Assignment-1

Ankit Goyal
Roll No - 17103011
Group - G1

1. Let n be a non-negative integer then gcd (3n+1, 2n+1)

(a) $3n+1 = (2n+1)*1 + n$

$\therefore$ gcd (3n+1, 2n+1) = gcd (2n+1, n)

(b) $2n+1 = n*2 + 1$

$\therefore$ gcd (2n+1, n) = gcd (n, 1)

(c) $n = 1*n + 0$

$\therefore$ gcd (n, 1) = gcd (1, 0)

as b = 0 ⇒ gcd (1, 0) = 1

$\therefore$ gcd (3n+1, 2n+1) = 1

gcd (301, 201)

here n = 100 ⇒ $\therefore$ gcd (3n+1, 2n+1) = 1

⇒ gcd (301, 201) = 1

gcd (121, 81) ⇒ gcd (121, 81) = 1

2. we need to prove that remainder of an integer divisible by 5 is same as the remainder of division of the rightmost digit by 5.

lets take a number abcd

where abcd is a 4 digit number with a, b, c, d digits.

we have to prove that

abcd % 5 = d % 5

we can write it as ⇒

abc * 10 + d

⇒ (abc * 10 + d) % 5

$\Rightarrow (abc * 10 \% 5 + d \% 5) \% 5$

$\Rightarrow (0 + d \% 5) \% 5 \Rightarrow d \% 5$

$\therefore \boxed{abcd \% 5 = d \% 5}$

3. we need to prove that remainder of an integer divisible by 4 is same as the remainder of division of two rightmost digit by 4.

let abcd be a 4 digit number with a, b, c, d as digits. we can write it as

$\Rightarrow abcd = abcd * 100 + cd$

in general form

$ab\_\_cd = ab\_\_ * 10^{n-2} + cd$

we need to prove

$ab\_\_cd \% 4 = cd \% 4$

$\Rightarrow (ab\_\_cd) \% 4 = (ab\_\_ * 100 + cd) \% 4$

$= (ab\_\_ * 100 \% 4 + cd \% 4) \% 4$

$= (0 + cd \% 4) \% 4$

$= cd \% 4$

$\therefore \boxed{ab\_\_cd \% 4 = cd \% 4}$

4. We have to prove $\Rightarrow$

$abcd \% 9 = (a+b+c+d) \% 9$

$\Rightarrow abcd \% 9$

$\Rightarrow (abc * 10 + d) \% 9$

$\Rightarrow (abc * 10 \% 9 + d \% 9) \% 9$

$\Rightarrow ((ab * 100 + 10c) \% 9 + d \% 9) \% 9$

$\Rightarrow ((ab * 100 \% 9 + 10c \% 9) \% 9 + d \% 9) \% 9$

$\Rightarrow (((a*1000 + b*100)\%9 + 10c\%9)\%9 + d\%9)\%9$

$\Rightarrow (((a*1000\%9 + b*100\%9)\%9 + c\%9)\%9 + d\%9)\%9$

$+ 9c\%9$

$\Rightarrow (((a*1000\%9 + 99*b\%9 + b\%9)\%9 + c\%9)\%9 + d\%9)\%9$

$\Rightarrow (((a*999\%9 + a\%9 + b\%9)\%9 + c\%9)\%9 + d\%9)\%9$

$\Rightarrow (((a\%9 + b\%9)\%9 + c\%9)\%9 + d\%9)\%9$

$\Rightarrow ((a+b)\%9 + c\%9)\%9 + d\%9)\%9$

$\Rightarrow ((a+b+c)\%9 + d\%9)\%9$

$\Rightarrow ((a+b+c+d)\%9)\%9$

$\Rightarrow (a+b+c+d)\%9$

$$\Rightarrow \boxed{abcd\%9 = (a+b+c+d)\%9}$$

5. The multiplicative inverse pairs in mod c is i.e. the modular inverse of A mod C is the B value that makes (A*B) mod C = 1. We can solve this with the help of extended euclidian algorithm

a mod c

(a*b) mod c = 1 mod c

b exist only when gcd(a,c) = 1

1 → gcd(1, 20) = 1

applying extended euclidian algorithm

20 = 1*20 + 0

⇒ 0 = 20 − 20*1

Hence pair is (1,1)

- $2 \rightarrow gcd(2,20) = 2$

multiplicative inverse modulus 20 doesn't exist.

