Sindhuja Yerramalla
Syrrmlla@memphis.edu
U00839259

COMP-2700
HomeWork 4

Problem 1

By the definition of Extended Euclidean Algorithm

$$\gcd(A,B) = Au + Bv.$$

$$\Rightarrow \gcd(192,21) = 192u + 21v \quad \text{---(*)}$$

and $192 = 21(9) + 3$ — (1)

$21 = 3(7) + 0$

$\Rightarrow \gcd(192,21) = 3$

and (1) $\Rightarrow$ $192 - 2(9) = 3$

$192(1) + 2(-9) = 3$

$\therefore$ Bezout coefficients of 192, 21 are: $(1, -9)$.

Problem 2.

Given $\gcd(a,b) = d$, then there exists u, v, where.

$$au + bv = d$$

$$\Rightarrow \frac{au}{d} + \frac{bv}{d} = 1 \quad \text{[by the def of extended Euclidean Algorithm]}$$

$$\left(\frac{a}{d}\right)u + \left(\frac{b}{d}\right)v = 1.$$

$$\Rightarrow \boxed{\gcd(a/d, b/d) = 1.}$$

Problem 3:

Let $d = \gcd(a,b) \Rightarrow d|a$ & $d|b$.

Let p, q be the quotients such that $a = pd$ & $b = qd$

Let $S = \{au + bv \mid u, v \in z\}$ and $T = \{t(a,b) \mid t \in z\}$

Let $D \in S \Rightarrow D = au + bv$ for $u, v \in z$

Now $a = pd$ & $b = qd \Rightarrow D = (pd)u + (qd)v$

$$\Rightarrow D = d(pu + qv) \quad \text{---(1)}$$

Hence 'D' is a multiple of d $[d = \gcd(a,b)]$

Now let $D \in T$

$\Rightarrow D = d \cdot s$ for $s \in z$

$\gcd(a,b) = ap + bq$ for some p, q integers

$\Rightarrow d = ap + bq$.

$D = (ap + bq)s$

$D = aps + bqs = a(ps) + b(qs)$ ---(2)

Hence D is a linear combination of a & b.

from (1) & (2), we can say

$$\{au + bv \mid u, v \in z\} = \{t(a,b) \mid t \in z\} \text{ //}$$

Problem 4 :-

Given $n \neq 0$ & $n \mid ab$ & $(a,n) = 1$

if $\gcd(a,n) = 1$ then we can say a, n are relatively prime, that means they have no common factors other than '1'.

$\gcd(a,n) = 1 \Rightarrow n \nmid a$.

there exists u & v such that

$$nu + av = 1. \quad \text{——(1)}$$

multiplying b on bothsides

$$nbu + abv = b.$$

Now $n \mid nbu$ [$\because$ nbu is multiple of n.]

and $n \mid (ab)v$ [$\because n \mid ab$]

$\Rightarrow n \mid nbu + abv$.

$\Rightarrow n \mid b$ // [from (1)]

$\therefore$ Hence proved that "n divides b".

Problem 5

1) $57^{2022} \bmod 17$.

$57 \equiv 6 \pmod{17}$

57 & 6 leaves same remainder when divided by 17.

$(57)^{2022} \equiv 6^{2022} \pmod{17}$ — (1)

$6^2 \equiv 2 \pmod{17}$

$(6^2)^{1011} \equiv 2^{1011} \pmod{17}$

$6^{2022} \equiv 2^{1011} \pmod{17}$ — (2)

from (1) & (2) ⇒ we get

$(57)^{2022} \equiv 2^{1011} \pmod{17}$ — (3).

$(2^4) \equiv -1 \pmod{17}$

$(2^4)^{252} \equiv (-1)^{252} \pmod{17}$

$2^{1008} \equiv 1 \pmod{17}$

$2^{1008} \times 2^3 \equiv 1 \times 2^3 \pmod{17}$

$2^{1011} \equiv 8 \pmod{17}$ — (4)

from (3) & (4) ⇒ $(57)^{2022} \equiv 8 \pmod{17}$

reminder = 8 //

ii) $(8)^{2020} \mod 15$.

