Discrete mathematics final examination – solutions

Section A

1) B (1 mk)
2) B (1 mk)
3) B (1 mk)
4) C (1 mk)
5) B (1 mk)
6) Negate the statement; ***All students do not take coffee.*** *(do not use the statement, it is not the case…or it is not true….) (1 mk)*
   Some students take coffee.
7) Determine the check digit for the ISBN – 13 digit 978-8-120-31502 (2 mks)

$$9 + 8 + 1 + 0 + 1 + 0 + x + 3(7 + 8 + 2 + 3 + 5 + 2) = 0 mod\ 10$$

$$19 + x + 81 = 0\ mod\ 10$$

$$x + 100 => x = 0$$

8) Outline an area where each of the following concepts can be applied in technology, graph theory, permutation functions, logic. (3 mks)
   Graph theory – designing networks; permutation functions – cryptography/ciphers; logic – automating reason for machines.
9) Explain a cryptosystem (2 mks)
   It is a structure with 5 -tuples is (P, C, E, D, K) – P set of plaintexts, C – set of ciphertexts, E – Encrypting functions, D – Decrypting functions, and K set of keys.

10) Explain rule of inference (2 mk)

    A compound proposition that is a tautology and involves an implication e.g. modus ponens.

11) State without proof the De Morgan's laws of logic (2 mk)
    Conjunction and disjunction interchanges under negation.
12) Explain a mathematical proof (1 mk)
    It is an inferential argument for a mathematical statement, showing that the stated assumptions logically guarantee the conclusion.
    (An argument that establishes the truth of a theorem)
13) Use the Euclidean algorithm to show that the gcd (846 , 264) satisfy the Bezout's theorem. (4 mks)

$$846 = 264 \cdot 3 + 54$$
$$264 = 54 \cdot 4 + 48$$
$$54 = 48 \cdot 1 + 6$$
$$48 = 6 \cdot 8 + 0$$

⇨ $6 = 54 - 1(48) = 54 - 1[264 - 4(54)] = 54 - 1(264) + 4(54) = 5(54) - 1(264)$

- $6 = 5[846 - 3(264)] - 1(264) = 5(846) - 15(264) - 1(264)$
- $6 = 5(846) - 16(264)$

14) Explain a major weakness of shift cipher and explain how affine cipher address this. (2 mks)

It is easy to hack or crack due to the frequency rate of the alphabet use. Affine complicates the function by adding a multiplication factor.

15) Define the following terms and illustrate each with a relevant example: a proposition, a theorem, and an axiom (6 mks)

Proposition is a statement that can be a signed a value e.g. today is Sunday.
Theorem is a proposition that has been proved to be true e.g. Pythagoras theorem.
An axiom is a statement that is assumed to be true e.g. a + b = b + a where a and b are any real numbers.

Section B

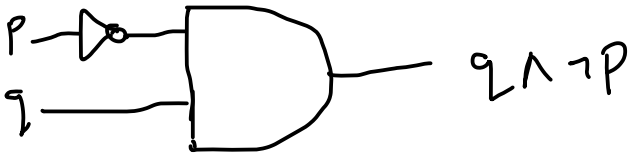
Question 1 (Compulsory – 20 marks)

a) Consider the following permutation functions: $\mathrm{p}_1 = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}; p_2 = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix}$ hence evaluate; $\mathrm{p}_2^{-1} \circ \mathrm{p}_2 \circ \mathrm{p}_1^{-1}$ **(2 marks)**

$\mathrm{p}_2^{-1} \circ \mathrm{p}_2 \circ \mathrm{p}_1^{-1} = \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}$

b) Consider the statement; ***If I do not read then I will not go home.*** Write down its converse and design a logic gate for the negation of the converse. **(3 marks)**

(Use p: I will not read; q: I will not go home)
If I will not go home, then I will not read i.e. $q \rightarrow p$
Its negation is $\neg(q \rightarrow p) \equiv q \wedge \neg p$



