10/06/22

Assignment - 3.

(1.) Multiplicative Inverses:-

(a) Find set of Multiplicative Inverses in GF(29).

Sol:-

$GF(29) \rightarrow Z_p = \{0, \dots, p-1\}$

$Z_{29} = \{0, 1, 2, \dots, 28\}$

we know that for each element $(w) = Z_p$; $w \neq 0$ there exists a; $z \in Z_p$, such that $w \cdot z \pmod p = 1$.

w (Integer)	z (Modular Inverse)	verification
0	doesnt Exist	
1	1	$1 \times 1 \pmod{29} = 1$
2	15	$2 \times 15 \pmod{29} = 1$.
3	10	$3 \times 10 \pmod{29} = 1$.
4	22	$4 \times 22 \pmod{29} = 1$.
5	6	$5 \times 6 \pmod{29} = 1$.
6	5	$6 \times 5 \pmod{29} = 1$
7	25	$7 \times 25 \pmod{29} = 1$
8	11	$8 \times 11 \pmod{29} = 1$
9	13	$9 \times 13 \pmod{29} = 1$
10	3	$10 \times 3 \pmod{29} = 1$
11	8	$11 \times 8 \pmod{29} = 1$
12	17	$12 \times 17 \pmod{29} = 1$
13	9	$13 \times 9 \pmod{29} = 1$
14	27	$14 \times 27 \pmod{29} = 1$
15	2	$15 \times 2 \pmod{29} = 1$
16	20	$16 \times 20 \pmod{29} = 1$
17	12	$17 \times 12 \pmod{29} = 1$.

18	21	$18 \times 21 \pmod{29} = 1$
19	26	$19 \times 26 \pmod{29} = 1$
20	16	$20 \times 16 \pmod{29} = 1$
21	18	$21 \times 18 \pmod{29} = 1$
22	4	$22 \times 4 \pmod{29} = 1$
23	24	$23 \times 24 \pmod{29} = 1$
24	23	$24 \times 23 \pmod{29} = 1$
25	7	$25 \times 7 \pmod{29} = 1$
26	19	$26 \times 19 \pmod{29} = 1$
27	14	$27 \times 14 \pmod{29} = 1$
28	28	$28 \times 28 \pmod{29} = 1$

6. use extended Euclidean Alg to Find multiplicative inverses of $(20 \bmod 79)$, $(3 \bmod 62)$, & $(22 \bmod 91)$ and $(5 \bmod 23)$

Sol:- (i) $(20 \bmod 79)$

let $a = 79$ & $b = 20$.

First Find $\gcd(a, b) = d$.

$r_1 = 79 \bmod 20 = 19$	$q_1 = 3$
$r_2 = 20 \bmod 19 = 1$ (gcd)	$q_2 = 1$
$r_3 = 19 \bmod 1 = 0$	$q_3 = 19$

$\therefore \gcd(79, 20) = 1 = d$

Now, Find x, y such that ;

$$x a + y b = d.$$

$$x \cdot 79 + y \cdot 20 = 1$$ (From Extended Euclidean)

We know, $r = \text{dividend} - q \cdot \text{divisor}$

$$1 = 20 - 1(19)$$

$$1 = 20 - 1(79 - 3(20))$$

$$1 = 20 - 1(79) + 3(20)$$

$$1 = 4(20) - 1(79)$$

$$\therefore x = -1 \ \& \ y = 4.$$

→ x is a Multiplicative Inverse of a,

$a \bmod b \Rightarrow a \cdot x \bmod b = 1$

$79 \bmod 20 \Rightarrow 79 \cdot (-1) \bmod (20) = 1$

→ y is a Multiplicative Inverse of b,

$b \bmod a \Rightarrow b \cdot y \bmod a = 1$

$20 \bmod 79 \Rightarrow 20 \cdot (4) \bmod 79 = 1$

(ii) $(3 \bmod 62)$

let $a = 62$ & $b = 3$ then find $\gcd(a, b) = d$.

