CS-206

ASSIGNMENT-8

- TARUSI MITTAL
- 1901CS65
- Tarusi Mittal

Tarusi Mittal
1901CS65

Que 1:- (a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$

→ since -15 is between -26 and 0.

$\boxed{a = -15}$ Ans.

(b) $a \equiv (24) \pmod{31}$ and $-15 \leq a \leq 15$

→ $a \equiv 24 \pmod{31}$

$a \equiv 24 - 31 \pmod{31}$

$a \equiv -7 \pmod{31}$

since -7 is between -15 and 15

$\boxed{a = -7}$ Ans

Que 2:- (a) $(99^2 \bmod 32)^3 \bmod 15$

→ We know if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then
$a + c = b + d \pmod m$ and $ac \equiv bd \pmod m$

Using this theorem, the above statement can be written as.

$= ((99 \bmod 32)^2 \bmod 32)^3 \bmod 15$

$= (3^2 \bmod 32)^3 \bmod 15$ $\quad [99 \bmod 32 = 3]$

$= (9 \bmod 32)^3 \bmod 15$

$= 9^3 \bmod 15$

$= 729 \bmod 15$

$= \boxed{9}$ Ans

Taruni Mittal 2.
1901CS65
Tarunimittal

(b) $(89^3 \bmod 79)^4 \bmod 26$

→ Using the theorem stated in the previous part

$= ((89 \bmod 79)^3 \bmod 79)^4 \bmod 26$

$= (10^3 \bmod 79)^4 \bmod 26$ [89 mod 79 is 10]

$= (1000 \bmod 79)^4 \bmod 26$

$= 52^4 \bmod 26$ [1000 mod 79 is 52]

again using the theorem.

$= (52 \bmod 26)^4 \bmod 26$

$= 0 \bmod 26$ [52 mod 26 = 0 as 52 = 26×2+0)

$= \boxed{0}$ Ans.

Que 3:- Find the inverse modulo m, for pair of prime integers:

⇒ (a) $a = 55$, $b = 89$

→ The inverse of a an integer a modulo m is an integer b such that $ab \equiv 1 \pmod m$

Performing Euclidean Algorithm

$89 = 1.55 + 34$

$55 = 1.34 + 21$

$34 = 1.21 + 13$

$21 = 1.13 + 8$

$13 = 1.8 + 5$

$8 = 1.5 + 3$

$5 = 1.3 + 2$

$3 = 1.2 + 1$

$2 = 2.1 + 0$

Taruni Mittal
1901CS65

The greatest common divisor gcd (a, m) = 1.

Now we write gcd as a multiple of a and m.

$$\gcd(a,m) = 1$$
$$= 3 - 1.2$$
$$= 1.3 - 1.2$$
$$= 1.3 - 1.(5 - 1.3)$$
$$= 2.3 - 1.5$$
$$= 2.(8 - 1.5) - 1.5$$
$$= 2.8 - 3.5$$
$$= 2.8 - 3.(13 - 1.8)$$
$$= 5.8 - 3.13$$
$$= 5.(21 - 1.13) - 3.13$$
$$= 5.21 - 8.13$$
$$= 13.21 - 8.34$$
$$= 13.(55 - 1.34) - 8.34$$
$$= 13.55 - 21.34$$
$$= 13.55 - 21.(89 - 1.55)$$
$$= 34.55 - 21.89.$$

So, the inverse comes out to be $\boxed{34}$ Ans

(b) $a = 89$, $m = 232$

→
$$232 = 2.89 + 54$$
$$89 = 1.54 + 35$$
$$54 = 1.35 + 19$$
$$35 = 1.19 + 16$$
$$19 = 1.16 + 3$$
$$16 = 5.3 + 1$$
$$3 = 3.1$$

Tarun Mittal
1901CS65

gcd (a,m) = 1

Now :

$$
\begin{aligned}
\gcd(a,m) &= 1 \\
&= 16 - 5.3 \\
&= 1.16 - 5.3 \\
&= 1.16 - 5.(19 - 1.16) \\
&= 6.16 - 5.19 \\
&= 6.(35 - 1.19) - 5.19 \\
&= 6.35 - 11.19 \\
&= 6.35 - 11.(54 - 1.35) \\
&= 17.35 - 11.54 \\
&= 17.(89 - 1.54) - 11.54 \\
&= 17.89 - 28.54 \\
&= 17.89 - 28.(232 - 2.89) \\
&= 73.89 - 28.232
\end{aligned}
$$

Thus the inverse is $\boxed{73}$ Ans.

