Problem-1

1. $14^{37} \bmod 5$

$$= 14 \cdot (14^{18})^2 \bmod 5$$

$$= 14 \cdot ((14^{9})^2)^2 \bmod 5$$

$$= 14 \cdot ((14 \cdot (14^{8}))^2)^2 \bmod 5$$

$$= 14((14 \cdot (14^{4})^2)^2)^2 \bmod 5$$

$$= 14 \cdot ((14 \cdot ((14^{2})^2)^2)^2)^2 \bmod 5$$

$$= 14 \cdot ((14 \cdot ((196)^2)^2)^2)^2 \bmod 5$$

$$= 14 \cdot \left(\left(14 \cdot ((1))^2 \right)^2 \right)^2 \bmod 5$$

$$= 14 \left((14)^2 \right)^2 \bmod 5$$

$$= 14 \left(1 \right)^2 \bmod 5$$

$$= 14 \bmod 5$$

$$= 4$$

2. $\sum_{i=1}^{100} i! \bmod 7$

So, all values of i more tran 6 will yield to 0 as they will all have 7 in it.

$= (1! + 2! + 3! + 4! + 5! + 6!) \bmod 7$

$= (1 + 2 + 6 + 24 + 120 + 720) \bmod 7$

$= 873 \bmod 7$

$= 5$

3. multiplicative inverse of 8 in $\mathbb{Z}_{13}$ or $8 \bmod 13$

Since we have to find multiplicative inverse of it then we are supposed to use Euclid Algorithm and Diophantine equation.

Lets say we are solving

$13x + 8y \equiv 1 \bmod 11$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 2 \cdot 1 + 0$

$5 = 13 - 1 \cdot 8$

$3 = 8 - 1 \cdot 5$

$2 = 5 - 1 \cdot 3$

$1 = 3 - 1 \cdot 2$

so, $r0 = 13$ $r1 = 8$

$5 = r_0 - 1 \cdot r_1$

$3 = r_1 - 1 \cdot (r_0 - r_1)$

$2 = r_0 - r_1 - (r_1 - 1 \cdot (r_0 - r_1))$

$1 = r_1 - 1(r_0 - r_1) - (r_0 - r_1 - (r_1 - 1(r_0 - r_1))$

$1 = r_1 - r_0 + r_1 - (r_0 - r_1 - (r_1 - r_0 + r_1))$

$1 = 2r_1 - r_0 - (r_0 - r_1 - r_1 + r_0 - r_1)$

$$1 = 2r_1 - r_0 - (2r_0 - 3r_1)$$

$$1 = 5r_1 - 3r_0$$

Thus, the multiplicative inverse is 5.

4. Multiplicative inverse
83 in Z_{191}

Since we have to find multiplicative inverse of it then we are supposed to use Euclid Algorithm and Diophantine equation.

Lets say we are solving

$$191 = 83 \cdot 2 + 25$$

$$83 = 25 \cdot 3 + 8$$

$$25 = 8 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

$$25 = 191 - 83 \cdot 2$$

$$8 = 83 - 25 \cdot 3$$

$$1 = 25 - 8 \cdot 3$$

Let's say $r_0 = 191$ and $r_1 = 83$

$$25 = r_0 - r_1 \cdot 2$$

$$8 = r_1 - (r_0 - r_1 2)3$$

$$1 = r_0 - 2r_1 - (r_1 - (r_0 - r_1 \cdot 2)3)3$$

$$1 = r_0 - 2r_1 - (r_1 - 3r_0 + 6r_1)3$$

$$1 = r_0 - 2r_1 - (3r_1 - 9r_0 + 18r_1)$$

$$1 = r_0 - 2r_1 - 3r_1 + 9r_0 - 18r_1$$

$$1 = 10r_0 - 23r_1$$

Since coefficient of r_1 is -23 & it is negative so we should add 191 to it.

$$-23 + 191 = 168$$

5.

$58 \cdot x + 26 \cdot y = \gcd(58, 26)$

we can solve for x & y using Diophantine Equation

$58 = 2 \cdot 26 + 6$

$26 = 4 \cdot 6 + 2$

$6 = 3 \cdot 2 + 0$

$6 = 58 - 2 \cdot 26$

$2 = \gcd(58, 26) = 26 - 4 \cdot 6$

$r_0 = 58 \qquad r_1 = 26$

$6 = 1 \cdot a - 2b$

$2 = b - 4(1 \cdot a - 2b)$

$2 = b - 4a + 8b$

$2 = -4a + 9b$

$x = -4$

$y = 9$

5. To Prove

If p is prime & $p \equiv 1 \bmod 5$

then it is $p \equiv 1 \bmod 10$

Given:-

p is prime means p has only two factors 1 and p.

Also, $p \equiv 1 \bmod 5$

This means

$$p \bmod 5 = 1 \bmod 5$$

That means.

$$p = 1 + 5 \cdot f \quad \text{--- (1)}$$

$$\Rightarrow (p-1) = 5f \quad \text{--- (11)}$$

If something is divisible by 10 then it is for sure divisible by 5 and 2.
Also, we know that every other prime number except 2 is odd number. That means p is odd and p - 1 is even, and p needs to be greater than 5 to hold eqn 1 true. and that means (p-1) is divisible by which leads to that.

Eqn (11) can be further simplified as-

$$(p-1) = 5 \cdot 2m$$

$$(p-1) = 10m$$

$$p = 10m+1$$

That means,

$$p \bmod 10 = 1 \bmod 10$$

$$p \equiv 1 \bmod 10$$

Hence, proved.