COL202: Discrete Mathematical Structures

Name: T Pratham
Entry no.: 2020EE10559
Group: 2

Tutorial Sheet 5

1.

a) <u>To show:</u> For any $n, m \in \mathbb{Z}$, $\exists\ x \in \mathbb{Z}$ s.t. $x \equiv m \pmod a$ and $x \equiv n \pmod b$ for co-prime a, b.

i.e. we want to show existence of an integer x which simultaneously satisfies: $x = q_1 a + m$ and $x = q_2 b + n$ $(q_1, q_2 \in \mathbb{Z})$

<u>Proof:</u>

We know $\gcd(a,b) = 1 = \text{spc}(a,b)$

$\Rightarrow sa + tb = 1 \quad (s, t \in \mathbb{Z})$

$\Rightarrow sa = 1 - tb$ and $\Rightarrow tb = 1 - sa$

$\Rightarrow san = n - tbn$ and $\Rightarrow tbm = m - sam$

$\Rightarrow san + tbm = n - tb(n-m)$ — ⓐ and $\Rightarrow san + tbm = m - sa(m-n)$ — ⓑ

Choosing $x = san + tbm$

From ⓐ: $x \pmod b \equiv n \pmod b$ {i.e. $x = q_1 b + n$}

From ⓑ: $x \pmod a \equiv m \pmod a$ {i.e. $x = q_2 a + m$}

Hence, for any m, n, there always exists an x.

b) <u>To prove:</u> $x \equiv 0 \pmod a \wedge x \equiv 0 \pmod b \Rightarrow x \equiv 0 \pmod{ab}$

<u>Proof:</u>

$x \equiv 0 \pmod a \quad \wedge \quad x \equiv 0 \pmod b$

$\Rightarrow x = q_1 a$ and $x = q_2 b$

$\therefore q_1 a = q_2 b$

Now, we know $\gcd(a,b) = 1$

and since $q_1 a = q_2 b \Rightarrow a \mid q_2 b$

$\therefore\ a \mid q_2 \qquad (\gcd(a,b) = 1)$

$\therefore\ q_2 = a q_3$

Hence, $x = q_2 b = q_3 ab$

$\therefore\ ab \mid x \qquad$ i.e. $\quad x \equiv 0 \pmod{ab}$

Hence proved.

c) To prove: $x \equiv x' \pmod a \wedge x \equiv x' \pmod b \Rightarrow x \equiv x' \pmod{ab}$

Proof:

$$x \equiv x' \pmod a \Leftrightarrow (x - x') \equiv 0 \pmod a$$
$$x \equiv x' \pmod b \Leftrightarrow (x - x') \equiv 0 \pmod b$$

$$\therefore\ x \equiv x' \pmod a \wedge x \equiv x' \pmod b \Leftrightarrow (x-x') \equiv 0 \pmod a \wedge (x-x') \equiv 0 \pmod b$$

Using part b), replacing x with $(x-x')$, we get:

$$(x-x') \equiv 0 \pmod a \wedge (x-x') \equiv 0 \pmod b \Rightarrow (x-x') \equiv 0 \pmod{ab}$$

$$\Updownarrow$$

$$x \equiv x' \pmod a \wedge x \equiv x' \pmod b \Rightarrow x \equiv x' \pmod{ab}$$

[$\because\ (x-x') \equiv 0 \pmod{ab} \Leftrightarrow x \equiv x' \pmod{ab}$]

Hence proved.

d)

Proof:

Using part a), we have proved that for integers $a > 1$ and $b > 1$ which are co-prime, for all integers m and n, $\exists$ an integer x which simultaneously satisfies:

$$x \equiv m \pmod{a} \quad \text{--- ①}$$
$$x \equiv n \pmod{b} \quad \text{--- ②}$$

We showed the existence of one such x given as
$x = san + tbm$; with $sa + tb = 1 = gcd(a, b)$

Hence, existence is proved true.

Now, let x' be another integer which satisfies both eqⁿ ① and ② simultaneously.

i.e.

$$x' \equiv m \pmod{a} \quad \text{--- ③}$$

and

$$x' \equiv n \pmod{b} \quad \text{--- ④}$$

Using symmetry and transitivity properties of congruence:

from ① and ③: $x \equiv x' \pmod{a}$

from ② and ④: $x \equiv x' \pmod{b}$

Therefore, using part c), we can say that $x \equiv x' \pmod{ab}$

Hence, any integer which simultaneously satisfies equation ① and ② is unique upto congruence modulo ab.

Hence, uniqueness of x is proved.

Thus, the statement of Chinese Remainder Theorem is proved true.