$r_1 = 62 \bmod 3 = 2$	$q_1 = 20$
$r_2 = 3 \bmod 2 = 1$ (gcd)	$q_2 = 1$
$r_3 = 2 \bmod 1 = 0$	$q_3 = 2$

$\therefore \gcd(62, 3) = 1 = d$

$\therefore$ From, $\boxed{x \cdot a + y \cdot b = d}$; we need to

1) 2(2
2
0

find x & y.

$$x \cdot 62 + y \cdot 3 = 1$$

we know that, $r = \text{dividend} - q \cdot \text{divisor}$

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

$$1 = 3 - 1 \cdot (62 - 20 \cdot (3))$$

$$1 = 3 - 1(62) + 20(3)$$

$$1 = 21(3) - 1(62)$$

$$\therefore x = -1 \ \& \ y = 21.$$

→ x is a multiplicative inverse of a;

a mod b ⇒ $a \cdot x \bmod b = 1$

$$62 \cdot (-1) \bmod 3 = \underline{1}.$$

→ y is a multiplicative inverse of b;

b mod a ⇒ $b \cdot y \bmod a = 1$

$$3 \cdot (21) \bmod 62$$

$$63 \bmod 62 = \underline{1}$$

iii. (22 mod 91).

let $a = 91$ & $b = 22$ then find, $\gcd(a, b) = d$.

$r_1 = 91 \bmod 22 = 3$	$q = 4$
$r_2 = 22 \bmod 3 = 1$ gcd	$q = 7$
$r_3 = 3 \bmod 1 = 0$	$q = 3$

$\therefore \gcd(91, 22) = 1 = d.$

$\therefore x \cdot a + y \cdot b = d$

$x \cdot 91 + y \cdot 22 = 1$

we know that r = dividend − $q \cdot$ divisor

$\therefore 1 = 22 - 7 \cdot (3)$

$1 = 22 - 7 \cdot (91 - 4 \cdot (22))$

$1 = 22 - 7 \cdot (91) + 28(22)$

$1 = 29(22) - 7 \cdot (91)$

$\therefore x = -7$ & $y = 29$.

→ x is a multiplicative inverse of a;

$a \bmod b \Rightarrow a \cdot x \bmod b = 1$

$91 \cdot (-7) \bmod 22 = 1$.

→ y is a Multiplicative Inverse of b;

$b \bmod a \Rightarrow b \cdot y \bmod a = 1$

$22 \cdot (29) \bmod 91 = 1$.

(iv) $(5 \bmod 23)$

Let $a = 23$ & $b = 5$.

Now Find $\gcd(a, b) = d$.

$r_1 = 23 \bmod 5 = 3$	$q_1 = 4$
$r_2 = 5 \bmod 3 = 2$	$q_2 = 1$
$r_3 = 3 \bmod 2 = 1$ (gcd)	$q_3 = 1$
$r_4 = 2 \bmod 1 = 0$	$q_4 = 2$

$\therefore \gcd(23, 5) = 1 = d$.

$\therefore x \cdot a + y \cdot b = d$

$\therefore x \cdot 23 + y \cdot 5 = 1$

we know that, $\boxed{r = \text{dividend} - q \cdot \text{divisor}}$

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

$$1 = 3 - 1 \cdot (5 - 1 \cdot (3))$$

$$1 = 3 - 5 + 1(3)$$

$$1 = 2(3) - 1 \cdot (5)$$

$$1 = 2(23 - 4 \cdot (5)) - 1 \cdot (5)$$

$$1 = 2(23) - 8(5) - 1(5)$$

$$1 = 2(23) - 9(5)$$

$$\therefore x = 2 \;\&\; y = -9.$$

→ x is a multiplicative inverse of a, $a \bmod b$ $\Rightarrow$ $a \cdot x \bmod b = 1$

$$23 \cdot (2) \bmod 5 = 1.$$

→ y is a multiplicative inverse of b; $b \bmod a$ $\Rightarrow$ $b \cdot y \bmod a = 1$

$$5 \cdot (-9) \bmod 23$$

$$-45 \bmod 23 = 1.$$

(2) How many integers modulo 11^3 have inverses?

<u>sol:-</u> $Z_p^* = 11^3 = 1331.$

$\therefore Z_p^* = \{ 1, \ldots, p-1 \}$

$\therefore Z_p^* = \{ 1, \ldots, 1330 \}$

→ A number 'x' has an inverse modulo 11^3, if and only if $GCD(x, 1331) = 1$.