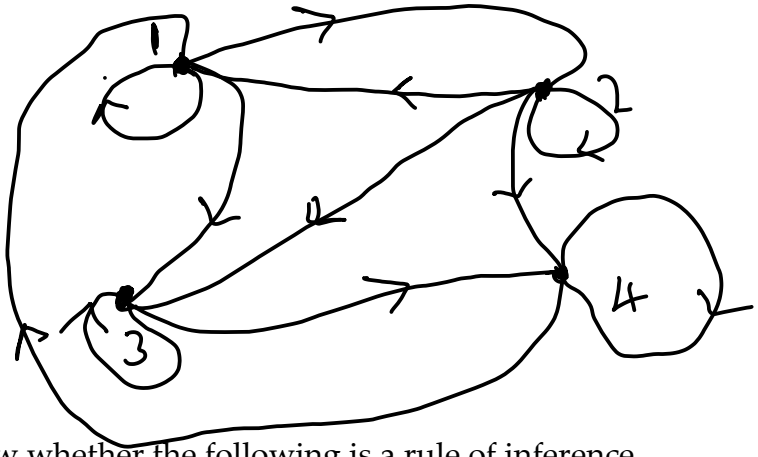
Alternatively correct circuit.

c) Let set A = {1,2,3,4} with relation R = {(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,3), (3,4), (2,4), (4,1), (4,4)}. Hence.

i) Write $\mathrm{M_R}$ **(1 mark)**

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

ii) Construct the diagraph for the relation **(1 mark)**



d) Show whether the following is a rule of inference. **(2 marks)**

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

We need to show $\neg q \wedge (p \rightarrow q) \rightarrow \neg p$ *is a tautology (alternatively show validity).*

p	q	$p \rightarrow q$	$\neg q$	$\neg q \wedge (p \rightarrow q)$	$\neg p$	$\neg q \wedge (p \rightarrow q) \rightarrow \neg p$
1	*1*	*1*	*0*	*0*	*0*	*1*
1	*0*	*0*	*1*	*0*	*0*	*1*
0	*1*	*1*	*0*	*0*	*1*	*1*
0	*0*	*1*	*1*	*1*	*1*	*1*

Alternatively, prove by contradiction that the argument is invalid i.e. the conclusion is false, and the assumptions are all true i.e.

1. $\neg p$ *is F*
2. $p \rightarrow q$ *is T (with p as T and q as T)*
3. $\neg q$ *is F*

Which is a contradiction, the argument is valid.

e) Determine the inverse of 17 (mod 31) using the Euclidean algorithm method (show working). **(4 marks)**

$$17x = 1(mod\ 31) => (17, 31) = 1$$

$$31 = 17 \times 1 + 14$$

$$17 = 14 \times 1 + 3$$

$$14 = 3 \times 4 + 2$$

$$3 = 2 \times 1 + 1$$

$$=> 1 = 3 - 1(2)$$

$$1 = 3 - 1[14 - 4(3)] = 3 - 1(14) + 4(3) = 5(3) - 1(14)$$

$$1 = 5[17 - 1(14)] - 1(14) = 5(17) - 6(14)$$

$$1 = 5(17) - 6[31 - 1(17)] = 5(17) - 6(31) + 6(17)$$

$$\therefore 1 = 11(17) - 6(31)$$

Hence, we have.

$$11(17)(\text{mod } 31) - 6(31)(\text{mod } 23) = 1 \text{ (mod } 31)$$

$$11(17)(\text{mod } 31) = 1 \text{ (mod } 31)$$

Hence the inverse of 17 is 11 mod 31.

Alternatively use Cayley table.

f) Solve the following linear congruence (show working); **(4 marks)**

$$13\text{x} \equiv 7(\text{mod } 33)$$

Introduce another parameter t such that $13t = 1\ mod\ 33\ i.e.$

$$13xt \equiv 7t(mod\ 33)$$

Hence, we have.

$$x = 7t\ mod\ 33$$

Since 13 and 33 are relatively prime then $13t + 33s = 1$

$$=> 33 = 2(13) + 7$$
$$13 = 1(7) + 6$$
$$7 = 1(6) + 1$$

Hence, we get.

$$1 = 7 - 6 = 7 - (13 - 7)$$
$$1 = 2(7) - 13$$
$$1 = 2(33 - 2 \cdot 13) - 13$$
$$1 = 2(33) - 4(13) - 13 = 2(33) - 5(13)$$
$$1 = 33(2) + 13(-5)$$
$$our\ t = -5\ and\ s = 2$$

Hence, we have.

$$x = 7(-5)mod\ 33 = 7(33 - 5)mod\ 33 = 7(28)mod\ 33 = 196\ mod\ 33 = 31\ mod\ 33$$
$$x = 31$$

1) Show that if n is a positive integer then (n^3 + n) is even **(3 marks)**

<u>*When n is even*</u>

$$n = 2k\ for\ some\ k \in R => n^3 + n = (2k)^3 + 2k = 8k^3 + 2k = 2(4k^3 + k)$$

$$if\ 4k^3 + k = K\ then\ n^3 + n = 2K - even$$

<u>*When n is odd*</u>

$$n = 2k + 1\ for\ some\ k \in R => n^3 + n = (2k + 1)^3 + (2k + 1)$$

$$= 8k^3 + 12k^2 + 6k + 1 + 2k + 1$$

$$= 8k^3 + 12k^2 + 8k + 2$$

$$= 2(4k^3 + 6k^2 + 4k + 1)$$

$$if\ 4k^3 + 6k^2 + 4k + 1 = K\ then\ n^3 + n = 2K - even$$

Question 2 (10 marks) – Optional

a) Use logic connectives to write the following statements.

