

# YORK UNIVERSITY

Faculty of Arts

Faculty of Pure and Applied Science

January - April 2003

AS/SC/MATH 2320 3.0 P

Term Test 1a

SOLUTIONS

1. (8 marks) Let  $f: \mathbb{R} \rightarrow \mathbb{Z}$  be defined by  $f(x) = \lceil 2x - 1 \rceil$ , where  $\mathbb{R}$  is the set of real numbers and  $\mathbb{Z}$  is the set of integers.

- (a) Is  $f(x)$  a one-to-one? Justify your answer.

*Answer:*

No,  $f(x)$  is not one-to-one.

Note that  $f(\frac{1}{2}) = \lceil (2)\frac{1}{2} - 1 \rceil = 0$ , and  $f(\frac{1}{3}) = \lceil (2)\frac{1}{3} - 1 \rceil = \lceil -\frac{1}{3} \rceil = 0$ .

- (b) Is  $f(x)$  an onto? Justify your answer.

*Answer:*

Yes,  $f(x)$  is not onto.

By the definition,  $f(x)$  is onto, if  $(\forall m \in \mathbb{Z})(\exists x \in \mathbb{R}) : f(x) = m$ , that is  $\lceil 2x - 1 \rceil = m$ .

But, by the definition of the ceiling function,

$m = \min\{y \in \mathbb{Z} \mid y \geq 2x - 1\}$ , which is attained at some value  $x_0 \in \mathbb{R}$ .

- (c) Determine  $f(\mathbb{N})$ , where  $\mathbb{N}$  is the set of natural numbers.

*Answer:*

$f(\mathbb{N}) = \{-1, 1, 3, 5, 7, \dots\} = \{-1\} \cup \{n = 2k - 1 \mid k \in \mathbb{Z}^+\}$ .

2. (8 marks)

- (a) Write a pseudocode for the insertion sort algorithm that puts all integers in the list of  $n$  integers ( $n$  is a positive integer) in increasing order.

*Answer:*

The insertion sort algorithm is described at page 127 of the textbook.

- (b) Describe how the number of comparisons used in the worst case changes when the size of the list to be sorted increases from  $n$  to  $2n$  when the insertion sort algorithm from part (a) is used.

*Answer:*

The insertion sort algorithm uses

$$2 + 3 + \dots + n = \frac{n(n+1)}{2} - 1 = \frac{n^2}{2} + \frac{n}{2} - 1$$

comparisons to sort a list with  $n$  integers. Therefore, to sort the list with  $2n$  integers it will use

$\frac{(2n)^2}{2} + \frac{2n}{2} - 1 = 4\frac{n^2}{2} + n - 1$  comparisons, i.e. the number of comparisons goes up by a factor of 4.

3. (8 marks) Let  $f: \mathbb{R} \rightarrow \mathbb{R}$  and  $g: \mathbb{R} \rightarrow \mathbb{R}$ . Show that  $f(x)$  is  $O(g(x))$  if and only if  $g(x)$  is  $\Omega(f(x))$ .

*Answer:*

$$f(x) \text{ is } O(g(x)) \iff (\exists \text{ constants } C, k) : x > k \implies |f(x)| \leq C |g(x)|.$$

Assume that  $C > 0$  and  $k > 0$ .

$$g(x) \text{ is } \Omega(f(x)) \iff (\exists \text{ constants } C' > 0, k' > 0) : x > k' \implies |g(x)| \geq C' |f(x)|.$$

Setting  $k' = k$ , we obtain

$$x > k \implies \frac{1}{C'} |g(x)| \geq |f(x)|,$$

$$\text{or } |f(x)| \leq C |g(x)|, \text{ with } C = \frac{1}{C'}.$$

4. (8 marks)

- (a) Let  $a$  and  $b$  be relatively prime positive integers. Prove that if  $a$  and  $b$  both divide an integer  $c$ , then  $ab$  divides  $c$ .

*Hint:* You may use the fact that the greatest common divisor of two positive integers can be written as a linear combination of these integers with integer coefficients.

