W228/201C, W282/201C,

DUBLIN INSTITUTE OF TECHNOLOGY

DT228 BSc. (Honours) Degree in Computer Science

Year 2

DT282 BSc. (Honours) Degree in Computer Science (International)

Year 2

WINTER EXAMINATIONS 2015/2016

MATHEMATICS 2 [CMPU2012]

MR. PAUL SMYTH
DR. DEIRDRE LILLIS

TUESDAY 12TH JANUARY 9.30 A.M. – 11.30 A.M.

TWO HOURS

INSTRUCTIONS
QUESTION 1 IS COMPULSORY.
ANSWER QUESTION 1 AND TWO OF THE OTHER THREE QUESTIONS.
ALL YOUR WORK MUST BE SHOWN.

MATHEMATICAL TABLES ARE AVAILABLE.

1. (a) State Fermat's Little Theorem. Using the fact that 1039 is prime, calculate the residue of

$$31^{5323905},$$

modulo 1039.

(8 marks)

(b) Figure 1 shows the state diagram for a finite state automaton M. Determine whether the automaton M recognises the words

i. λ

ii. aba^3b^2a

iii. ab^2a^3

Construct a table for the state transition function for M.

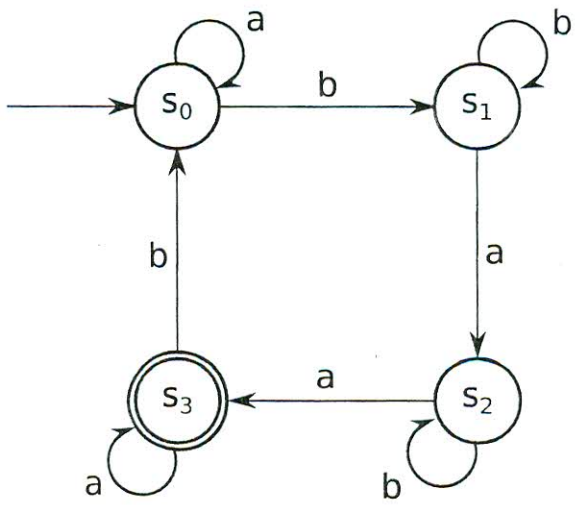

Figure 1: The finite state automaton M.

(8 marks)

(c) Write down the steps of Kruskal's algorithm for constructing a minimal weight spanning tree for a graph and use it to construct a minimal weight spanning tree for the weighted graph H shown in Figure 2. What is the weight of this minimal spanning tree?

(8 marks)

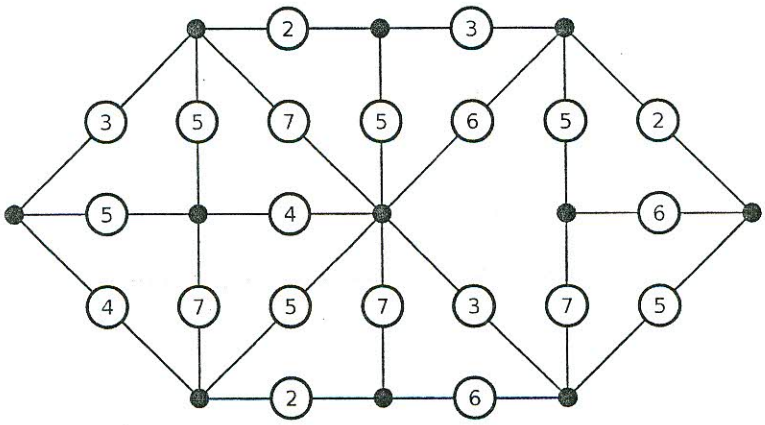

Figure 2: The weighted graph H.

(d) Let the domain of discourse be the set of integers $\mathbb{Z}$. Given the predicates

$$\begin{aligned} E(x) &= x \text{ is even} \\ O(x) &= x \text{ is odd} \\ D(x,y) &= x|y \\ P(x) &= x \text{ is prime} \end{aligned}$$

then express the following statements symbolically using logical notation

(i). Every integer which is even is divisible by 2

(ii). Some odd integers are divisible by 3

(iii). Not every integer is prime

(iv). No integer is both even and odd

(8 marks)

(e) Show that 6 is a primitive root of 11 and hence find the following discrete logarithms, modulo 11,

i. $\log_6 5$

ii. $\log_6 7$

(8 marks)

2. (a) A state diagram for a finite state machine is shown in Figure 3. Write down the state table for the machine. Determine the output sequence produced by the machine if the input sequence is 0110111.