Que 4:- (a) $f(p) = (3p+7) \bmod 26$ [the Caesar cipher]

→ In Caesar Cipher : A = 0, B = 1 → ... Y = 24, Z = 25

DO NOT PASS GO → 3, 14, 13, 14, 19, 15, 0, 18, 18, 6, 14

$f(P) = (3p+7) \bmod 26$ → 16, 23, 20, 23, 12, 0, 7, 9, 9, 25, 23

$\boxed{\text{QX UXM AHJJ ZX}}$ Ans

Tarun Mittal
1901CS65
Tarun Mittal

Que 5:- Prime factorization

(a) 729

→

3	729
3	243
3	81
3	27
3	9
	3

$729 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3.$

$\boxed{729 = 3^6}$ Ans.

(b) 1001

7	1001
11	143
	13

$\boxed{1001 = 7 \cdot 11 \cdot 13}$ Ans.

Que 6:- Convert $(1011\ 0111\ 1011)_2$ from binary expansion to hexadecimal

→ The binary expansion has base 2.

$= 1 \cdot 2^{11} + 0 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3$
$+ 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

$= 2048 + 512 + 256 + 64 + 32 + 16 + 8 + 2 + 1$

$= 2939$

P.T.O.

Tarush Mittal
1901CS65

To obtain binary :

In hexadecimal.

$A = 10$
$B = 11$
$\vdots$

$2939 = 16 \cdot 183 + 11$

$183 = 16 \cdot 11 + 7$

$11 = 16 \cdot 0 + 11$

The successive remainders of each division represents binary representation from bottom to up

$= \boxed{(B7B)_{16}}$

Ans.

Que 7: $(ABCDEF)_{16}$

$\rightarrow$

$(ABCDEF)_{16} = 10 \cdot 16^5 + 11 \cdot 16^4 + 12 \cdot 16^3 + 13 \cdot 16^2 + 14 \cdot 16^1 + 15 \cdot 16^0$

$= 10485760 + 720896 + 49152 + 3328 + 224 + 15$

$= 11259375$

Now consecutively dividing the number by 2 until we obtain 0.

$11259375 = 2 \cdot 5629687 + 1$

$5629687 = 2 \cdot 2814843 + 1$

$2814843 = 2 \cdot 1407421 + 1$

$1407421 = 2 \cdot 703710 + 0$

$703710 = 2 \cdot 351855 + 0$

$351855 = 2 \cdot 175927 + 1$

$175927 = 2 \cdot 87963 + 1$

$87963 = 2 \cdot 43981 + 1$

$43981 = 2 \cdot 21990 + 1$

$21990 = 2 \cdot 10995 + 0$

Tanusi Mittal
19010365
Assignment 1

$10995 = 2 \cdot 5497 + 1$

$5497 = 2 \cdot 2748 + 1$

$2748 = 2 \cdot 1374 + 0$

$1374 = 2 \cdot 687 + 0$

$687 = 2 \cdot 343 + 1$

$343 = 2 \cdot 171 + 1$

$171 = 2 \cdot 85 + 1$

$85 = 2 \cdot 42 + 1$

$42 = 2 \cdot 21 + 1$

$21 = 2 \cdot 10 + 1$

$10 = 2 \cdot 5 + 0$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 1$

The successive remainders of each division represents binary expansion from bottom to top.

$$\boxed{(1010\ 1011\ 1100\ 1101\ 1110\ 1111)_2}$$

Ans.

Ques 8: Convert octal expansion to binary.

(a) $(572)_8$

→ $(572)_8 = 5 \cdot 8^2 + 7 \cdot 8^1 + 2 \cdot 8^0$

$= 320 + 56 + 2$

$= 378$

Tanush Mittal
1901CS65

We will consequtively divide by 2 until we get 0.

$378 = 2 \cdot 189 + 0$

$189 = 2 \cdot 94 + 1$

$94 = 2 \cdot 47 + 0$

$47 = 2 \cdot 23 + 1$

$23 = 2 \cdot 11 + 1$

$11 = 2 \cdot 5 + 1$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 1$

The successive remainders give binary expansion from bottom to top.

$\boxed{(1\ 0111\ 1010)_2}$ Ans.

—x—x—x—x—x—x—x—x—x—x—