Iffate Jahan Nilima
ID: IT-21063

Prove fermat's Little theorem and use it to compute $a^{p-1} \bmod p$ for given values of $a=7$, $p=13$. Then discuss how this theorem is useful in cryptographic algorithms Like RSA.

→ Theorem:

If p is a prime number and a is an integer not divisible by p, then

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

proof: Consider the integers,

1, 2, 3, 4 ---- (p-1) they leave the remainders 1, 2, 3, ---- (p-1) when divided by p.

Consider an integer a relatively prime to p.

$a \cdot 1, a \cdot 2, a \cdot 3 \text{ ---- } a \cdot p-1$

observe that if,

$a \cdot i \equiv a \cdot j \pmod p, 1 \leq i, j \leq p-1$

Nilima
IT-21063

then $a(i-j) \equiv 0 \pmod{p}$

which is true if and only if $i=j$

$\therefore ai \not\equiv aj \pmod{p}$, for $1 \leq i, j \leq p-1, i \neq j$

$\therefore a.1, a.2, a.3 \text{ ---- } a(p-1)$ leaves $p-1$ number of different remainders when divided by p that is $a.1, a.2, a.3 \text{ --- } a(p-1)$ which are congruent to $1, 2, 3 \text{ --- } p-1$ but in some order.

$a.1 \cdot a.2 \cdot a.3 \text{ ---- } a(p-1) \equiv 1 \cdot 2 \cdot 3 \text{ ---- } (p-1) \pmod{p}$

$a^{p-1}(p-1)! = (p-1)! \pmod{p}$

$\Rightarrow (p-1)!\{a^{p-1} - 1\} \equiv 0 \pmod{p}$

$\Rightarrow a^{p-1} - 1 \equiv 0 \pmod{p}$

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

Given that,

$a = 7$

$p = 13$

Nilima
ID: IT-21063

We know that, $a^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow 7^{13-1} \equiv 1 \pmod{13}$

$\Rightarrow 7^{13-1} \bmod 13 = 1$

Or, $7^{12} \bmod 13 = 1$

Fermat's Little Theorem plays a vital role in modern cryptography, especially in RSA by enabling secure and efficient modular exponentiation.

Use in RSA algorithm:

RSA encryption and decryption involve raising numbers to large powers modulo n, where $n = P \times Q$. Fermat's theorem helps in two key ways:

1. **Efficiency in computation:**

Instead of directly computing $a^k \bmod P$, Fermat's theorem simplifies calculations using:

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

This helps reduce the exponent modulo $p-1$, making operations faster

2) foundation of Reversibility:

RSA ensures that: $(M^e)^d \equiv M \bmod n$

fermat's theorem guarantees that the decryption operation returns the original message correctly by using properties of mod arithmetic

fermat's theorem contributes to the mathematic backbone of RSA ensuring

- Correctness of encryption/decryption
- Efficient computation
- Resistance to brute force attacks due to large number handling.

Nilima
IT-21063

Q2| Euler Tuotient function: compute $\varphi(n)$ for $n = 35, 45, 100$. Prove that if a and n are are co-prime then $a^{\varphi(n)} \equiv 1 \bmod n$

→ $\varphi(35) = \varphi(7*5)$

$= \varphi(7) * \varphi(5)$

$= 6 \times 4$

$= 24$

$\varphi(45) = \varphi(3^2 \times 5)$

$= \varphi(3^2) \times \varphi(5)$

$= (3^2 - 3^{2-1}) \times 4$

$= (9-3) \times 4 = 24$

3 | 45
3 | 15
5

$3^2 \times 5^1$

$\varphi(100) = \varphi(2^2 \times 5^2)$

$= \varphi(2^2) \times \varphi(5^2)$

$= (2^2 - 2^1) \times (5^2 - 5^1)$

$= (4-2) \times (25-5)$

$= 2 \times 20 = 40$

2 | 100
2 | 50
5 | 25
5 | 5
1

Nilima
IT-21063

Statement: If n is a positive integer and a be any integer relatively prime to n, then,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where ϕ is the Euler ϕ function

Proof: Let $[x]$ denote the residue class of the set of integers mod n. Let $G = [a] : a$ is an integer relatively prime to n

Then we know that w.r.t multiplication of residue classes G is a group of order $\phi(n)$. The identify element of this group be the residue class $[1]$.