→ If $GCD(x, 1331) \neq 1$, then $x = 0$ (or) shares a common factor with 11^3.

→ The only factors of 11^3 are $11, 121, 1331$. Thus a non-zero number doesn't have an inverse, if and only if it is a multiple of 11.

→ The no. of multiples of 11 btw 1 & 1330 is,

$$\frac{1331}{11} - 1 = 120$$ (Because we only consider upto 1330.)

Thus, the no. of numbers that have an inverse is, $1331 - 120 - 1 = \underline{\underline{1210}}$.

(3.) Find the set of polynomials in $GF(2^5)$ and $GF(5^2)$.

<u>sol:-</u> → we know that for $GF(p^n)$, if p is prime, & $n > 0$ has exactly p^n polynomials.

Where, $\boxed{f(x) = \sum_{i=0}^{n-1} a_i \cdot \ldots x^i}$

where $a_i \in \{0, \cdots, p-1\}$

(i) $GF(2^5)$

$\hookrightarrow p = 2$ & $n = 5$.

Now, $a_i \in \{0, \cdots, p-1\}$ such that

$a_i \in \{0, 1\}$ and

Now, $f(x) = \sum_{i=0}^{n-1} a_i \cdot \cdots x^i$.

$$f(x) = \sum_{i=0}^{4} a_i \cdot x^i$$

$\underline{i=0:}$ $f(x) = a_0 \cdot x^0$

$\therefore S_0 = \{0, 1\}$

$\underline{i=1:}$ $f(x) = a_0 \cdot x^0 + a_1 x^1$

$\therefore S_1 = \{\overset{(0,0)}{0}, \overset{(0,1)}{x}, \overset{(1,0)}{1}, \overset{(1,1)}{1+x}\}$

$\underline{i=2:}$ $f(x) = a_0 \cdot x^0 + a_1 \cdot x^1 + a_2 \cdot x^2$

$\therefore S_2 = \{0, x, 1, 1+x, x^2, 1+x^2, x+x^2, x^2+x+1\}$

$\underline{i=3:}$ $f(x) = a_0 \cdot x^0 + a_1 \cdot x^1 + a_2 \cdot x^2 + a_3 \cdot x^3$

$\therefore S_3 = \{0, x^3, x^2, x^2+x^3, x, x+x^3, x+x^2, x+x^2+x^3, 1, 1+x^3, 1+x^2, 1+x^2+x^3, 1+x, 1+x+x^3, 1+x+x^2,$

$1+x+x^2+x^3\}$.

<u>$i=4$:</u> $f(x) = a_0 \cdot x^0 + a_1 \cdot x^1 + a_2 \cdot x^2 + a_3 \cdot x^3 + a_4 \cdot x^4$.

$\therefore S_4 = \{0, x^4, x^3, x^3+x^4, x^2, x^2+x^4, x^2+x^3, x^2+x^3+x^4, x, x+x^4, x+x^3, x+x^3+x^4, x+x^2, x+x^2+x^4, x+x^2+x^3, x+x^2+x^3+x^4, 1, 1+x^4, 1+x^3, 1+x^3+x^4, 1+x^2, 1+x^2+x^4, 1+x^2+x^3, 1+x^2+x^3+x^4, 1+x, 1+x+x^4, 1+x+x^3, 1+x+x^3+x^4, 1+x+x^2, 1+x+x^2+x^4, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4\}$

$\therefore S = S_1 \cup S_2 \cup S_3 \cup S_4$.

$\therefore S = \{0, x^4, x^3, x^3+x^4, x^2, x^2+x^4, x^2+x^3, x^2+x^3+x^4, x, x+x^4, x+x^3, x+x^3+x^4, x+x^2, x+x^2+x^4, x+x^2+x^3, x+x^2+x^3+x^4, 1, 1+x^4, 1+x^3, 1+x^3+x^4, 1+x^2, 1+x^2+x^4, 1+x^2+x^3, 1+x^2+x^3+x^4, 1+x, 1+x+x^4, 1+x+x^3, 1+x+x^3+x^4, 1+x+x^2, 1+x+x^2+x^4, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4\}$

(ii) $GF(5^2)$.