*Answer:*

Since  $a$  and  $b$  are relatively prime,  $\gcd(a, b) = 1$ . Then  $(\exists s, t \in \mathbb{Z}) : 1 = sa + tb$ .

Multiplying both sides by  $c$ , we obtain  $c = csa + ctb$ .

Now,  $a \mid c \implies c = ka$ , for some  $k \in \mathbb{Z}$ ,

$b \mid c \implies c = lb$ , for some  $l \in \mathbb{Z}$ .

Hence,  $c = csa + ctb = (lb)sa + (ka)tb = (ls)ab + (kt)ab = (ls + kt)ab = (q)ab$ , for some  $q = (ls + kt) \in \mathbb{Z}$ , that is  $ab \mid c$ .

- (b) Use the Euclidean Algorithm to find  $\gcd(580, 50)$ .

*Answer:*

$$580 = 50 \cdot 11 + 30$$

$$50 = 30 \cdot 1 + 20$$

$$30 = 20 \cdot 1 + 10$$

$$20 = 10 \cdot 2 + 0.$$

Hence,  $\gcd(580, 50) = \gcd(50, 30) = \gcd(30, 20) = \gcd(20, 10) = \gcd(10, 0) = 10$ .

5. (8 marks)

- (a) Find an inverse of 5 modulo 12, and an inverse of 12 modulo 5.

*Answer:* Since  $\gcd(5, 12) = 1$ , both inverses exist.

$$12 = 5 \cdot 2 + 2$$

$$5 = 2 \cdot 2 + 1.$$

$$\text{So, } 1 = 5 + (-2)2 = 5 + (-2)[12 + (-2)5] = 5 \cdot 5 + (-2)12,$$

that is, 5 is an inverse of 5 modulo 12, and  $-2$  is an inverse of 12 modulo 5.

Note that  $-2 \equiv 3 \pmod{5}$ . Hence, 3 is also an inverse of 12 modulo 5.

- (b) Find all solutions to the linear congruence  $19x \equiv 3 \pmod{141}$ .

*Answer:*

Since  $\gcd(19, 141) = 1$ , there exists an inverse of 19 modulo 141.

$$141 = 19 \cdot 7 + 8$$

$$19 = 8 \cdot 2 + 3$$

$$8 = 3 \cdot 2 + 2$$

$$3 = 2 \cdot 1 + 1.$$

$$\text{So, } 1 = 3 + (-1)2 = 3 + (-1)[8 + (-2)3] = 3 \cdot 3 + (-1)8 = 3[19 + (-2)8] + (-1)8 =$$

$$3 \cdot 19 + (-7)8 = 3 \cdot 19 + (-7)[141 + (-7)19] = (-7)141 + 52 \cdot 19,$$

and 52 is an inverse of 19 modulo 141.

Multiplying the both sides of the linear congruence by 52, we obtain

$$x = 52 \cdot 3 = 156 \equiv 15 \pmod{141} \text{ or } \{15 + k141 \mid k \in \mathbb{Z}\}.$$

*Bonus* (5 marks) Let  $a, b, c, m \in \mathbb{Z}$ , with  $m$  greater than one. Prove the implication:

$$d = \gcd(c, m) \ \& \ ac \equiv bc \pmod{m} \implies a \equiv b \pmod{\frac{m}{d}}.$$

*Answer:*

$$d = \gcd(c, m) \implies d \mid c \ \& \ d \mid m \ \& \ \gcd\left(\frac{c}{d}, \frac{m}{d}\right) = 1.$$

$$ac \equiv bc \pmod{m} \implies m \mid ac - bc \implies m \mid c(a - b)$$

$$\implies \frac{m}{d} \mid \frac{c}{d}(a - b) \implies \frac{m}{d} \mid a - b, \quad \because \frac{m}{d} \nmid \frac{c}{d}. \quad \text{Hence, } a \equiv b \pmod{\frac{m}{d}}.$$

The end