CSE4003 : Cyber Security DA-1

Sharadindu Adhikari, 19BCE2105

↳ register number modulo 5

$\Leftrightarrow$ 2105 modulo 5 = 0 $\Leftrightarrow$ set-5

Q1. Find GCD (7469, 2464) using Euclidean algorithm.
Find x, y, MMI for the same using EEA.

Soln: We've, $c = dq + r$; $0 \le r < d$.

here, $c = 7469$ and $d = 2464$ (at step-1).

Euclidean algorithm corresponds:

$$7469 = 2464 * 3 + 77$$

$$\Leftrightarrow 2464 = 77 * 32 + 0$$

$\therefore$ gcd (7469, 2464) = 77.

again, using the Extended Euclidean Algorithm, we've:

[assumption: at step-1, $x = 1$, $s_1 = 0$, $y = 0$, $t_1 = 1$,

and: $s_2 = x - q \cdot s_1$; $t_2 = y - q \cdot t_1$]

[[table on the next page. s_2 and t_2's calculations here]]

↳ $s_2 = 1 - 3 \cdot 0 = 1$ | $t_2 = 0 - 3 \cdot 1 = -3$

again, $s_2 = 0 - 32 \cdot 1 = -32$ | again, $t_2 = 1 - 32 \cdot (-3) = 97$

19BCE2105

EEA table:

q	a	b	r	x	s_1	s_2	y	t_1	t_2
3	7469	2464	77	1	0	1	0	1	-3
32	2464	77	0	0	1	-32	1	-3	97
x	77	0	x	1		-32		-3	97

$\therefore x = 1.$ $\quad$ again, gcd = 77

$y = -3.$

this also implies that, $ax + by$ must be $= 77$

let's check: $\quad 7469 \cdot (1) + 2464 \cdot (-3)$

$= 7469 - 739$ ✓

$= 77.$ $\quad$ checks out.

Hence, $\gcd(7469, 2464) = 77 \neq 1$

$\therefore$ MMI does not exist

19BCE2105

Q2. (i) find the result : $-5432 \bmod 38$

solve: $-5432 \bmod 38$

$= 38 - (5432 \bmod 38)$

$= 38 - 36$

$= 2$

(ii) find the result: $\phi(606)$.

solve: $\phi(606) = \phi(101 \times 6)$

$= \phi(101) \cdot \phi(6)$

$= 100 \cdot \phi(3 \times 2)$

$= 100 \cdot \phi(3) \cdot \phi(2)$

$= 100 : 2 : 1$

$= 200$

(7.5.0)

19BCE2105

Q3.

Find $18^{1001} \bmod 11$.

Soln: we've: $18^{1001} \bmod 11$

$\Leftrightarrow 18^{1} \bmod 11 = 7$

$\Leftrightarrow 18^{2} \bmod 11 = 5$

$\Leftrightarrow 18^{4} \bmod 11 = 25 \bmod 11 = 3$

$\Leftrightarrow 18^{8} \bmod 11 = 9 \bmod 11 = 9$

$\Leftrightarrow 18^{16} \bmod 11 = 81 \bmod 11 = 4$

$\Leftrightarrow 18^{32} \bmod 11 = 16 \bmod 11 = 5$

$\Leftrightarrow 18^{64} \bmod 11 = 25 \bmod 11 = 3$

$\Leftrightarrow 18^{128} \bmod 11 = 9 \bmod 11 = 9$

$\Leftrightarrow 18^{256} \bmod 11 = 81 \bmod 11 = 4$

$\Leftrightarrow 18^{512} \bmod 11 = 5$

now:

$\Leftrightarrow 18^{1001} \bmod 11 = \left(18^{1000} \times 18^{1}\right) \bmod 11$

$= \left(18^{512} \times 18^{256} \times 18^{128} \times 18^{64} \times 18^{32} \times 18^{8} \times 18^{1}\right) \bmod 11$

(P.T.O.)

19BCE2105

$$\Leftrightarrow \quad 18^{1001} \bmod 11 = (5 \times 4 \times 9 \times 3 \times 5 \times 9 \times 7) \bmod 11$$

$$= 170100 \bmod 11$$

$$= 7$$

$$\therefore \quad 18^{1001} \bmod 11 = 7 \quad \text{ans.}$$