Name: Subhojit Ghimire

Scholar Id.: 1912160

Subject Name: Discrete Structures

Subject Code: CS 202

Date: 14th October, 2020

MID SEM EXAMINATION: UG III$^{RD}$ SEM

BRANCH: CSE

---

Q.1.

a) Ans) Given, a and b are integers.

m is positive integer.

To prove, $a \equiv b \mod m$ if and only if $a \mod m = b \mod m$.

Assuming, $a \equiv b \pmod m$ — (i)

Then, $m \mid (a-b)$, $\therefore$ there exists $k \in \mathbb{Z}$ such that $a-b = mk$ — (ii)

Let, $a \mod m = r$ — (iii)

According to division algorithm, there exists $q \in \mathbb{Z}$

Such that $a = mq + r$. — (iv)

where, $0 \leq r < m$

Taking (ii) and (iv), we get,

$$mq + r - b = mk$$

Or, $mq - mk + r = b$

$\therefore m(q-k) + r = b.$

Here, r is remainder when b is divided by m.

$\therefore b \mod m = r = a \mod m.$

$\therefore$ If $a \equiv b \pmod m$, then $a \mod m = b \mod m$.

Again.

Assuming. $a \bmod m = b \bmod m$

Let, $r = a \bmod m = b \bmod m$.

Then,

According to division algorithm,

there exists $q_1, q_2 \in \mathbb{Z}$ such that,

$$a = mq_1 + r$$
$$b = mq_2 + r$$

where, $0 \leq r < m$.

Then,

$$a - b = mq_1 + r - (mq_2 + r)$$

or, $a - b = mq_1 + r - mq_2 - r$

or, $a - b = mq_1 - mq_2$

$\therefore$ $a - b = m(q_1 - q_2)$

This shows that $m \mid (a-b)$.

$\therefore$ $a \equiv b \pmod m$

$\therefore$ If $a \bmod m = b \bmod m$, then $a \equiv b \pmod m$

From these two conclusions, we can say that,

$$a \equiv b \pmod m \Leftrightarrow a \bmod m = b \bmod m$$

i.e., $a \equiv b \pmod m$ if and only if $a \bmod m = b \bmod m$.

Hence, proved.

Q.1

b) Ans) Given, $a, b, c$ are integers.

$a \neq 0$.

To prove, if $a|b$ and $b|c$, then $a|c$.

Since $a|b$, there exists $K_1$ such that,

$$a = bK_1 \qquad -(i)$$

Also, $b|c$, so there exists $k_2$ such that,

$$b = cK_2 \qquad -(ii)$$

from (i) and (ii),

$$a = (cK_2)K_1$$

or, $a = cK_1K_2$

$\therefore a = cK_3$ (Let $K_3 = K_1K_2$)

$\therefore a | c$

$\therefore$ By the definition of divides, $a|c$.

Hence, proved.

Q.2

(a) Ans) Let, $S(x)$ : $x$ can keep a secret

No one can keep a secret.

$$\forall x\,(\neg S(x))$$

Negation of this proposition can be expressed as,

$$\neg(\forall x\, \neg(S(x)))$$
$$\equiv \exists x(\neg(\neg(S(x))))$$
$$\equiv \exists x\, S(x)$$

i.e, There exists someone who can keep a secret.

Q.2.

(b) Ans) Let, $A(x)$ : $x$ has good attitude

There is someone in the class who does not have a good attitude.

$$\exists x\,(\neg A(x))$$

Negation of this proposition can be expressed as,

$$\neg(\exists x(\neg A(x)))$$
$$\equiv \forall x\,(\neg(\neg A(x)))$$
$$\equiv \forall x\, A(x)$$

i.e, Everyone in the class has a good attitude.

Q.3

Ans) Given, $ax+by=c$

or, $5x+20y=200$.

Here, $d = \gcd(5,20) = \gcd(5,0)$

This means, we have infinitely many solutions.

$a_1 x + b_1 y = c_1$

Or, $1x + 4y = 40$

Using Extended Euclidean Algorithm.

| q | $r_1$ | $r_2$ | r | $s_1$ | $s_2$ | s | $t_1$ | $t_2$ | t |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 4 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 4 | 4 | 1 | 0 | 0 | 1 | -4 | 1 | 0 | 1 |
| | 1 | 0 | | 1 | -4 | | 0 | -4 | |

$\therefore$ $s = 1$

$t = 0$

i.e., $x_0 = sc_1 = 1 \times 40 = 40$

$y_0 = 0 \times 40 = 0$.

And, $x = x_0 + Kb$

$y = y_0 - Ka$

where, K is an arbitrary constant.

Therefore,

$x = 40 + 4K$

and $y = -K$

are the possible combinations.

Q.40

Ans) ~~Taking letter~~

Since private and public keys are not used, we will be comparing the most commonly used letters in the cypher text.

Analysing the cypher text corresponding to integers such that $A \to 0$
$B \to 1$
$\vdots$
$Z \to 25$

And with few hit and trials, we can see that the letters have +8 shift in Caesar cypher.

~~Thef~~ Therefore, translating to the corresponding plain text we get,

~~Everyone~~
EVERYONE KNOWS THAT PROOFS ARE IMPORTANT THROUGHOUT MATHEMATICS BUT MANY PEOPLE FIND IT SURPRISING HOW IMPORTANT PROOFS ARE IN COMPUTER SCIENCE

Q. 5.

Ans: Given,

$p = 67$
$q = 79$

~~priv~~
public key $= 179 = e$

To find, private key (d)

$n = p \times q = 67 \times 79 = 5293$

$\phi(n) = 66 \times 78 = 5148$

We know,

$d \equiv e^{-1} \bmod \phi(n)$

or, $d \equiv (179)^{-1} \bmod 5148$

or, $d \equiv \frac{1}{179} \bmod 5148.$

i.e., $\gcd(5148, 179) = 1$

Using Multiplicative Inverse of Euclidean Algorithm,

| q | $r_1$ | $r_2$ | r | $t_1$ | $t_2$ | t |
|---|---|---|---|---|---|---|
| 28 | 5148 | 179 | ~~580~~ 136 | 0 | 1 | -28 |
| 1 | ~~580~~ 179 | 136 ~~580~~ | 43 ~~1179~~ | 1 | -28 | 29 |
| 3 | 136 ~~580~~ | 43 ~~1179~~ | 7 ~~43~~ | -28 | 29 | -115 ~~-138~~ |
| 6 | 43 ~~1179~~ | 7 ~~143~~ | 1 | 29 | -115 ~~-138~~ | 719 ~~1141~~ |
| ~~6~~ | ~~143~~ | ~~7~~ | ~~1~~ | ~~-138~~ | ~~1141~~ | ~~-881~~ |
| 7 | 7 | 1 | 0 | 719 ~~1141~~ -115 | 719 ~~-881~~ | -5148 ~~6308~~ |
| | 1 | 0 | | ~~-881~~ 719 | ~~6308~~ -5148 | |

$\underbrace{719}$

719

$\therefore 719 \equiv (179)^{-1} \bmod 5148$

$\therefore d = 719$ is the private key