↳ let $p=5$ & $n=2$.

Now, $\left(b(x) = \sum_{i=0}^{n-1} a_i \cdot x^i\right) \Rightarrow b(x) = \sum_{i=0}^{1} a_i \cdot x^i$

$a_i \in \{0, 1, 2, 3, 4\}$

<u>$i=0$:</u> $b(x) = a_0 \cdot x^0$

$\therefore S_0 = \{0, 1, 2, 3, 4\}$

<u>$i=1$:</u> $b(x) = a_0 \cdot x^0 + a_1 \cdot x^1$

$\therefore S_1 = \{0, 1+x, 2+2x, 3+3x, 4+4x, x, 2x, 3x, 4x, 1, x+2x, x+3x, x+4x, 2, 2+x, 2+3x, 2+4x, 3, 3+x, 3+2x, 3+4x, 4, 4+x, 4+2x, 4+3x.\}$

$\therefore S = S_0 \cup S_1$.

$\therefore S = \{0, 1+x, 2+2x, 3+3x, 4+4x, x, 2x, 3x, 4x, 1, x+2x, x+3x, x+4x, 2, 2+x, 2+3x, 2+4x, 3, 3+x, 3+2x, 3+4x, 4, 4+x, 4+2x, 4+3x.\}$

(4) (a) Find $d = \gcd(423, 128)$

Sol:-

let $a = 423$ & $b = 128$.

then,

$r_1 = 423 \bmod 128 = 39$	$q_1 = 3$
$r_2 = 128 \bmod 39 = 11$	$q_2 = 3$
$r_3 = 39 \bmod 11 = 6$	$q_3 = 3$
$r_4 = 11 \bmod 6 = 5$	$q_4 = 1$
$r_5 = 6 \bmod 5 = 1$ (gcd)	$q_5 = 1$
$r_6 = 5 \bmod 1 = 0$	$q_6 = 5$.

$\therefore \gcd(423, 128) = 1 = d$.

→ Here gcd = 1, and Hence they are co-prime

$1 = x \cdot 423 + y \cdot 128$

we know that dividend = divisor $\cdot q + r$

r = dividend − $q \cdot$ divisor

$1 = 6 - 1 \cdot 5$

$= 6 - 1 \cdot (11 - 1 \cdot 6)$

$= 6 \cdot 1 - 1(11 - 6 \cdot 1)$

$= 2(6) - (11)1$

$= 2(39 - 3 \cdot (11)) - 1 \cdot (11)$

$$= 2\cdot(39) - 6(11) - 1(11)$$

$$= 2\cdot(39) - 7(11)$$

$$= 2(39) - 7(128 - 3\cdot(39))$$

$$= 2(39) - 7(128) + 21(39)$$

$$= 23(39) - 7(128)$$

$$= 23(423 - 3(128)) - 7(128)$$

$$= 23(423) - 69(128) - 7(128)$$

$$= 23(423) - 76(128)$$

$$\therefore x = 23 \;\&\; y = -76.$$

(6.) Find $d = \gcd(588, 210)$.

Sol: Let $a = 588$ & $b = 210$.

then,

$r_1 = 588 \bmod 210 = 168$	$q_1 = 2$
$r_2 = 210 \bmod 168 = 42$ (gcd)	$q_2 = 1$
$r_3 = 168 \bmod 42 = 0$	$q_3 = 4$

$$\therefore \gcd(588, 210) = 42 = d.$$

→ The gcd is not 1, Hence they are not co-prime.

$$\therefore 42 = x\cdot 588 + y\cdot 210.$$

we know that, $\boxed{\text{dividend} = \text{divisor}\cdot q + r}$

$$r = \text{dividend} - q\cdot\text{divisor}$$

$$42 = 210 - 1 \cdot 168$$

$$= 210 - 1 \cdot (588 - 2 \cdot (210))$$

$$= 210 - 1 \cdot 588 + 2(210)$$

$$= 3(210) - 1 \cdot 588$$

$$\therefore x = -1 ; y = 3.$$

(c) Find gcd(899, 493).

