University of Asia Pacific

Department of Computer Science and Engineering

Assignment 1

Course Title: Computer and Cyber Security

Course Code: CSE 317

Section: E

Date of Submission: 29/11/2025

Submitted by:

Kamrun Nahar Konika (22201241)

Submitted to:

Rashik Rahman

Lecturer,

Department of Computer Science and Engineering

University of Asia Pacific

Assignment Question:

Find modular inverse of the last two digits of your **id mod 101** using

I. Extended Euclidean Algorithm

II. Euler's Theorem : **id mod n ;** where n is the next co-prime number with your id (2 digits)

III. Fermat's Little Theorem

Kamrun Nahar Konika
ID - 22201241 (E)

1] Extend Euclidian Algorithm

⇒ what is the value of $41^{-1} \bmod 101$

Ans:

$Z_{101} = \{1, 2, 3, 4, 5 \cdots 100\}$

$Z_{101}^{*} = \{1, 2, 3, 4, 5 \cdots 100\}$

$|Z_{101}^{*}| = \phi(n) = 100$

GCD (~~100~~ 41, 101):

$$\boxed{41)\,101\,(2 \quad \cancel{82} \quad 9}$$

$$
\begin{array}{l}
41)\,101\,(2 \\
\quad\ 82 \\
\hline
\quad 19)\,41\,(2 \\
\qquad\ 38 \\
\hline
\qquad 2)\,19\,(9 \\
\qquad\quad 18 \\
\hline
\qquad\quad 1)\,41\,(41 \\
\qquad\qquad 41 \\
\hline
\qquad\qquad 0
\end{array}
$$

$101 = 2(41) + 19$

$41 = 2(19) + 3$

$19 = 6(3) + 1$

$3 = 3(1) + 0$

Now, back substitute,

1.

2. $1 = 19 - 6 \cdot 3$

$3 = 41 - 2 \cdot 19$

$1 = 19 - 6(41 - 2 \cdot 19) = 13 \cdot 19 - 6 \cdot 41$

3. $13 = 101 - 2 \cdot 41$

$1 = 13(101 - 2 \cdot 41) - 6 \cdot 41 = 13 \cdot 101 - 32 \cdot 41$

$\therefore$

$-32 \cdot 41 + 13 \cdot 101 = 1$

~~According to definition:~~

~~$41^{-1} \bmod 101 = 69$~~

Taking mod 101:

$41^{-1} = -32 \equiv 101 - 32$

$= 69 \pmod{101}$

$\therefore$ According to definition:

$41^{-1} \bmod 101 = 69.$

(Ans)

2] Euler's Theorem:

$Z_{101} = \{1, 2, 3, 4, 5, \ldots 100\}$

$Z_{101}^* = \{1, 2, 3, 4, 5 - 100\}$

$|Z_{101}^*| = \varphi(n) = 100$

For each element in Z_n^*

$x^{\varphi(n)} \bmod n = 1$

$1^{41} \bmod 101 = 1$

$2^{41} \bmod 101 = 72$

$\vdots$

~~$100^{41} \bmod 101 =$~~ $41^{100} \bmod 101 =$

As we need the base(41^{-1}). So, we calculate the value of 41^{100} using modular exponential.

Here, $(41)_{10} \rightarrow (?)_2$

$$41 = \underset{2^5\,2^4\,2^3\,2^2\,2^1\,2^0}{101001}$$

$$41^{100} = 41^{64} \cdot 41^{32} \cdot 41^{4} = 41^{64} \cdot 41^{32} \cdot 41^{4}$$

$41^1 \bmod 101 = 41$

$41^2 \bmod 101 = 65$

$41^4 \bmod 101 = (41^2 \bmod 101)^2 \bmod 101$
$= 84$

$41^8 \bmod 101 = (41^4 \bmod 101)^2 \bmod 101$
$= 87$

$41^{16} \bmod 101 = (41^8 \bmod 101)^2 \bmod 101$
$= 95$

$41^{32} \bmod 101 = (41^{16} \bmod 101)^2 \bmod 101$
$= 36$

$41^{64} \bmod 101 = (41^{32} \bmod 101)^2 \bmod 101$
$= 84$

$41^{100} \bmod 101 = (41^{64} \bmod 101)(41^{32} \bmod 101)(41^4 \bmod 101) \bmod 101$
$= 84 \times 36 \times 84 \bmod 101$
$= 1$

Here,

$41^{100} \bmod 101 = 1$

$(41^{1})(41^{99}) \bmod 101 = 1$

$(41^{-1}) \bmod 101 = 41^{99} \bmod 101$ —— (1)

Here,

41^{99} modular exponential is=

$(99)_{10} \rightarrow (?)_2 = \underset{2^6}{1}\,\underset{2^5}{1}\,\underset{2^4}{0}\,\underset{2^3}{0}\,\underset{2^2}{0}\,\underset{2^1}{1}\,\underset{2^0}{1}$

$= 64 + 32 + 2 + 1$

$41^{99} = 41^{64} \cdot 41^{32} \cdot 41^{2} \cdot 41^{1}$

$41^{99} = (84) \times (36) \times (65) \times 41 \bmod 101$

$\cancel{69 \bmod 101} = 69$

From (1) ⇒

$(41)^{-1} \bmod 101 = 41^{99} \bmod 101$

$= 41^{99} \bmod 101$

$= 69.$

(Ans)

3. **Fermat's Little Theorem:** Find the inverse of 41 mod 101. (5)

Fermat's little theorem states that if p is a prime number and a is not divisible by p.

$$a^{p-1} \equiv 1 \pmod p$$

Here, $p = 101$, $a = id = 41$

Here, $p = 101$ (which is prime)

$$\text{Inverse} = 41^{101-2} \pmod{101}$$

$$\text{Inverse} = 41^{99} \bmod 101$$

we need to calculate $41^{99} \pmod{101}$. Binary representation of 99 is $64+32+2+1$

(1) $41^1 \equiv 41$

(2) $41^2 \equiv 1681 = 16(101) + 65 \equiv 65$

(3) $41^4 \equiv (65)^2 = 4225$

(4) $41^8 \equiv (4225)^2 = 17850625 = 176738(101) + 87 \equiv 87$

(5) $41^{16} \equiv (87)^2 = 7569 = 74(101) + 95 \equiv 95$

(6) $41^{32} \equiv (95)^2 = 9025 = 89(101) + 36 = 36$

(7) $41^{64} \equiv (36)^2 = 1296 = 12(101) + 84 = 84$

combining the result:

$$41^{99} = 41^{64} \times 41^{32} \times 41^{2} \times 41^{1}$$

$$41^{99} = 84 \times 36 \times 65 \times 41 \pmod{101}$$

$$= (84 \times 36) \times (65 \times 41) \bmod 101$$

$$= 69.$$

From FTP,

$$41^{100} \bmod 101 = 1$$

$$(41)^{1} \cancel{m} (41^{99}) \bmod 101 = 1$$

by definition $(41^{-1}) \bmod 101 = 41^{99} \bmod 101$

$$= 69.$$

(Ans)