King Fahd University of Petroleum & Minerals

College of Computer Science and Engineering

Information and Computer Science Department

First Semester 191 (2019/2020)

ICS 254 – Discrete Structures II

Solution to Midterm Exam

Thursday, 24 October, 2019

Time: 90 minutes

Name: ______________________________

ID#									

Please circle your section number below:

02 – Faisal Alvi – 1100-1215	01 – Faisal Alvi – 1230-1345

Question #	Max Marks	Marks Obtained	Remarks
1	10		
2	10		
3	10		
4	10		
5	10		
Total	50		

Q. 1 [10 marks] Show that if n is a positive integer, then $n^2 \equiv 0$ or 1 (**mod 3**)

Let

$n \equiv 0$ or 1 or $2 \pmod 3$

i.e

$n = 3k$	or $n = 3k+1$	or $n = 3k+2$
$\therefore n^2 = 9k^2$	$n^2 = 9k^2 + 6k + 1$	$n^2 = 9k^2 + 12k + 4$
$n^2 \equiv 0 \pmod 3$	$n^2 \equiv 0 + 0 + 1 \pmod 3$	$n^2 \equiv 0 + 0 + 1 \pmod 3$

From all 3 cases

$n^2 \equiv 0$ or $1 \pmod 3$.

Proved.

Q. 2: [7 + 3 = 10 marks]

(a) Use the Euclidean algorithm to find the gcd of 10,227 and 33,341.

(b) Then use this value of gcd to find the lcm of 10,227 and 33,341.

$33341 = 3(10227) + 2660$

$10227 = 3(2660) + 2247$

$2660 = 2247 + 413$

$2247 = 5(413) + 182$

$413 = 2(182) + 49$

$182 = 3(49) + 35$

$49 = 1.35 + 14$

$35 = 2.14 + 7$

$14 = 2.7$

$\therefore \ gcd = 7$

$\because \ ab = gcd \times lcm$

$\therefore \ lcm = \dfrac{33341 \times 10227}{7}$

$\boxed{= 48711201}$

Q. 3: [10 marks] Find all solutions to $x \equiv 7 \pmod 9$, $x \equiv 4 \pmod{12}$, using back substitution.

$\because\ x \equiv 7 \pmod 9$

$\Rightarrow\ x = 9u + 7$

② $x \equiv 4 \pmod{12}$ $\Rightarrow$ $9u + 7 \equiv 4 \pmod{12}$

$\Rightarrow\ 9u \equiv -3 \pmod{12}$

$\Rightarrow\ 9u \equiv 9 \pmod{12}$

$\because$ if $ac \equiv bc \pmod{mc} \Rightarrow a \equiv b \pmod m$

$\therefore\ 3u \equiv 3 \pmod 4$

Solving this, we first find inverse 'q', i.e.

$3q \equiv 1 \pmod 4$

gcd (4,3)

$4 = 1 \cdot 3 + 1$

As a linear comb.,

$1 = 4 + (-1) \cdot 3$

$\therefore\ \text{Inv} \equiv q \equiv -1 \equiv 3 \pmod 3$

Mult. both sides by 3,

$3(3u) \equiv 3 \cdot 3 \pmod 4$

$u \equiv 1 \pmod 4$

$\therefore\ u = 4w + 1$

Subst. back, we find,

$x = 9(4w+1) + 7$

$x = 36w + 16$

$\therefore\ \boxed{x \equiv 16 \pmod{36}}$ ANS.

Q. 4: [10 marks] The modulus for an RSA public key cryptosystem is 77. The public key of a user "Ed" of the system is 43. Decrypt the following message: 11 48 37 (Consider groups of two integers at a time only)

$\because\ n = 7 \times 11 = 77 = pq$

$\therefore\ \phi(n) = (p-1)(q-1) = 6 \times 10 = 60$

Let $e = 43,\ d = ?$

$\therefore\ 43d \equiv 1 \mod 60$

$\because\ 60 = 1 \cdot 43 + 17$
$43 = 2 \cdot 17 + 9$
$17 = 1 \cdot 9 + 8$
$9 = 1 \cdot 8 + 1$

$\therefore\ \gcd = 1$

$1 = 9 - 8$
$= -17 + 2 \cdot 9$
$= 2 \cdot 43 - 5 \cdot 17$
$= -5 \cdot 60 + 7 \cdot 43$

$\therefore\ \text{Inv} \equiv d = 7.$

Now for decryption,

$M_1 = C_1^{d} \mod n = 11^7 \mod 77$
$= 11 = K$

$M_2 = 48^7 \mod 77$
$= 27$

$M_3 = 37^7 \mod 77$
$= 16$

$\therefore$ Original Message is 11 27 16

Q. 5: [6 + 4 = 10 marks] (a) Let S be the set of all strings of English letters. Determine whether these relations are reflexive, irreflexive, symmetric, asymmetric, antisymmetric, and/or transitive.

(i) R1 = $\{(a, b) \mid a$ and b have no letters in common$\}$
(ii) R2 = $\{(a, b) \mid a$ is longer than $b\}$

Property	R1	R2
Reflexive	No	No
Irreflexive	Yes	Yes
Symmetric	Yes	No
Asymmetric	No	Yes
Antisymmetric	No	Yes/No
Transitive	No	Yes

(b) Find the (i) reflexive closure of R1, and (ii) transitive closure of R2.

(i) Reflexive Closure (R1)

= { (a, b) | a = b OR 'a' & 'b' have no letters in common }

(ii) Trans. Closure (R2) = R2.