We have, $[a] \in G \Rightarrow [a]^{O(G)} \Rightarrow [a]^{\phi(n)} = [1]$

$\Rightarrow [a], [a], [a], \ldots$ up to n times $= [1]$

$\Rightarrow [aa, \ldots$ upto $\phi(n)$ times $] = [1]$

$\Rightarrow [a^{\phi(n)}] = [1]$

$\Rightarrow a^{\phi(n)} = 1 \pmod n$

Q3] solve the system of congruences using the chinese Remainder Theorem and prove that x congruent to 11 on mod $N \equiv 3 \times 4 \times 5 = 60$. $x \equiv 2 \bmod 3x$

$\equiv 3 \bmod 4x \equiv 1 \bmod 5$

→

The chinese Remainder Theorem (CRT) is used to solve a set of different congruent equations with one variable but different module which are relatively prime as shown below:

$X \equiv a_1 \pmod{m_1}$

$X \equiv a_2 \pmod{m_2}$

...

$X \equiv a_n \pmod{m_n}$

CRT that the above equations have a unique solution of the module

Nilima
IT-21063

are relatively prime;

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}) \bmod M$$

$X \equiv 2 \bmod 3$ $\quad X \equiv a_1 \pmod{m_1}$

$X \equiv 3 \bmod 4$ $\quad X \equiv a_2 \pmod{m_2}$

$X \equiv 1 \bmod 5$ $\quad X \equiv a_3 \pmod{m_3}$

$a_1 = 2$, $a_2 = 3$, $a_3 = 1$

$m_1 = 3$, $m_2 = 4$, $m_3 = 5$

$M = m_1 \times m_2 \times m_3$
$= 3 \times 4 \times 5$
$= 60$

$M_1 = \frac{M}{m_1}$
$= \frac{60}{3}$
$= 20$

$M_2 = \frac{M}{m_2}$
$= \frac{60}{4}$
$= 15$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$20 \times 2 = 1 \bmod 3$

$M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$15 \times 3 = 1 \bmod 4$

$M_2^{-1} = 3$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$12 \times M_3^{-1} = 1 \bmod 5$

$12 \times 8 = 1 \bmod 5$

$M_3^{-1} = 8$

Nilima
IT-21063

$M_3 = \frac{M}{m_3}$

$= \frac{60}{5}$

$= 12$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2 \times 20 \times 2 + 3 \times 15 \times 3 + 12 \times 12 \times 8) \bmod 60$

$= (80 + 135 + 96) \bmod 60$

$\equiv 311 \bmod 60$

$= 11$

60) 311 (5
300
11

So, $x \equiv 11 \pmod{60}$

$x = 11$ satisfies all three congruences

Nilima
IT-21063

Q4] find whether 561 is a carmichael number by checking its divisibility and fermat's test

→ The composite number n is a carmichael number if whenever a is relatively prime to n, we have;

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

561 is a carmichael number

i) The prime factorization of 561 is

$561 = 3 \times 11 \times 17$

So, 561 is composite

ii) $a^{560} \equiv 1 \pmod{561}$ if $(a, 561) = 1$

we have, $561 = 3 \times 11 \times 17$

$(a, 561) = 1 \Rightarrow 3 \nmid a$

Similarly, $11 \nmid a \rightarrow (11, a) = 1$ and

$17 \nmid a \rightarrow (17, a) = 1$

Nilima
IT-21063

Now by fermat's theorem,

3 is a prime with $(3, a) = 1$

$\Rightarrow a^{2} = 1 \pmod 3$

$(a^2)^{280} \equiv 1 \pmod 3$

$a^{560} = 1 \pmod 3$ ——(i)

Similarly, 11 is a prime with $(11, a) = 1$

$\rightarrow a^{10} \equiv 1 \pmod{11}$

$\rightarrow (a^{10})^{56} = 1 \pmod{11}$

$a^{560} \equiv 1 \pmod{11}$ ——(ii)

17 is a prime with $(17, a) = 1$

$\rightarrow a^{16} \equiv 1 \pmod{17}$

$(a^{16})^{35} \equiv 1 \pmod{17}$

$a^{560} \equiv 1 \pmod{17}$ ——(iii)

Since 3, 11 and 17 are distint prime and are relatively prime to another, from (i), (ii) and (iii)

Nilima
IT-21063

$a^{560} \equiv 1 \mod (3 \cdot 11 \cdot 17)$

$a^{560} \equiv 1 \pmod{561}$

Thus by definition of carcmichael number 561 is a carcmichael number.

