

1. (a) What is the definition of a prime number  $p$ ?

An integer  $p > 1$  with no positive divisors other than 1 and  $p$ .

(b) Use the Euclidean algorithm to find integers  $s$  and  $t$  such that

$$17s + 101t = 1.$$

Show your working!

$$(10) = 5 \cdot (17) + (16)$$

$$(17) = (16) + (1)$$

$$1 = (17) - (16)$$

$$= (17) - (10) - 5 \cdot (17) = 6 \cdot (17) - (10)$$

$$\boxed{\begin{array}{l} s = 6 \\ t = -1 \end{array}}$$

← answer (make sure this is clear!)

(c) Use your answer to (b) to solve the congruence equation  $17x \equiv 66 \pmod{101}$ . Note  $1 \equiv 6 \cdot 17 \pmod{101}$  by (b)

$$17x \equiv 66 \pmod{101}$$

$$\therefore x \equiv 6 \cdot 66 \pmod{101}$$

$$\therefore x \equiv 93 \pmod{101}$$

2. Let  $G$  be the digraph with

$$V(G) = \{v_1, v_2, v_3, v_4\},$$

$$E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6\}$$

and directed edges defined by the function

$$\gamma : E(G) \rightarrow V(G) \times V(G)$$

$$e_1 \mapsto (v_3, v_1),$$

$$e_2 \mapsto (v_3, v_2),$$

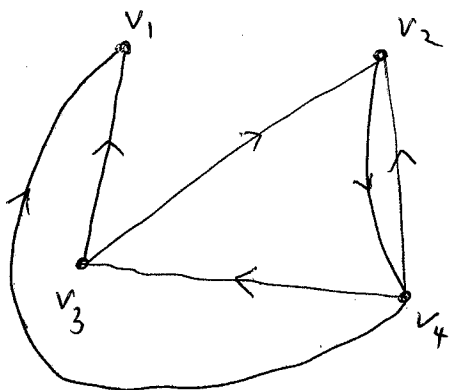
$$e_3 \mapsto (v_4, v_3),$$

$$e_4 \mapsto (v_4, v_1),$$

$$e_5 \mapsto (v_4, v_2),$$

$$e_6 \mapsto (v_2, v_4).$$

(a) Draw a picture representing the digraph  $G$ .



(b) Write down the adjacency matrix of  $G$ .

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

(c) What is the length of the shortest path that passes through every vertex?

$$v_2 \rightarrow v_4 \rightarrow v_3 \rightarrow v_1 \quad 3 \quad \underline{\text{Length } 3}$$

3. (a) What does it mean to say an integer  $m$  divides an integer  $n$ ? Prove directly from your definition that if  $m$  divides  $n$  and  $m$  divides  $p$  then  $m$  divides  $n + p$ .

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

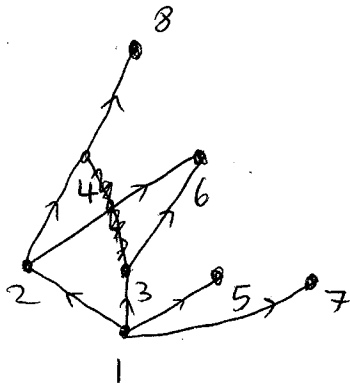
If  $m|n$  and  $m|p$  then  $n = mk, p = ml$

$$\therefore n+p = mk + ml = m(k+l)$$

$\therefore n+p$  is a multiple of  $m$

$$\therefore m \mid \underline{\underline{(n+p)}}$$

(b) Draw the digraph of the partial order  $|$  on  $\{1, 2, 3, 4, 5, 6, 7, 8\}$  defined by  $m|n$  if  $m$  divides  $n$ .



(By convention you're not meant to draw any other edges than this!)

(c) Define a relation  $\trianglelefteq$  on  $\mathbb{Z}$  by  $m \trianglelefteq n$  if  $m^2 \leq n^2$ . Is  $\trianglelefteq$  a partial order?

No e.g.  $-2 \trianglelefteq 2$  and  $2 \trianglelefteq -2$  but  $2 \neq -2$

$\therefore$  fails (A5)

4. (a) Work out the truth table for the compound propositions  $p \vee (q \wedge r)$  and  $(p \vee q) \wedge (p \vee r)$ .

