Abdus Salam
IT-21016

Q1: Solution:

If p is a prime number and a is an integer such that $\gcd(a, p) = 1$, then

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

The set of integer, $S = \{1, 2, 3, 4, 5, \dots, p-1\}$

multiplying each element by a, modulo p gives:

$$a \cdot S = \{a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)\} \bmod p$$

Since $\gcd(a, p) = 1$, so,

$$a \cdot 1, a \cdot 2 \dots a \cdot (p-1) \equiv 1, 2, \dots, (p-1) \bmod p$$

$$\Rightarrow a^{p-1} \cdot (p-1)! \equiv (p-1)! \bmod p$$

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

$a = 7$, $p = 13$, So, $7^{12} \bmod 13$

- $7^2 = 49$, $7^4 = (7^2)^2 = (49)^2 = 2401$
- $7^4 \bmod 13 = 2401 \bmod 13 = 9$
- $7^{12} = 7^8 \cdot 7^4 = 3 \cdot 9 = 27$
- $27 \bmod 13 = 1$

$$\therefore 7^{12} \equiv 1 \bmod 13$$

CamScanner

Abdus Salam
IT-21016

Format's Little Theorem is the foundation of modular arithmetic in public-key cryptography.

In RSA,

- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$

where $ed \equiv 1 \bmod \phi(n)$. Euler's theorem (generalizing Format's theorem) ensures:

$$M^{\phi(n)} \equiv 1 \bmod n$$

when $\gcd(M, n) = 1$

This ensures correct decryption:

$$M = (M^e)^d = M^{ed} = M \bmod n.$$

Ans.

Abdus Salam

IT-21016

Q-2:

Solution:

Euler's Totient Function $\phi(n)$. The totient function $\phi(n)$ counts the number of integers less than n that are coprime to n. If $n = p_1^{a_1}, p_2^{a_2} \cdots p_k^{a_k}$.

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\cdots\left(1-\frac{1}{p_k}\right)$$

$n = 35 = 3 \times 7$

$$\phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$$

$n = 45 = 3^2 \times 5$

$$\phi(45) = 45\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 45 \cdot \frac{2}{3} \cdot \frac{4}{3} = 24$$

$n = 100 = 2^2 \times 5^2$

$$\cancel{\phi(100)}$$

$$\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

If $\gcd(a,n) = 1$,

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

Let $S = \{x \in Z_n^* \mid \gcd(x,n) = 1\}$. $|S| = \phi(n)$

$$\prod_{x \in S} x \equiv \prod_{x \in S} a \cdot x = a^{\phi(n)} \cdot \prod_{x \in S} x \bmod n$$

$\therefore a^{\phi(n)} \equiv 1 \bmod n$ (proved)

Abdess Salam

IT-21016

Q-3:

Solution:

We are giving the following system of congruences: $x \equiv 2 \mod 3$

$x \equiv 3 \mod 4$

$x \equiv 1 \mod 5$

$N = 3 \times 4 \times 5 = 60$

• $n_1 = 3, n_2 = 4, n_3 = 5$; • $a_1 = 2, a_2 = 3, a_3 = 1$

$N = n_1 \cdot n_2 \cdot n_3 = 60$, $N_i = \frac{N}{n_i}$

$N_1 = \frac{60}{3} = 20$, $N_2 = \frac{60}{4} = 15$, $N_3 = \frac{60}{5} = 12$

$M_i \cdot N_i \equiv 1 \mod n_i$

For, $M_1 \cdot 20 \equiv 1 \mod 3$;

$20 \mod 3 = 2 \Rightarrow M_1 \cdot 2 \equiv 1 \mod 3 \Rightarrow M_1 = 2$

For, $M_2 \cdot 15 \equiv 1 \mod 4$:

$15 \mod 4 = 3 \Rightarrow M_2 \cdot 3 \equiv 1 \mod 4 \Rightarrow M_2 = 3$

For, $M_3 \cdot 12 \equiv 1 \mod 5$:

$12 \mod 5 = 2 \Rightarrow M_3 \cdot 2 \equiv 1 \mod 5 \Rightarrow M_3 = 3$

Abdus Salam
IT-21016

$$x \equiv a_1 \cdot M_1 \cdot N_1 + a_2 \cdot M_2 \cdot N_2 + a_3 \cdot M_3 \cdot N_3 \mod N$$

$$x \equiv 2 \cdot 2 \cdot 20 + 3 \cdot 3 \cdot 15 + 1 \cdot 3 \cdot 12 \mod 60$$

$$x \equiv 80 + 135 + 36 = 251 \mod 60$$

$$x \equiv 251 \mod 60 = 11$$

$\therefore x \equiv 11 \mod 60.$ Ans.

