CS 2214-B
Assignment 5

Student Name : Ashna Mittal
Student ID : 251206758

Problem 1 :-

e : Integer
d : modular multiplicative inverse of e mod m

To prove: for an integer x, $x^{ed} \equiv x \bmod m$
Theorem: RSA Theorem
Since, d is the modular multiplicative inverse of e mod m for some positive integer m, we get — $ed \equiv 1 \bmod m$
Let, k be an integer such that :
$ed * k = k \bmod m$
Considering x^{ed},
$x^{ed} = (x^k)^{ed}$
Here, $(x^k)^{ed}$ is congruent to $x^k \bmod m$ since we showed $ed * k$ is congruent to $k \bmod m$.
Hence, $x^{ed} \equiv (x^k)^{ed} \equiv x^k \bmod m$
Therefore, for any integer x, $x^{ed} \equiv x^k \bmod m$ for some positive integer k which is an arbitary term and can be any positive integer co-prime to m.

Problem 2 :-

Using well ordering principle,
Let a, b, g be positive integers such that $g = gcd(a, b)$. There exists s, t such that $g = sa + tb$.

Considering the set of all (+) Integral linear combinations of a and b,

$S = \{ma + nb \cup m, n \in Z \wedge ma + nb > 0\}$;

By well ordering principle, there exists a smallest element in Set and is denoted by $c = sa + tb$ for s, t integers.

Since, $c = gcd(a, b)$, ~~have~~ has to be shown by ① c divides both a and b; ② any common divisor of a and b also divides c.

① For Contradiction, assuming, c doesn't divide ~~a~~ ~~b~~ one of the two numbers, then assuming that is 'a', we get $a = cq + r$ from some q and $0 < r < c$.

Substituting: $a = (sa + tb)q + r$.

$\Rightarrow r = a(1 - sq) - btq$.

Since r is (+) and less than c, it $\in S$. This contracts our assumption and so similarily c divides b also.

② Let d be the common divisor of a and b. Since c is a linear combination of a & b, d also must divide c. Hence, $c = gcd(a, b)$. This can be expressed as $sa + tb$ for some integers s and t. $s = s'/c$, $t = t'/c$ such that $sa' + tb' = c$.

$\Rightarrow sa + tb = (s'/c)a + (t'/c)b = (s'a + t'b)/c = c/c = 1$

Hence, the theorem is proved.

Problem 3:-

Mathematical Induction: Prove P(n) is true for all natural numbers(n) that are greater than some natural no. n_0.
Base Case :- Show $P(n_0)$ is true directly.
Inductive Case :- Show $P(k) \rightarrow P(k+1)$ is true for $k \in N, k \geq n_0$
IF both cases are true, then by MI, P(n) is true $\forall n \in N$ and greater than or equal to n_0.

To prove: $\overline{(A_1 \cup A_2 \ldots \cup A_n)} = \bar{A}_1 \cap \bar{A}_2 \ldots \cap \bar{A}_n$ for (+) n

Base Case :- For $n=1$, $\overline{(A_1)} = \bar{A}_1$

Inductive Case: Suppose for some positive integer k, the statement $\overline{(A_1 \cup A_2 \cup \ldots \cup A_k)} = \bar{A}_1 \cap \bar{A}_2 \ldots \cap \bar{A}_k$ holds true. To show: $\overline{(A_1 \cup A_2 \ldots \cup A_k \cup A_{k+1})} = \bar{A}_1 \cap \bar{A}_2 \cap \ldots \bar{A}_k \cap \bar{A}_{k+1}$.

Applying De Morgan's law,

$\overline{(A_1 \cup A_2 \cup A_3 \ldots \cup A_k \cup A_{k+1})} = \overline{(A_1 \cup A_2 \ldots \cup A_k)} \cap \bar{A}_{k+1}$ (★)

As per the Inductive hypothesis, we know:

$\Rightarrow \overline{(A_1 \cup A_2 \cup A_3 \ldots \cup A_k)} = \bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \ldots \cap \bar{A}_k$

Substituting the above equation in (★),

$\Rightarrow \overline{(A_1 \cup A_2 \ldots \cup A_k \cup A_{k+1})} = (\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_k) \cap \bar{A}_{k+1}$

Using intersection over Union Distributive property,

$(\bar{A}_1 \cap \bar{A}_2 \cap \ldots \bar{A}_k) \cap \bar{A}_{k+1} = \bar{A}_1 \cap \bar{A}_2 \cap \ldots \bar{A}_k \cap \overline{(A_{k+1})}$

Hence, we get:

$\overline{(A_1 \cup A_2 \cup \ldots A_k \cup A_{k+1})} = \bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_k \cap \bar{A}_{k+1}$

Thus, By mathematical induction, the statement $\overline{(A_1 \cup A_2 \cup \ldots \cup A_n)} = (\bar{A}_1 \cap \bar{A}_2 \ldots \cap \bar{A}_n)$ holds true for any positive integer n.