$8^2 \equiv 4 \pmod{15}$

$8^2 \equiv 2^2 \pmod{15}$

$(8^2)^{1010} \equiv (2^2)^{1010} \pmod{15}$

$(8)^{2020} \equiv (2)^{2020} \pmod{15}$ —(1)

$2^4 \equiv 1 \pmod{15}$

$(2^4)^{505} \equiv (1)^{505} \pmod{15}$

$2^{2020} \equiv 1 \pmod{15}$ —(2)

from (1) & (2) $\Rightarrow (8)^{2020} \equiv (1) \pmod{15}$

remainder is 1 //

iii) $(3^{256} - 256^3) \mod 21$

$3^{256} \mod 21 \Rightarrow 3^3 \not\equiv 6 \pmod{21}$

$\Rightarrow 3^4 \equiv -3 \pmod{21}$ $(3^3)^{85} \not\equiv 6^{85} \pmod{21}$

—(*)

$\Rightarrow (3^4)^{64} \equiv (-3)^{64} \pmod{21}$

$3^{256} \equiv 3^{64} \pmod{21}$ — (1)

$(*) \Rightarrow (3^4)^{16} \equiv (-3)^{16} \pmod{21}$

$\Rightarrow 3^{64} \equiv 3^{16} \pmod{21}$ — (2)

from (1) & (2)

$$3^{256} \equiv 3^{16} \pmod{21} \quad \text{— (3)}$$

(*) $\Rightarrow (3^4)^4 \equiv (-3)^4 \pmod{21}$

$$3^{16} \equiv 3^4 \pmod{21} \quad \text{— (4)}$$

from (3) & (4)

$$3^{256} \equiv 3^4 \pmod{21} \quad \text{— (5)}$$

from (*) & (5)

$$3^{256} \equiv -3 \pmod{21} \quad \text{— (A)}$$

$(256)^3 \bmod 21 \Rightarrow 256 \equiv 4 \pmod{21}$

$$(256)^3 \equiv 4^3 \pmod{21}$$

$$4^3 \equiv 1 \pmod{21}$$

$$\therefore (256)^3 \equiv 1 \pmod{21} \quad \text{— (B)}$$

(A) & (B)

$$3^{256} \equiv -3 \pmod{21}$$
$$256^3 \equiv 1 \pmod{21}$$

WKT $a \equiv b \pmod{n}$,
$c \equiv d \pmod{n}$ then

$$(a-c) \equiv (b-d) \pmod{n}$$

$\therefore (3^{256} - 256^3) \equiv -3-1 \pmod{21}$

$\Rightarrow (3^{256} - 256^3) \equiv -4 \pmod{21}$

-4 rem 21 is 17.

$\Rightarrow (3^{256} - 256^3)$ rem 21 is 17 //

Problem 6

We proved in the class that, If P is a prime. and $a, b \in z$ and $P|ab$ then $P|a$ (or) $P|b$ —(1)

if we consider an integer m, where.

$P|m$ and
$q|m$.

$\Rightarrow Pq|m^2 \Rightarrow Pq|m * m$.

given P,q are different primes $Pq|m$ or $Pq|m$

$\Rightarrow Pq|m$. — (2)

given $n \equiv 1 \pmod{P}$ & $n \equiv 1 \pmod{q}$

[$a \equiv b \pmod{n}$ if and only if $n|(a-b)$] —(3)

$\Rightarrow P|(n-1)$ &.

$\Rightarrow q|(n-1)$

from (2) $\Rightarrow$ $\boxed{Pq|(n-1)}$

from (3)
we can write.
$\boxed{n \equiv 1 \pmod{Pq}}$ //