Sol:- Let $a = 899$ & $b = 493$.

then,

$r_1 = 899 \bmod 493 = 406$	$q_1 = 1$
$r_2 = 493 \bmod 406 = 87$	$q_2 = 1$
$r_3 = 406 \bmod 87 = 58$	$q_3 = 4$
$r_4 = 87 \bmod 58 = 29$ (gcd)	$q_4 = 1$
$r_5 = 58 \bmod 29 = 0$	$q_5 = 2$

$$\therefore \gcd(899, 493) = 29 = d$$

→ Here GCD is not 1, & hence they are not co-prime.

$$\therefore 29 = x \cdot 899 + y \cdot 493.$$

we know that $\boxed{r = \text{dividend} - q \cdot \text{divisor}}$

$$29 = 87 - 1 \cdot 58$$

$$= 87 - 1 \cdot (406 - 4 \cdot 87)$$

$$= 87 - 1 \cdot 406 + 4(87)$$

$$= 5(87) - 1\cdot(406)$$

$$= 5(493 - 1\cdot(406)) - 1\cdot 406$$

$$= 5(493) - 5(406) - 1(406)$$

$$= 5(493) - 6(406)$$

$$= 5(493) - 6(899 - 1\cdot(493))$$

$$= 5(493) - 6(899) + 6(493)$$

$$= 11(493) - 6(899)$$

$$\therefore x = -6 \ \& \ y = 11.$$

5. a. $3^{1000} \bmod 100.$

Sol: Here, $\mathbb{Z}_{100} = \{0, 1, 2, \ldots, 99\}$

$G = \mathbb{Z}^*_{100} = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97, 99\}$

$x = |\mathbb{Z}^*_{100}| = 40.$

we know from given, $y = 1000$ &
we know that, If G is a group of order x and $a \in G$,
then $\boxed{a^y \bmod n = a^{y \bmod x} \bmod n.}$

$\therefore 3^{1000} \bmod 100 = 3^{1000 \bmod 40} \bmod 100.$

$= 3^{0} \bmod 100.$

$= 1 \bmod 100$

$= \underline{1}.$

(b) $101^{4,800,000,002} \bmod 35.$

Sol:- $\mathbb{Z}_{35} = \{0, 1, 2, \ldots, 34\}$

$G = \mathbb{Z}_{35}^{*} = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$

$x = |\mathbb{Z}_{35}^{*}| = 24.$ & $y = 4,800,000,002$ (from given)

→ we know that if 'G' is a group of order x and $a \in G$, then $\boxed{a^{y} \bmod n = a^{y \bmod x} \bmod n}$

$\therefore 101^{4,800,000,002} \bmod 35 = 101^{4,800,000,002 \bmod 24} \bmod 35$

$= 101^{2} \bmod 35.$

$= \underline{16}.$

(c) $46^{51} \bmod 55.$

Sol:- $\mathbb{Z}_{55} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots, 54\}$

$\mathbb{Z}_{55}^{*} = \{1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 21, 23, 24, 26, 27, 28, 29, 31, 32, 34,$

36, 37, 38, 39, 41, 42, 43, 46, 47, 48, 49, 51, 52, 53, 54}

$x = |Z_{55}^*| = 40$ & $y = 51$ (from given)

→ we know that if 'G' is a group of order x and $a \in G$, then $\boxed{a^y \bmod n = a^{y \bmod x} \bmod n}$

$$46^{51} \bmod 55 = 46^{51 \bmod 40} \bmod 55$$

$$= 46^{11} \bmod 55$$

$$= \underline{46}.$$

(6) Is $(4^{1536} - 9^{4824})$ divisible by 25?

Sol:

$$(4^{1536} - 9^{4824}) \bmod 25$$

→ we know that $\boxed{(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n}$

from Modular Arithmetic property.

let $a = 4^{1536}$ & $b = 9^{4824}$ & $n = 25$.

$$\Rightarrow [(4^{1536} \bmod 25) - (9^{4824} \bmod 25)] \bmod 25.$$

→ we can apply group order property for the above.