Problem 4 :-

Strong Induction makes a stronger hypothesis than mathematical induction.

To prove: $A_n < 2^n$ for all (+) Integers n.

- Base Cases :-

$n = 1$, Given $A_1 = 1$

$A_1 = 2^1 = 2$

So, $A_1 = 1 < 2$; $A_1 < 2^1$

The result holds for $n = 1$

$n = 2$, Given $A_2 = 1$

$A_2 = 2^2 = 4$

So, $A_2 = 1 < 4$; $A_2 < 2^2$

The result holds for $n = 2$

$n = 3$, Given $A_3 = 1$

$A_3 = 2^3 = 8$

So, $A_3 = 1 < 8$; $A_3 < 2^3$

The result holds for $n = 3$.

- Inductive Cases :-

Suppose the result holds for $n = 1, 2 \ldots k$ so, $A_k < 2^k$ for $n \leq k$. To show that $A_{(k+1)} < 2^{k+1}$ when $k \geq 3$, $A_k < 2^k$, $A_{(k-1)} < 2^{k-1}$ and $A_{(k-2)} < 2^{k-2}$ hold true.

By recursive definition of the sequence,

$A_{k+1} = A_k + A_{k-1} + A_{k-2}$.

Substituting the inductive hypothesis, we get, $A_{k+1} < 2^k + 2^{(k-1)} + 2^{(k-2)}$

Hence, we have, $A_k < 2^k$, $A_{(k-1)} < 2^{(k-1)}$ and $A_{(k-2)} < 2^{(k-2)}$.

Factoring out $2^{(k-2)}$ from RHS, we get:

$A^{(k+1)} < 2^{(k-2)} \times (4+2+1)$

$A^{(k+1)} < 2^{(k-2)} \times 7$

Since, $k \geq 3$, we have $2^{(k-2)} > 4$. Hence,

$A_{(k+1)} < 4 \times 7$

$A_{(k+1)} < 28$

Also, $2^{(k+1)} = 2 \times 2^k > 2 \times 2^{(k-2)}$

$= 8 \times 2^{(k-2)} > 28$

Hence, $A_{k+1} < 2^{k+1}$ is true.

Alternatively, $A_{k+1} = A_{(k+1)-3} + A_{(k+1)-2} + A_{(k+1)-1}$

(as per the given condition).

$A_{k+1} = A_{k-2} + A_{k-1} + A_k$.

But, the result holds for $n \leq k$.

$\therefore A_{k-2} < 2^{k-2}$, $A_{k-1} < 2^{k-1}$, $A_k < 2^k$.

$\Rightarrow A_{k-2} + A_{k-1} + A_k < 2^{(k-2)} + 2^{(k-1)} + 2^k$.

i.e., $A_{k+1} = a_{k-2} + A_{k-1} + A_k < 2^{k-2} + 2^{k-1} + 2^k$

$\Rightarrow A_{k+1} < 2^{k-2} + 2^{k-1} + 2^k$

$\Rightarrow A_{(k+1)} < 2^k \left(\frac{1}{2^2} + \frac{1}{2} + 1\right) \Rightarrow A_{(k+1)} < 2^k \left(\frac{7}{4}\right)$ — ①

Since $\frac{7}{4} < 2 \Rightarrow 2^k \left(\frac{7}{4}\right) < 2^{(k+1)}$ — ②

Using ① and ②, $A_{(k+1)} < 2^k \left(\frac{7}{4}\right) < 2^{k+1}$

Hence, $A_{k+1} < 2^{k+1}$ is true. The result holds for $n = k+1$.

By the principle of strong induction, $A_n < 2^n$ $\forall n \in \mathbb{N}$.

Problem 5 :-

(a) Number of excess mushroom : 2000 − 200
= 1800

Number of purchases of the dish = 160
As per the generalized pigeonhole theorem :, if N objects (1800 excess mushrooms) are to be placed into k boxes (160 feature purchases), then there is atleast one box containing $\lceil N/k \rceil$ or more objects.
As per, the above formula, to ensure that all excess mushroom is used, Ricardo will have to use $\lceil 1800/160 \rceil = \lceil 11.25 \rceil$
= 12 mushrooms in each serving of the featured dish.