(i) It is not the case that for every student x there exists a student y such that student x works smarter than y. **(1 mark)**

$\neg(\forall x \exists y, F(x,y))$ *where* $F(x,y) - x\ works\ smarter\ than\ y$

(ii) Some students are illogical or not all phones are *smartphone*. **(1 mark)**

$(\exists x, p(x)) \vee (\exists y, \neg q(y))$ where $p(x) - illogical\ students, q(y) smartphones$

b) Consider the argument.

If 11 is less than 6, then 11 is not a prime number
11 is not less than 6
$\therefore$ 11 is a prime number

Let p: 11 is less than 6, and q: 11 is a prime number. Hence.

(i) Write the following argument using logic connectives. **(2 marks)**

$$\begin{array}{l} p \rightarrow \neg q \\ \neg p \\ \hline q \end{array}$$

(ii) Determine the validity of the argument. **(3 marks)**

NB: Use truth table or rule of inference

1. $q\ is\ F$
2. $\neg\ p\ is\ T$
3. $p \rightarrow \neg q\ \ is\ T,\ \ since\ p\ is\ F\ from\ (2) and\ \neg q\ is\ T\ from\ (1)$

$\therefore\ the\ argument\ is\ invalid$

c) Evaluate; $(12345) \circ (5634)(27) \circ (4652317)$ and determine the number and length of the cycles of the solution. **(3 marks)**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 4 & 5 & 6 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 1 & 6 & 2 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 2 & 4 & 7 & 6 & 1 \end{pmatrix}$$

$$= (13257)$$

1 cycle, length 5

Question 3 (10 marks) – Optional

a) Using the transposition cipher based on the permutation of the set {1,2,3,4,5} with $p(1) = 5, p(2) = 3, p(3) = 4, p(4) = 1, p(5) = 2$, to.

i) Encrypt the plaintext; THE DUST STORM AND A FOOL **(2 marks)**

plaintext	*T*	*H*	*E*	*D*	*U*	*S*	*T*	*S*	*T*	*O*	*R*	*M*	*A*	*N*	*D*	*A*	*F*	*O*	*O*	*L*
ciphertext	*D*	*U*	*H*	*E*	*T*	*T*	*O*	*T*	*S*	*S*	*N*	*D*	*M*	*A*	*R*	*O*	*L*	*F*	*O*	*A*

ii) Decrypt the ciphertext; NEJEM DTYEOCLISHFRSSAAYMDOEEHRT **(2 marks)**

ME ENJOYED THIS CLASS FROM DAY THREE

b) Use Fermat's Little theorem to simplify; **(3 marks)**

$$7^{65}(\text{mod } 19) = (7^{18})^{3+11}(\text{mod } 19) = (7^{18})^3 \times 7^{11} \text{ mod } 19 = 7^{11}\text{mod } 19 = 11$$

c) Prove by mathematical induction that for all positive integers n **(3 marks)**

$$3 + 11 + \cdots + (8\text{n} - 5) = 4\text{n}^2 - \text{n}$$

$$p(1) = 4 - 1 = 3$$

Assume it is true for $n = k$

$$3 + 11 + \cdots + (8\text{k} - 5) = 4\text{k}^2 - \text{k}$$

$$Then\ we\ prove\ for\ n = k + 1$$

$$3 + 11 + \cdots + (8\text{k} - 5) + 8(\text{k} + 1) - 5 \ = 4\text{k}^2 - \text{k} + 8(\text{k} + 1) - 5$$

RHS becomes.

$$4\text{k}^2 - \text{k} + 8(\text{k} + 1) - 5 = 4\text{k}^2 - k + 8k + 8 - 5$$

$$= 4k^2 + 7k + 3$$

$$= 4k^2 + 4k + 3k + 3$$

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

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

This is $4n^2 - n$ with $n = k + 1$, hence it is true for all positive integers.

'And now, Lord, what wait I for? My hope is in thee.'
Psalms 39:7 (RSV)