Abdus Salam
4th Year 1st Semester
ID: 21016 Session: 2020-21
Dept: ICT

1)

I) $-17 \bmod 23$?

We can write, $a \bmod m$

the remainder when a is divided by m.

and ~~we~~ the answer in the range:

$$0 \leq \text{result} < m$$

now, $a \bmod m = (a+m) \bmod m$

$-17 \bmod 23 = (-17+23) \bmod 23$

$= 6 \bmod 23$

Since 6 is already in the range [0, 22],

so, $-17 \bmod 23 = 6$

(Ans)

Abdus Salam
4th Year 1st Semester
ID: IT-21016
Dept: ICT

2) Ans: Multiplicative inverse of -13 upon modulo 23?

The multiplicative inverse of a modulo m is a number x such that $ax \equiv 1 \pmod{m}$.

Since, $-13 \equiv 10 \pmod{23}$, we can find the multiplicative inverse of 10 modulo 23.

Step-1:

-13 as an equivalent positive number modulo 23.

$$-13 \equiv -13 + 23 \pmod{23}.$$

$$-13 \equiv 10 \pmod{23}$$

Step-2:

We can use trial and error the extended Euclidean algorithm and trying small multiples of 10:

$$10x \equiv 1 \pmod{23}$$

When, $x = 1$, $10.1 = 10 \equiv 10 \pmod{23}$.

Abdus Salam
4th year 1st Semester
ID: IT-21016 Session: 2020-21
Dept: ICT

$x=2$, $10.2 = 20 \equiv 20 \pmod{23}$

$x=3$, $10.3 = 30 \equiv 7 \pmod{23}$

$x=4$, $10.4 = 40 \equiv 17 \pmod{23}$

$x=5$, $10.5 = 50 \equiv 4 \pmod{23}$

$x=6$, $10.6 = 60 \equiv 14 \pmod{23}$

$x=7$, $10.7 = 70 \equiv 1 \pmod{23}$

Thus, $x=7$ is the multiplicative inverse of 10 modulo 23.

Step-3:

$10.7 = 70$

$70 \div 23 = 3$ with a remainder 1

$70 \equiv 1 \pmod{23}$

23	70	3
	69	
	1	

The multiplicative inverse of -13 modulo 23 is 7.