- since $n = 25$, so $Z_{25}^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

$\therefore x = |Z_{25}^*| = 20.$

→ we know that if 'G' is a group of order x and $a \in G$, then $\boxed{a^y \bmod n = a^{y \bmod x} \bmod n}$

$$\Rightarrow \left[\left(4^{1536 \bmod 20} \bmod 25\right) - \left(9^{4824 \bmod 20} \bmod 25\right)\right] \bmod 25$$

$$\Rightarrow \left[\left(4^{16} \bmod 25\right) - \left(9^{4} \bmod 25\right)\right] \bmod 25$$

$$\Rightarrow \left[\left(2^{2(16)} \bmod 25\right) - \left(9^{4} \bmod 25\right)\right] \bmod 25.$$

$$\Rightarrow \left(\left(2^{32} \bmod 25\right) - \left(9^{4} \bmod 25\right)\right) \bmod 25.$$

$$\Rightarrow \left[\left(2^{32 \bmod 20} \bmod 25\right) - \left(9^{4} \bmod 25\right)\right] \bmod 25.$$

$$\Rightarrow \left[\left(2^{12} \bmod 25\right) - \left(9^{4} \bmod 25\right)\right] \bmod 25.$$

$$\Rightarrow \left(4096 \bmod 25\right) - \left(6561 \bmod 25\right)\Big] \bmod 25.$$

$$\Rightarrow 10 \bmod 25$$

$$\Rightarrow 10 \neq 0.$$

Hence, It is not divisible by 25, as the remainder is not '0'.

7. Is the difference btw $5^{30,000}$ and 6^{123456} a multiple of 23?

Sol:- → we can apply group order property for each of them and then find if the difference btw them is a multiple of 23 or not.

$$\mathbb{Z}_{23} = \{0, 1, 2, 3, \ldots, 22\}$$

$$G = \mathbb{Z}_{23}^{*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$$

$$\therefore x = |\mathbb{Z}_{23}^{*}| = 22.$$

$$5^{30,000} \bmod 23.$$

$$\equiv 5^{30,000 \bmod 22} \bmod 23.$$

$$\equiv 5^{16} \bmod 23.$$

$$\equiv (5^2 \cdot 5^{12}) \bmod 23$$

$$\equiv (25 \bmod 23 \cdot 5^{12} \bmod 23) \bmod 23$$

$$\equiv (2 \cdot (5^6 \cdot 5^6) \bmod 23) \bmod 23$$

$$\equiv (2 \cdot ((5^6 \bmod 23) \cdot (5^6 \bmod 23)) \bmod 23) \bmod 23$$

$$\equiv (2 \cdot 15625 \bmod 23 \cdot 15625 \bmod 23) \bmod 23$$

$$\equiv ((2 \cdot 8 \cdot 8) \bmod 23) \bmod 23 \qquad \bmod 23$$

$$\equiv (128 \bmod 23) \bmod 23$$

$$= \underline{13}.$$

$6^{123,456} \bmod 23.$

$\equiv 6^{123,456 \bmod 22} \bmod 23.$

$\equiv 6^{14} \bmod 23.$

$\equiv (6^2 \cdot 6^{12}) \bmod 23$

$\equiv (36 \cdot 6^{12}) \bmod 23$

$\equiv ((36 \bmod 23) \cdot (6^{12} \bmod 23)) \bmod 23.$

$\equiv (13 \cdot (6^6 \cdot 6^6 \bmod 23)) \bmod 23.$

$\equiv (13 \cdot ((6^6 \bmod 23) \cdot (6^6 \bmod 23)) \bmod 23) \bmod 23$

$\equiv (13 \cdot ((46656 \bmod 23) \cdot (46656 \bmod 23)) \bmod 23) \bmod 23$

$\equiv (13 \cdot (12 \cdot 12) \bmod 23) \bmod 23$

$= \underline{9.}$

$\therefore$ The difference btw $5^{30,000}$ and $6^{123,456}$ is, $(5^{30,000} \bmod 23) - (6^{123,456} \bmod 23) \bmod 23$

$= (5^{30,000} - 6^{123,456}) \bmod 23 = 13 - 9 = \underline{4.}$

$\therefore$ It is not a multiple of 23.