Foundation of Cryptography

Session 13

Date: 02 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

i) Find 3^{110} mod 13

ii) 7^6 mod 13

iii) 3^{101} mod 57

iv) 13^{670} mod 59

v) 7^{301} mod 23

vi) 7^{119} mod 38

Answers

i. 9
ii. 12
iii. 48
iv. 45
v. 14
vi. 11

Euclidean Algorithm

Greatest Common Divisor (GCD)

- Suppose p and q are two numbers.
- GCD(p, q) is the largest number that divides evenly both p and q.
- Euclidean algorithm is used to compute the greatest common divisor (GCD) of two integer numbers.
- This algorithm is also known called as *Euclid's algorithm*.

GCD(p, q) = GCD(q, p mod q)

Euclid's algorithm to compute GCD(p, q):

n = p, m = q

while m > 0

r = n mod m

n = m, m = r

return n

Compute GCD(7, 38)

n = -- x m + r

38 = 5 × **7** + 3 n = 38 and m = 7

r = n mod m = 38 mod 7 = 3

Compute GCD(7, 38)

$38 = 5 \times 7 + 3$ $\quad$ $n = m = 7,\ m = r = 3$

$7 \ = 2 \times 3 + 1$ $\quad$ $7 \bmod 3 = 1$

Compute GCD(7, 38)

$38 = 5 \times 7 + 3$

$7 = 2 \times 3 + \underline{\mathbf{1}}$ ---------GCD $\qquad$ $n = m = 3;\ \ m = r = 1$

$3 = 3 \text{ x } 1 + 0$

GCD $(7, 38) = 1$ $\qquad$ $m > 0$

Compute GCD(10, 25)

$25 = 2 \times 10 + 5$

$n = 25$ and $m = 10$

$25 \bmod 10 = 5 = r$

Compute GCD(10, 25)

$25 = 2 \times 10 + \underline{\mathbf{5}\text{ ------}\mathbf{GCD}}$

$10 = 2 \times 5 + \mathbf{0}$

GCD $(10, 25) = 5$

Compute GCD(831, 366)

$$831 = 2 \times 366 + 99$$

Compute GCD(831, 366)

$$831 = 2 \times 366 + 99$$

$$366 = 3 \times 99 + 69$$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

$69 = 2 \times 30 + 9$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

$69 = 2 \times 30 + 9$

$30 = 3 \times 9 + 3$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

$69 = 2 \times 30 + 9$

$30 = 3 \times 9 + \mathbf{3}$ **(GCD)**

$9 = 3 \times 3 + \mathbf{0}$

GCD $(831, 366) = 3$

Prime Numbers

- The number which is divisible only by itself and 1 called prime number
- For example: {2, 3, 5, 7, 11, 13, 17, ...}

Prime Factorization

- To factor a number *n* is to write it as a product of other numbers.
- *n = a * b * c*
- Or, 100 = 5 * 5 * 2 * 2
- Prime factorization of a number *n* is writing it as a product of prime numbers.
- 143 = 11 * 13

Relatively Prime Numbers

- Two numbers are called relatively prime if the greatest common divisor (GCD) of those numbers is 1.
- The numbers 8 and 15 are relatively prime number, in respect to each other.
- The factors of 8 are 1, 2, 4, 8 and the factors of 15 are 1, 3, 5 15.
- The Greatest Common Divisor (GCD) of two relatively prime numbers can be determined by comparing their prime factorizations and selecting the least powers.

Contd...

State whether the two numbers 81 and 99 are relatively prime or not?

Contd…

The factors of these numbers are:

81 = 1 * 9 * 9

Contd…

The factors of these numbers are:

$81 = 1 * 9 * 9$

$= 1 * 3 * 3 * 3 * 3$

Contd…

The factors of these numbers are:

$81 = 1 * 9 * 9$

$= 1 * 3 * 3 * 3 * 3$

$= 1 * 3^4$

Contd…

The factors of these numbers are:

$81 = 1 * 9 * 9 = 1 * 3 * 3 * 3 * 3 = 1 * 3^4$

$99 = 1 * 3 * 33 = 1 * 3 * 3 * 11 = 1 * 3^2 * 11$

Contd…

The factors of these numbers are:

$81 = 1 * 9 * 9 = 1 * 3 * 3 * 3 * 3 = 1 * 3^4$

$99 = 1 * 3 * 33 = 1 * 3 * 3 * 11 = 1 * 3^2 * 11$

The GCD is the least power of a number in the factors,

So, $GCD(81, 99) = 1 * 3^2 * 11^0 = 9$

Contd…

The factors of these numbers are:

$81 = 1 * 9 * 9 = 1 * 3 * 3 * 3 * 3 = 1 * 3^4$

$99 = 1 * 3 * 33 = 1 * 3 * 3 * 11 = 1 * 3^2 * 11$

The GCD is the least power of a number in the factors,

So, $GCD(81, 99) = 1 * 3^2 * 11^0 = 9$

If the GCD of two numbers is 1, then those numbers are relatively prime.

GCD(81, 99) is 9

So, 81 and 99 are not relatively prime numbers.

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

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

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

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

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

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

Suppose, the prime number p = 7 and a positive integer number n = 3 then fine the value of 3^6 mod 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:

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

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

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

therefore $7^{69} = y \text{ mod } 23$

can be written as

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

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

$$= (1)^3 * 7^3 \text{ mod } 23$$

$$= 343 \text{ mod } 23 = 21$$

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.

$$\text{GCD}(4, 11) = 1$$

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 $12345^{23456789} \bmod 101 = 85$.