Q5] find a generator (primitive root) of the multiplicative group modulo 17:

Primitive root: A number α is a primitive root modulo n if every number coprime to n is congruent to a power of a modulo n

In a simple sentence,

a is said to be a primitive root of prime number p, if $(a^1 \bmod p, a^2 \bmod p, a^3 \bmod p, a^p \bmod p$ are distinct

Nilima
IT-21063

2 is not a primitive root of modulo 17. Because,

$2^1 = 2 \mod 17$

$= 2$

$2^9 = 512 \mod 17$

$= 2$

$3^1 = 3 \mod 17$

$= 3$

$3^2 = 9 \mod 17$

$= 9$

$3^3 = 27 \mod 17$

$= 10$

$3^4 = 81 \mod 17$

$= 13$

$3^5 = 243 \mod 17$

$= 5$

$3^6 = 729 \mod 17$

$= 15$

$3^7 = 2187 \mod 17$

$= 11$

$3^8 = 6561 \mod 17$

$= 16$

$3^9 = 19683 \mod 17$

$= 14$

$3^{10} = 59049 \mod 17$

$= 8$

$3^{11} = 177147 \mod 17$

$= 7$

Here, 2 is not distinct value, so, 2 is not a primitive root.

Nilima
IT-21063

$3^{12} = 531441 \mod 17$

$= 4$

$3^{13} = 1594323 \mod 17$

$= 12$

$3^{14} = 4782969 \mod 17$

$= 2$

$3^{15} = 14348907 \mod 17$

$= 6$

$3^{16} = 43046721 \mod 17$

$= 1$

So, 3 is a primitive root of modulo 17.

Nilima
IT-21063

Q6] Solve the discrete Logarithm problem: find x such that $3^x \equiv 13 \bmod 17$

→ We can do this by computing the power of 3 modulo 17 until we reach 13.

$3^1 \equiv 3 \bmod 17 = 3$

$3^2 \equiv 9 \bmod 17 = 9$

$3^3 = 27 \bmod 17 = 10$

$3^4 = 81 \bmod 17 = 13$

From the calculation we can see that $3^4 \equiv 13 \bmod 17$

Therefore $x = 4$

Nilima
IT-21063

Q7| Discuss the role of the discrete logarithm in the Diffie-Hellman key exchange.

→ Role of discrete logarithm in Diffie-Hellman key exchange -

1) public parameters : Large prime generator g.

2) key Exchange :
- Alice sends $A = g^a \bmod p$
- Bob sends $B = g^b \bmod p$
- shared key : $g = g^{ab} \bmod p$

3) Discrete Logarithm Problem (DLP):
Hard to find a from $A = g^a \bmod$
• This difficulty ensures security.

4) Attacker's challenge!
• Can not compute shared key without solv DLP.
• DLP is computationally hard for larg

Nilima
IT-21063

Q8| Compare and contrast the substitution ciphers, transposition ciphers and playfair ciphers.

→ 1. Substitution ciphers:

Encryption Mechanism: Each letters is replaced by another letters.

Example: Caesar cipher shifts each letter by fixed number.

Key space: for monoalphabetic: 26! ≈ 40

2) Transposition ciphers:

Encryption Mechanism:

- Letters are rearranged based on a pattern or key.
- No change to actual letters

Nilima
IT-21063

3) Playfair cipher:

Encryption Mechanism:

- Encrypt digraphs (pairs of letters)
- use rules: same row, column or rectangle

Q9| $E(X) = (ax + b) \bmod 26$, $a = 5$, $b = 8$

(a) Encrypt the plaintext "Dept of ICT, MBSTU"