- $3 \rightarrow gcd(3,20) = 1$

$20 = 3 \times 6 + 2$

$3 = 2 \times 1 + 1$

$\Rightarrow$ $1 = 3 - 2 \times 1$

$1 = 3 - (20 - 3 \times 6) \times 1$

$1 = 3 - (20 - 3 \times 6)$

$1 = 3 \times 1 - 20 + 3 \times 6$

$1 = 3 \times 7 - 20 + 1$

pair is (3, 7)

- $4 \rightarrow gcd(4,20) \Rightarrow 4$

multiplicative inverse doesn't exist.

- $5 \rightarrow gcd(5,20) \Rightarrow 5$

MI not exist.

- $6 \rightarrow gcd(6,20) \Rightarrow 2$

MI not exist

- $7 \rightarrow gcd(7,20) \Rightarrow 1$

already taken

- $8 \rightarrow gcd(8,20) \Rightarrow 4$

MI not exist

- $9 \rightarrow gcd(9,20) = 1$

$20 = 9 \times 2 + 2$ $\quad \Rightarrow 2 = 20 - 9 \times 2$

$9 = 2 \times 4 + 1$ $\quad \Rightarrow 1 = 9 - 2 \times 4$

$\Rightarrow 1 = 9 - 2 \times 4$

$= 9 - (20 - 9 \times 2) \times 4$

$= 9 - (20 \times 4 - 9 \times 8)$

$1 = 9*1 - 20*4 + 9*8$

$1 = 9*9 - 20*4$

pair is $(9,9)$

- $10 \Rightarrow \gcd(10,20) = 10$ X
- $11 \Rightarrow \gcd(11,20) = 1$

$20 = 11*1 + 9$ $\qquad 9 = 20 - 11*1$

$11 = 9*1 + 2$ $\qquad 2 = 11 - 9*1$

$9 = 2*4 + 1$ $\qquad 1 = 9 - 2(4)$

$$
\begin{aligned}
1 &= 9 - 2(4) \\
&= 9 - (11 - 9(1))4 \\
&= 9 - (11*4 - 9*4) \\
&= 9*5 - 11*4 \\
&= (20 - 11)5 - 11*4 \\
&= 20*5 - 11*5 - 11*4 \\
1 &= 20*5 - 11*9
\end{aligned}
$$

pair $\Rightarrow (11, -9)$

- $12 \Rightarrow \gcd(12,20) \Rightarrow 4$ X
- $13 \Rightarrow \gcd(13,20) = 1$

$\therefore$ $20 = 13*1 + 7$ $\qquad 7 = 20 - 13*1$

$13 = 7*1 + 6$ $\qquad 6 = 13 - 7*1$

$7 = 6*1 + 1$ $\qquad 1 = 7 - 6*1$

$$
\begin{aligned}
\Rightarrow 1 &= 7 - 6*1 \\
&= 7 - (13*1 - 7*1)*1 \\
&= 7 - (13*1) + 7*1 \\
&= 7*2 - 13*1 \\
&= (20 - 13*1)*2 - 13*1 \\
&= (20*2 - 13*2) - 13*1 \\
&= 20*2 - 13*3
\end{aligned}
$$

pair $(13, -3)$

- 17 ⇒ $\gcd(20, 17) = 1$

$20 = 17 \times 1 + 3$

$17 = 3 \times 5 + 2$

$3 = 2 \times 1 + 1.$

$1 = 3 - 2 \times 1$

$= 3 - (17 - 3 \times 5) \times 1$

$= 3 \times 6 - 17 \times 1$

$= (20 - 17 \times 1) \times 6 - 17 \times 1$

$1 = 20 \times 6 - 17 \times 7$

$\therefore$ pair is $(17, -7)$

- 19 ⇒ $\gcd(19, 20) = 1$

$20 = 19 \times 1 + 1$

$1 = 20 - 19 \times 1$

$\therefore$ pair is $(19, -1)$.