# Foundation of Cryptography

## Session 14

## Date: 03 March 2021

Dr. V. K. Pachghare

# Number Theory

- Modular Arithmetic
- Euclidean Algorithm
- Prime Numbers
- Fermat's Little Theorem
- Euler Totient Function
- Extended Euclidean Algorithm
- Chinese Remainder Theorem

# Fermat's Theorem

# Fermat’s Theorem

- Fermat’s theorem is one of the most important theorems in cryptography.
- It is also known as Fermat’s Little theorem.
- It is useful in public key encryption techniques and primality testing

# Fermat's Little Theorem

Fermat's theorem states that if $p$ is a prime number and $n$ is a positive integer number which is not divisible by $p$ i.e. $GCD(n, p) = 1$, then

$n^{\mathrm{p}} = n \bmod p$

Therefore, $n^{\mathrm{p}-1} = 1 \bmod p$

$n^{\mathrm{p}-1} \bmod p = 1$

where $p$ is prime and GCD $(n, p) = 1$

Fermat's theorem $n^{\mathrm{p}-1} \bmod p = 1$

Suppose, the prime number $p = 7$ and a positive integer number $n = 3$ then fine the value of $3^6 \bmod 7$.

We apply Modularity Theorem:

$3^6 \bmod 7 = (3^2)^3$

$= (9 \bmod 7)^3 \bmod 7$

$= 2^3 \bmod 7$

$= 8 \bmod 7$

$= 1$

We know that GCD (7, 3) = 1

So, We can apply Fermat's Little theorem: $n^{p-1} \bmod p = 1$

$n = 3$ and $p = 7$ therefore

$3^{7-1} \bmod 7 = 3^6 \bmod 7$

$= 1$

Find the smallest positive residue $y$ in the following congruence.

$$7^{69} = y \bmod 23$$

Here n = 7 and p = 23.

GCD (7, 23) = 1

So, we can apply Fermat's Little theorem to solve this problem.

Here n = 7 and p = 23.

GCD (7, 23) = 1

So, we can apply Fermat's Little theorem to solve this problem.

Fermat's Little theorem is

$$n^{P-1} = 1 \bmod p$$

Or

$$n^{P-1} \bmod p = 1$$

By substituting the values of n and p and rewrite the equation:

$$7^{(23-1)} \bmod 23 = 1$$

$$7^{(22)} \bmod 23 = 1$$

Here n = 7 and p = 23.

GCD (7, 23) = 1

So, we can apply Fermat's Little theorem to solve this problem.

Fermat's Little theorem is

$$n^{P-1} = 1 \bmod p$$

Or $$n^{P-1} \bmod p = 1$$

By substituting the values of n and p and rewrite the equation:

$$7^{(23-1)} \bmod 23 = 1$$

$$7^{(22)} \bmod 23 = 1$$

we can write $7^{69}$ as $(7^{22})^3 * 7^3$

therefore $$7^{69} = y \bmod 23$$

can be written as

$$7^{69} = 7^{66} * 7^3$$

Here n = 7 and p = 23.

GCD (7, 23) = 1

So, we can apply Fermat's Little theorem to solve this problem.

Fermat's Little theorem is

$$n^{P-1} = 1 \bmod p$$

Or

$$n^{P-1} \bmod p = 1$$

By substituting the values of n and p and rewrite the equation:

$$7^{(23-1)} \bmod 23 = 1$$

$$7^{(22)} \bmod 23 = 1$$

we can write $7^{69}$ as $(7^{22})^3 * 7^3$

therefore $7^{69} = y \bmod 23$

can be written as

$$7^{69} = 7^{66} * 7^3$$

$$7^{69} = (7^{22})^3 * 7^3 \bmod 23$$

$$= (1)^3 * 7^3 \bmod 23$$

$$= 343 \bmod 23 = 21$$

Find all solutions of the following congruence

$4x = 8 \bmod 11$

Find all solutions of the following congruence

$$4x = 8 \bmod 11$$

1. Calculate the GCD of 4 and 11.

$$GCD(4, 11) = 1$$

Find all solutions of the following congruence

$$4x = 8 \bmod 11$$

1. Calculate the GCD of 4 and 11.

$$GCD(4, 11) = 1$$

2. As GCD is 1, find the multiplicative inverse of 4 mod 11 we have to find out the value of "n" such that

$$(4\ n) \bmod 11 = 1$$

The multiplicative inverse of 4 mod 11 ($4^{-1} \bmod 11$) is 3.

$$(\text{As } 4 * 3 = 12 \bmod 11 = 1)$$

Find all solutions of the following congruence

$$4x = 8 \bmod 11$$

1. Calculate the GCD of 4 and 11.

$$GCD(4, 11) = 1$$

2. As GCD is 1, find the multiplicative inverse of 4 mod 11

The multiplicative inverse of 4 mod 11 is 3.

3. $4x = 8 \bmod 11$ can be rewritten as $x = 8 \times 4^{-1} \bmod 11$

$$x = 8 * 3 \bmod 11$$

$$x = 2 \bmod 11$$

All the solutions of the given congruence is $x = 2 \bmod 11$.

Compute the value of $12345^{23456789} \bmod 101$.

By Fermat's Little theorem $n^{p-1} = 1 \bmod p$

where $n = 12345$ and $p = 101$.

$$12345^{(101-1)} \bmod 101 = 1$$

$$12345^{100} \bmod 101 = 1$$

Therefore, $12345^{23456789} \bmod 101$

$$= (12345^{100})^{234567} * 12345^{89} \bmod 101$$

$$= 1 * 12345^{89} \bmod 101$$

$$= 12345^{89} \bmod 101$$

But $$12345 \bmod 101 = 23$$

Therefore, $23^{89} \bmod 101$

$$\begin{aligned}
23 \bmod 101 &= 23 \\
23^2 \bmod 101 &= 24 \\
23^3 \bmod 101 &= 47 \\
23^4 \bmod 101 &= 71 \\
23^5 \bmod 101 &= 17 \\
23^7 \bmod 101 &= 4 \\
23^{89} \bmod 101 &= (23^7)^{12}\ 23^5 \bmod 101 \\
&= 4^{12} * 17 \bmod 101 \\
&= 5 * 17 \bmod 101 \\
&= 85
\end{aligned}$$

Therefore, the value of $12345^{23456789} \bmod 101 = 85$.