

1. (a) What does it mean to say an integer  $m$  divides an integer  $n$ ? Prove carefully using your definition that if  $m$  divides  $n$  then  $m$  divides  $pn$  for any integer  $p$ .

$m|n$  means  $n = mk$  for some integer  $k$ .

Say  $m|n$ . Then  $n = mk$

$$\therefore pn = m \underbrace{pk}_{\text{an integer}}$$

$$\therefore m | pn$$

(b) State the fundamental theorem of arithmetic as carefully as you can.

Every  $n \geq 1$  can be written as

$$n = p_1 \cdots p_k \quad \text{for unique } k \geq 0$$

and unique primes  $p_1 \leq \cdots \leq p_k$ .

(c) Suppose  $n \geq 1$  and  $p_1 < p_2 < \cdots < p_n$  are distinct primes. How many positive divisors does the number  $p_1 p_2 \cdots p_n$  (their product) have? Justify your answer carefully.

We have to pick a (possibly empty) subset of  $\{p_1, \dots, p_n\}$  and take the product of those guys.

So it's the same as the number of subsets of  $\{p_1, \dots, p_n\}$ , i.e.  $2^n$ .

2. (a) Use the Euclidean algorithm to find integers  $s$  and  $t$  such that

$$31s + 97t = 1.$$

Show your working!

$$(97) = 3 \cdot (31) + (4)$$

$$(31) = 7 \cdot (4) + (3)$$

$$(4) = (3) + (1)$$

$$\begin{aligned} \Rightarrow (1) &= (4) - (3) \\ &= (4) - ((31) - 7(4)) = 8(4) - (31) \\ &= 8((97) - 3(31)) - (31) \\ &= 8 \cdot (97) - 25 \cdot (31) \end{aligned}$$

$$\begin{aligned} s &= -25 \\ t &= 8 \end{aligned}$$

(b) Use mathematical induction to prove that  $57 | (7^{n+2} + 8^{2n+1})$  for all  $n \geq 0$ .

Base case  $n=0$ :  $7^2 + 8 = 49 + 8 = 57 \quad \checkmark \quad 57 | 57$

Induction step Assume  $57 | (7^{k+2} + 8^{2k+1})$

Seek to prove  $57 | (7^{(k+1)+2} + 8^{2(k+1)+1})$

Well  $7^{k+3} + 8^{2k+3} = 7^2 \cdot 7^{k+2} + 8^2 \cdot 8^{2k+1} \quad \leftarrow 8^2 = 7 + 57!$

$$= 7 \underbrace{(7^{k+2} + 8^{2k+1})}_{\substack{\text{div. by } 57 \\ \text{by induction} \\ \text{hypothesis}}} + 57 \cdot \underbrace{8^{2k+1}}_{\text{div. by } 57}$$

3

$\therefore$  div by 57  $\checkmark$   
(linear comb.)

Done by PMI

3. (a) What does it mean to say that a function  $f : A \rightarrow B$  is 1-1?

$$a \neq a' \Rightarrow f(a) \neq f(a')$$

Onto?

$$\forall b \in B \exists a \in A \text{ s.t. } f(a) = b$$

Bijjective?

1-1 and onto

Invertible?

There's a two-sided inverse  $f^{-1} : B \rightarrow A$   
 s.t.  $f^{-1} \circ f = 1_A$ ,  $f \circ f^{-1} = 1_B$ .

(b) Suppose that  $f : A \rightarrow B$  has a right inverse  $g : B \rightarrow A$ . Prove that  $f$  is onto.

$$f \circ g = 1_B$$

Take  $b \in B$ . Set  $a = g(b)$ .

$$\text{Then } f(a) = f(g(b)) = (f \circ g)(b) = 1_B(b) = b$$

$\therefore f(a) = b$   $\checkmark$   $f$  is onto.

(c) How many 1-1 functions are there from  $\{1, 2, 3, 4, 5\}$  to  $\{6, 7, 8, 9\}$ ? How zero many onto functions are there from  $\{1, 2, 3, 4, 5\}$  to  $\{6, 7, 8, 9\}$ ?

$\binom{5}{2} \cdot 4 \cdot 3!$  ← remaining 3 go to 3 in  $3!$  ways  
 $\uparrow$   $\uparrow$   
 Pick apart going to one of four

$$\frac{5! \cdot 4!}{3! \cdot 2!} = 5 \cdot 4 \cdot 3 \cdot 4 = \underline{\underline{240}}^4$$

4. Calculate the truth tables of the following compound propositions. Which of them is a tautology?

(a)  $[(p \rightarrow q) \vee (q \rightarrow r)] \rightarrow (p \rightarrow r)$ .