Q-4:

Solution:

n is square-free (not divisible by any square of a prime), For every prime p dividing n, p-1 divides n-1.

561 is not prime, $561 = 3 \times 11 \times 17$

all factors are distinct primes square free and it is composite.

Let's check for all primes $p \in \{3, 11, 17\}$:

- $3 - 1 = 2$, $560 \div 2 = 280$
- $11 - 1 = 10$, $560 \div 10 = 56$
- $17 - 1 = 16$, $560 \div 16 = 35$

CamScanner

Abdus Salam
IT-21016

If n is a Carmichael number, then for any integer a that is coprime to n:

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

$a=2$ $\gcd(2,561)=1$, $2^{560} \bmod 561 = 1$

$a=10$ $\gcd(10,561)=1$, $10^{560} \bmod 561 = 1$

$a=50$ $\gcd(50,561)=1$, $50^{560} \bmod 561 = 1$

This is consistent with known Carmichael behavior.

561 is a Carmichael number.

Q-5:

Solution:

We are looking for a number $g \in \mathbb{Z}_{17}^*$ such that:

$$\{g^1, g^2, \dots, g^{16}\} \bmod 17 \equiv \mathbb{Z}_{17}^* = \{1,2,3,\dots,16\}$$

The multiplicative group modulo 17 has order $\phi(17)=16$ Since 17 is prime.

So, a number g is a primitive root mod 17 if:

$g^k \not\equiv 1 \bmod 17$ for any $1 \le k < 16$,

Abdus Salam
IT-21016

but $g^{16} \equiv 1 \mod 17$.

We will test small integers to see if their powers modulo 17 produce all residuce from 1 to 16. Let, $g = 3$:

Compute powers $3^k \mod 17$ for $k = 1$ to 16.

$k=1$, $3^k \mod 17 \Rightarrow 3^1 \mod 17 = 3$

$k=2$, $3^2 \mod 17 = 9 \mod 17 = 9$

$k=3$, $3^3 \mod 17 = 27 \mod 17 = 10$

$k=4$, $3^4 \mod 17 = 81 \mod 17 = 13$

⋮

$k=14$, $3^{14} \mod 17 = \mod 17 = 2$

$k=15$, $3^{15} \mod 17 = \mod 17 = 6$

$k=16$, $3^{16} \mod 17 = \mod 17 = 1$

All values from 1 to 16 appear.

3 is a primitive root modulo 17.

Other primitive roots mod 17 includes: 3, 5, 6, 7, 10, 11, 12, 14. (Ans.)

Abdus Salam
IT-21016

Q-6:
Solution:

Find x such that:

$$3^x \equiv 13 \mod 17$$

Now, compute powers of 3 modulo 17 until the result is 13.

$x = 1$, $3^x \mod 17 = 3^1 \mod 17 = 3$

$x = 2$, $3^x \mod 17 = 3^2 \mod 17 = 9 \mod 17 = 9$

$x = 3$, $3^x \mod 17 = 3^3 \mod 17 = 27 \mod 17 = 10$

$x = 4$, $3^4 \mod 17 = 3^4 \mod 17 = 81 \mod 17 = 13$

$x = 4$ (Ans)

Since $3^4 = 81 = 13 \mod 17$

(Ans.)

Q-7

Solution:

The Role of the Discrete logarithm in the ~~~~ Diffie-Hellman Key Exchange.

It is a method for two parties to securely

Abdus Salam
IT-21016

share a secret key over an insecure channel.

It uses properties of modular arithmetic and public parameters: A large prime p

A primitive root g (also called a generator)

Each party selects a private key and computes a public key using exponentiation:

Party	Private Key	Public Key
Alice	a	$A = g^a \bmod p$
Bob	b	$B = g^b \bmod p$

They exchange public keys and compute the shared secret. Alice computes: $S = B^a \bmod p = g^{ba} \bmod p$

Bob computes: $S = A^b \bmod p = g^{ab} \bmod p$

They security of Diffie-Hellman depends on the difficultly of solving the Discrete Logarithm Problem:

Given g, p and $g^a \bmod p$, find a.

Abdus Salam
IT-21016

This is called the Discrete Log Problem (DLP), and it is computationally hard when p is large.

So, even if an attacker knows: g, p

$A = g^a \bmod p$, $B = g^b \bmod p$

They cannot compute $g^{ab} \bmod p$ without solving the DLP.

Q-8

Solution: