) X=X

Pairing For 2 sets, x, y there is a set {x,y} w/x, y as only eles Axia As Esen ill

(5 = X Or 5 -1)/

Union Union of 2 is also a set

42 JUHX (JY, XEY AND YEZ) Iff XEV.

Infinity there is an as set. A nonempty Set x, such that for any set yex the set (y) is also a member of

Power Set All subsets form another set. LX. YX, Jp YU, UEX iff UEP