$p$	$q$	$r$	$p \rightarrow q$	$q \rightarrow r$	$p \rightarrow r$	$(p \rightarrow q) \vee (q \rightarrow r)$	$[(p \rightarrow q) \vee (q \rightarrow r)] \rightarrow (p \rightarrow r)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	0	1	1	1	1
0	1	1	0	1	1	1	1
1	0	0	0	1	0	1	0
1	0	1	0	1	1	1	1
1	1	0	1	0	0	1	0
1	1	1	1	1	1	1	1

(b)  $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ .

$p$	$q$	$r$	$p \rightarrow q$	$q \rightarrow r$	$p \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r)$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	0	1	1	0	1
0	1	1	0	1	1	0	1
1	0	0	0	1	0	0	1
1	0	1	0	1	1	0	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

Tautology

5. (a) Let  $g: \mathbb{Z} \rightarrow \mathbb{N}$  be the function defined by  $g(n) = |n|$ . For each  $n \in \mathbb{N}$ , describe the set  $g^{-1}(\{n\})$  of all pre-images of  $n$ . Is  $g$  1-1 and/or onto?

$$g^{-1}(\{0\}) = \{0\}$$

$$g^{-1}(\{n\}) = \{n, -n\} \text{ for } n > 0$$

It's onto (every  $n \in \mathbb{N}$  has at least one pre-image)

It's not 1-1 (some  $n \in \mathbb{N}$  has two pre-images)

(b) Answer the same questions as in (a) for the function  $g: \mathbb{Z} \rightarrow \mathbb{N}$  defined by  $g(n) = 1 + (-1)^n$ .

$$g^{-1}(\{0\}) = \{\text{all odd integers}\}$$

$$g^{-1}(\{2\}) = \{\text{all even integers}\}$$

$$g^{-1}(\{n\}) = \emptyset \text{ for all } n \in \mathbb{N} - \{0, 2\}.$$

Neither 1-1 nor onto.

6. (a) Write the sum  $1 + 3 + 5 + \dots + (2n - 1)$  of the first  $n$  odd numbers using the  $\sum$  notation.

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

(b) Prove by mathematical induction that  $1 + 3 + 5 + \dots + (2n - 1) = n^2$ .

Base case LHS = 1 RHS =  $1^2$  ✓

Induction step Assume  $1 + 3 + \dots + (2k - 1) = k^2$

Add  $(2k+1)$  to b.s.

$$1 + 3 + \dots + (2k - 1) + (2k + 1) = k^2 + 2k + 1$$

$$\therefore 1 + 3 + \dots + (2(k+1) - 1) = (k+1)^2 \quad \checkmark$$

Done by PMI

7. How many integer solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 = 100$$

subject to the constraints  $x_1 \geq 1, x_2 \geq 2, x_3 \geq 3$  and  $x_4 \geq 4$ ? Explain.

Same as  $y_1 + y_2 + y_3 + y_4 = 90$   $y_1, y_2, y_3, y_4 \geq 0$

90 balls in 4 boxes

90 o's 3 x's

$$\frac{93!}{90! 3!}$$

8. (a) Let  $f : \mathbb{R} \rightarrow \mathbb{R}$  be a function such that  $f(xy) = xf(y) + f(x)y$  for every  $x, y \in \mathbb{R}$ . Prove that  $f(x^n) = nx^{n-1}f(x)$ .

Induction on  $n$ .

Base case  $f(x^1) = f(x) = 1 \cdot x^0 \cdot f(x)$  ✓

Induction step Assume  $f(x^k) = kx^{k-1}f(x)$

Consider  $f(x^{k+1}) = f(x^k \cdot x) = x^k f(x) + f(x^k)x$   
 $= x^k f(x) + kx^k f(x)$   
 $= (k+1)x^k f(x)$  ✓ Done by PMI

(b) Solve the following recurrence relations:

(i)  $2a_n - 3a_{n-1} = 0$  for  $n \geq 1$ , subject to the boundary condition  $a_4 = 81$ .

$$a_n = \frac{3}{2} a_{n-1}$$

$$a_n = \left(\frac{3}{2}\right)^n a_0$$

$$81 = \left(\frac{3}{2}\right)^4 a_0 \quad \therefore a_0 = 16$$

$$a_n = 16 \cdot \left(\frac{3}{2}\right)^n$$

(ii)  $a_n = 5a_{n-1} + 6a_{n-2}$  for  $n \geq 2$ , subject to the boundary conditions  $a_0 = 1$  and  $a_1 = 3$ .

Characteristic equation:  $x^2 - 5x - 6 = 0$

$$(x-6)(x+1) = 0 \quad \text{roots } 6, -1$$

$$\therefore a_n = A \cdot 6^n + B \cdot (-1)^n$$

$$\begin{cases} A+B=1 \\ 6A-B=3 \end{cases} \quad A = \frac{4}{7}, B = \frac{3}{7}$$

$$a_n = \frac{4}{7} \cdot 6^n + \frac{3}{7} \cdot (-1)^n$$