$p$	$q$	$r$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$	$q \wedge r$	$p \vee (q \wedge r)$
0	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	1	1	1	1
1	0	0	1	1	1	0	1
1	0	1	1	1	1	0	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

(b) Using your answer to (a), explain why  $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ .

These two columns are the same, so

$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$  is always true, i.e. a tautology.

This is what  $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$  means.

(c) Explain as clearly as you can how to translate the statement you just proved into the following theorem about sets:  $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$ .

Let  $p = "x \in A"$ ,  $q = "x \in B"$ ,  $r = "x \in C"$ .

Then  $"x \in A \cup (B \cap C)"$  is  $p \vee (q \wedge r)$  and  $"x \in (A \cap B) \cup (A \cap C)"$  is  $(p \wedge q) \vee (p \wedge r)$ .

So (b) shows  $x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$

This is what  $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$  means.

5. (a) Prove that  $369^{123456789} - 13579$  is divisible by 10.

Reduce modulo 10:

$$\equiv 9^{123456789} - 9 \pmod{10}$$

$$\equiv 9 - 9 \equiv 0 \pmod{10}$$

$\therefore$  It is divisible by 10.

$$9^2 = 81 \equiv 1 \pmod{10}$$

$$9^{\text{any even power}} \equiv 1 \pmod{10}$$

$$9^{\text{any odd power}} \equiv 9 \pmod{10}$$

(b) If  $x$  is rational and  $y$  is irrational prove that  $x + y$  is irrational.

Let  $x$  be rational and  $y$  irrational.

To prove  $x+y$  is irrational, assume for a contradiction that  $x+y$  is rational.

Then  $(x+y) - x = y$  is rational ~~///~~.

6. Consider the function  $f: \mathbb{N} \rightarrow \mathbb{N}$  defined by the formula  $f(n) = \lfloor \sqrt{n} \rfloor$ .

(a) Compute  $f^{-1}(1)$ .

$$f^{-1}(1) = \{1, 2, 3\}$$

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ 2 &\mapsto 2 \\ 3 &\mapsto 1 \\ 4 &\mapsto 2 \\ &\vdots \end{aligned}$$

(b) Is this function 1-1, onto, or a 1-1 correspondence?

Not 1-1.

onto (eg as  $g: \mathbb{N} \rightarrow \mathbb{N}$ ,  $n \mapsto n^2$  is a right inverse)

Not a 1-1 correspondence.

7. Prove by induction on  $n = 1, 2, \dots$  that

$$\sum_{i=1}^n i2^i = (n-1)2^{n+1} + 2.$$

Base case  $n=1$  LHS = 2 RHS = 2 ✓

Induction step Assume true when  $n=k$ , some fixed  $k \geq 1$ ,

i.e.  $\sum_{i=1}^k i2^i = (k-1)2^{k+1} + 2$  ← ind. hyp.

Seek to prove it when  $n=k+1$ .

$$\sum_{i=1}^{k+1} i2^i = \sum_{i=1}^k i2^i + (k+1)2^{k+1}$$

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

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

$$= 2k \cdot 2^{k+1} + 2$$

$$= k \cdot 2^{k+2} + 2$$

Done by P.M.I.

8. Suppose  $(S(n))_{n \geq 0}$  is the sequence defined by the following pseudo-computer program:

```

S(n)
Input : an integer  $n \geq 0$ 
begin
  if  $n = 0$  then return 1
  if  $n = 1$  then return 4
  return  $4S(n-1) - 4S(n-2)$ 
end

```

(a) Compute  $S(2)$

$$S(2) = 0$$

(b) Write down the recurrence relation defining  $S(n)$  in usual mathematical notation.

$$S(0) = 1 \quad S(1) = 4$$

$$S(n) = 4S(n-1) - 4S(n-2)$$

(c) Solve the recurrence relation to find an explicit formula for  $S(n)$ .

Characteristic equation:  $x^2 - 4x + 4 = 0$   
 $(x-2)^2 = 0$  repeated roots

$\therefore$  general solution is  $S(n) = (A+1) \cdot 2^n$

$$S(0) = 1 = B$$

$$S(1) = (A+1) \cdot 2 = 4 \quad \therefore A = 1$$

$$\therefore \underline{\underline{S(n) = (n+1)2^n}}$$