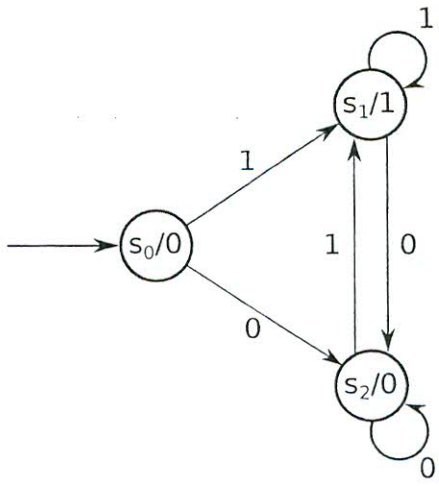

Figure 3: A state diagram for a finite state machine.

(10 marks)

(b) A random experiment consists of rolling two fair dice once. Define the events

A : the numbers rolled are not the same

B : the sum of the two dice is 7

C : both numbers rolled are even

and calculate $P(B|A)$ and $P(C|A)$ giving your answer as a fraction in each case. Is event B independent of A?

(11 marks)

(c) A chess player enters a tournament with 6 rounds. Based on past performance the player has a 3/5 chance of winning any given game against another player in his section of the tournament. Assuming each game is an independent Bernouilli trial, calculate the probability that:

i. The player wins exactly three games.

ii. The player wins no games.

iii. The player wins at least four games.

In each case give your answer as a fraction.

(9 marks)

3. (a) If $9454 \equiv 1 \mod 137$ then solve the linear congruence equation

$$4727x \equiv 61 \mod 137.$$

(5 marks)

(b) Calculate the ISBN−10 check digit for

$$0 - 201 - 02969 - ?$$

and determine if $0 - 7167 - 0344 - 0$ is a valid ISBN−10 number.

(5 marks)

(c) Generate the first five values for a linear congruential pseudorandom number generator with a starting seed of 3, a modulus of 29, a multiplier of 19 and an increment of 373.

(5 marks)

(d) The ciphertext

RIUA♡E

was encrypted by means of a Hill digraph cipher, using the matrix

$$A = \begin{pmatrix} 11 & 13 \\ 1 & 15 \end{pmatrix}$$

modulo 27, where $\heartsuit = 0, A = 1, B = 2, \ldots, Z = 26$. Find the inverse of A modulo 26 and hence retrieve the message plaintext.

(15 marks)

4. (a) Define the graph theory terms
   i. Simple path
   ii. Cycle
   iii. Euler cycle

(6 marks)

(b) For the graph G shown in Figure 4, answer each of the following questions. Be careful to justify your answers.
   i. Is G complete?
   ii. Is G bipartite? If it is bipartite then draw the graph in partitioned form.
   iii. Is G complete bipartite?

iv. Does G have an Euler path?

v. Does G have an Euler cycle?

(10 marks)

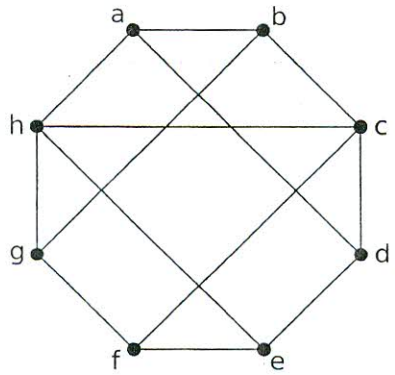

Figure 4: The graph G.

(c) Using Dijkstra's Algorithm calculate a minimum weight path, from a to f, for the weighted graph K, shown in Figure 5.

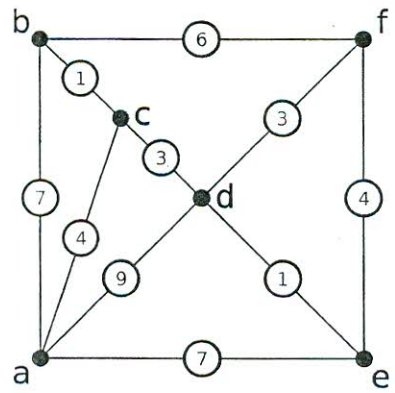

Figure 5: The weighted graph K.

(14 marks)

Back down 10:22

COLLEGE EXAMINATIONS

AMENDMENTS TO EXAMINATION QUESTION PAPER

K304 & K106 & K204

COURSE REF: D228/282/201C VENUE: B2 & B3.

SUBJECT: MATHEMATICS

DATE: 12/1/16

TIME: 10:06

SIGNED:

INSTRUCTIONS:

Q3 (d)

They should be the ~~modulo~~ same modulo 27.

3 (d) should read

.... using the matrix $A = \begin{pmatrix} 11 & 13 \\ 1 & 15 \end{pmatrix}$

modulo 27, where $\cup = 0$, $A = 1$, $B = 2$, ... $Z = 26$

Find the inverse of A modulo 27 and hence retrieve the message plaintext.