Step A: Encryption

1. Prepocessing the plaintext:
Remove punctuation and spaces, convert to uppercase:
plaintext = "DEPTOFICTMBSTU"

2. Convert letters to numbers
D = 3, E = 4, P = 15, T = 19, O = 14,
F = 5, I = 8, C = 2, T = 19, M = 12, B = 1

Nilima
IT-21063

S=18, T=19, U=20

3)

letter	X	E(X)	cipher
D	3	$(5\times3+8)\%26 = 23$	X
E	4	$(5\times4+8)\%26 = 2$	C
P	15	$(5\times15+8)\%26 = 1$	B
T	19	$(5\times19+8)\%26 = 21$	V
O	14	$(5\times14+8)\%26 = 01$	A
F	5	$(5\times5+8)\%26 = 7$	H
I	8	$(5\times8+8)\%26 = 22$	W
C	2	$(5\times2+8)\%26 = 18$	S
T	19	$(5\times19+8)\%26 = 21$	V

Nilima
IT-21063

M	12	$(5\times12+8)\%26$	Q
		$=16$	
B	1	$(5\times1+8)\%26$	N
		$=13$	
S	18	$(5\times18+8)\%26$	Q
		$=16$	
T	19	$(5\times19+8)\%26$	V
		$=21$	
U	20	$(5\times20+8)\%26$	G
		$=6$	

Step B: Decryption

The decryption function of Affine cipher is:

$$D(j) = a^{-1}(j-b) \bmod 26$$

where $\bar{a}$ is the modular inverse of $a = 5$ modulo 26.

since: $5 \cdot 21 \equiv 105 \equiv 1 \bmod 26 \Rightarrow \bar{a} = 21$

So, the decryption function becomes

Nilima
IT-21063

$D(j) = 21 \cdot (j-8) \bmod 26$

2. Apply decryption on ciphertext:

Ciphertext : XCBVAHWSVQNQVG

Converts letters to numbers:

X=23, C=2, B=1, V=21, A=0, H=7,
W=22, S=18, Q=16, N=13, Q=16, V=21,
G=6

Apply $D(y) = 21(j-8) \bmod 26$:

Letter	y	D(j)	Plain
X	2^3	$21 \times (23-8) \% 26 = 3$	D
C	2	$21 \times (2-8) \% 26 = 4$	E
B	1	$21 \times (1-8) \% 26 = 15$	P
V	21	$21 \times (21-8) \% 26 = 19$	T
A	0	$21 \times (0-8) \% 26 = 14$	O
H	7	$21 \times (7-8) \% 26 = 5$	F
W	22	$21 \times (22-8) \% 26 = 8$	I

Nilima
IT-21063

S	18	$21 \times (18-8) \% 26 = 2$	C
V	21	$21 \times (21-8) \% 26 = 19$	T
Q	16	$21 \times (16-8) \% 26 = 12$	M
N	13	$21 \times (13-8) \% 26 = 1$	B
Q	16	$21 \times (16-8) \% 26 = 12$	S
V	21	$21 \times (21-8) \% 26 = 19$	T
G	6	$21 \times (6-8) \% 26 = 20$	U

Cipher text : XCBUAHWSVQNQUG

Decrypted text : DEPTOFICTMBSTU

Nilima
IT-21063

Q:1 of Design a simple novel cipher.

→

Substitution: Each character is substitution using a keyed caesar shift.

Permutation: Blocks of text are permuted using a PRNG-based shuffle.

PRNG: Custom linear congruential generator

Key

K1: Integer

K2: seed value for PRNG

Block size: fixed Block size

Encryption process:

step 1: substitution:-

Each character c in plain text

Nilima
IT-21063

is shifted forward using a caesare-like method with a varing shift based on the PRNG.

PRNG : $X_{n+1} = (ax_n + c) \bmod m$

Example: Inputs:

plaintext : "Hello"

$K1 = 3$, $K_2 = 7$, Block size = 2

Step 1: substitution

Let's say PRNG gives shifts = [5, 12, 7, 19, 2]

H → H(7) +5+3 = 15 → P
E → E(4) +12+3 = 19 → T
L → L(11) + 7 +3 = 21 → V
L → L(11) + 19 +3 = 33 → H (mod 26)
O → O(14) +2+3 = 19 → T
Substituted : "PTVHT"

Step 2: Permutation (Block size 2)

split : [PT] [VH] [T_]
final ciphertext : "TPHV_T"