(b) Let Ivana run a total of N kilometres per week. It is given that Ivana has to run atleast 250 kilometres as per her training plan and so N = 250.
Since, there are 7 days a week, k = 7.
Let $\lceil \frac{N}{k} \rceil$ be the kilometres needed to run by Ivana.
$\lceil \frac{N}{k} \rceil = \lceil \frac{250}{7} \rceil = \lceil 35.71 \rceil = 36$. However, she runs $35 \times 7 = 245$ kilometres if she runs 35 kilometres every day of the week.
Hence, it is necessary that she runs more

35 kilometres ~~per~~ one day of the week to meeting her training ~~pe~~ plans.
Alternatively, using the pigeonhole principle, let us assume that Ivana need not run more than 35 kilometres a day of a week. To achieve her training goal, she must run atleast $\lceil 250/35 \rceil = 8$ days $\{\lceil 7.14 \rceil\}$ However, she has only 7 days to acheive her goal. Therefore she must run $\lceil 250/7 \rceil = \lceil 35.717 \rceil = 36$ ~~hours~~ kilometres a day. But she runs $35 \times 7 = 245$ kilometres a week which leaves her goal unachieved. As per these calculations, our assumption is contradicted and hence if she keeps on running 35 kilometres a day, she will have to run more than 35 kilometres on one day of the week to meet her goal of running 250 kilometres a week.

(c) Here, $\mathbb{Z}$ represents the set of all integers. To prove that $\mathbb{Z}$ is an infinite set, ~~it~~ it must be shown that there does not exist a natural number 'n' such that a bijection from $\mathbb{Z}$ to $\{1, 2, 3, \ldots n\}$ exists.
By proof by contradiction, let us assume that there exists a bijection between $\mathbb{Z}$ and $\{1, 2, \ldots n\}$. Then, every element of $\mathbb{Z}$ has a unique mapping in the set $\{1, 2 \ldots n\}$ However, since $\mathbb{Z}$ is infinite, it is not possible map every element of $\mathbb{Z}$ with $\{1, 2 \ldots n\}$ and vice-versa, since the $\{1, 2 \ldots n\}$ set has only 'n' number of elements.

Also, since the bijection f is one-to-one, $f(m) \neq f(n)$ for any distinct integers m & n. Let $S = \{f(2), f(-2) \ldots f(k), f(-k)\}$ where $f(1) = a$, $f(-1) = b$; then k is the maximum value such that $f(k) <= n/2$ and k is positive. By the pigeonhole principle, two distinct elements in S that map to the same element in $\{1, 2, \ldots n\}$ under f. Suppose ~~$f(i) = f(j)$~~ $f(i) = f(j)$, $1 \leq i < j \leq k$, then $f(j - i) = f(j) - f(i) = 0$. This is a contradiction since $0 \notin \{1, 2 \ldots n\}$. Hence, our assumption is false and there does not exist a natural number 'n' such that a bijection from $\mathbb{Z}$ to $\{1, 2 \ldots n\}$ exists.

Hence, $\mathbb{Z}$ is an infinite set.

Problem 6 :-

(a) Adjacency Matrix using Lexicographical ordering :

G_1 where $V_1 = \{a, b, c, d, e\}$.

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

→ Figure 1 (G_1)

Adjacency Matrix using Lexicographial ordering:

G_2 where $V_2 = \{u, v, x, y, z\}$

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

→ Figure 2 (G_2)

(b) Two graphs $G_1 = (V_1, E_1)$ and $G(V_2, E_2)$ are isomorphic if there exists a bijection function f from V_1 to V_2 with a property that two vertices $v_1, v_1 \in V_1$ are adjacent in G_1 if and only if $f(v_1)$ and $f(v_2)$ are adjacent in G_2. Then the bijective function f is called ~~is~~ an isomorphism.
Thus, we must have $|V_1| = |V_2|$ and $|E_1| = |E_2|$ alongside maintaining adjacencies.

To show $f: G_1 \rightarrow G_2$ is a one-one onto mapping.

$f(a) = x$
$f(b) = u$
$f(c) = z$
$f(d) = v$
$f(e) = y$

Degree of G_1 :
$\deg(a) = 2$; $\deg(b) = 3$; $\deg(c) = 3$;
$\deg(d) = 2$; $\deg(e) = 2$;

Degree of G_2 :
$\deg(x) = 2$; $\deg(y) = 2$; $\deg(z) = 3$
$\deg(u) = 3$; $\deg(v) = 2$;

From above, we can see that both the graphs have three vertices of degree 2 and two vertices of degree 3. The bijection works:

1. 'a' is connected to 'b' and 'c' in G_1 and $f(a) = x$ is connected to $f(b) = u$ and $f(c) = z$ in G_2.
2. 'b' is connected to 'a', 'c' and 'e' in G_1 and 'u' is connected to 'x', 'z', 'y' in G_2
3. 'c' is connected to 'a', 'b', 'd' in G_1 and 'z' is connected to 'x', 'u', 'v' in G_2.
4. 'd' is connected to 'c', 'e' in G_1 and 'v' is connected to 'z', 'y' in G_2.
5. 'e' is connected to 'b' and 'd' in G_1 and y is connected to 'u' and 'v' in G_2.

Hence, the graphs are bijective and so isomorphic and here isomorphism can be defined as :
$f(a) = 'x'$, $f(b) = 'u'$, $f(c) = 'z'$, $f(d) = 'v'$ and $f(e) = y$.