09/02/21

Lecture 8

Topic : Modular Arithmetic & Number Theory

1. GCD
   - Euclid's Algorithm
2. Fermat's Theorem

1

1. GCD = Greatest Common Divisor
   (The largest integer which can divide both a & b)
   a) gcd(a,0) = a
      As 0 is the smallest integer & can't divide
   b) gcd(a,a) = a
      Factors of a are a itself & 1
      Factors of aa are a itself & 1
   c) gcd(a,1) = 1
      Factors of a are 1
      Factors of 1 are 1 itself

2. Modular Arithmetic
   Modular arithmetic is a simple concept of using Remainder when a fact arises in integer division.
   a) Let a, b ∈ Z & n ∈ N,
      then a ≡ b (mod n)
      if (a−b)/n
      where
      Z → Set of integers
      N → Set of natural numbers
   Example:
   23 ≡ 2 (mod 7)
   Congruence calculus is often called as Modular arithmetic. It considers that 23 & 11 mod (12) is equivalent as both are equivalent when divided by 12

   b) If a, b ∈ Z be any integers, then ∃ q, r such that b = aq + r where 0 ≤ r < a
      where q → quotient , r → remainder

   c) Modular Arithmetic exhibits the following properties:
      1) [(a mod n) + (b mod n)] mod n = (a+b) mod n
      2) [(a mod n) − (b mod n)] mod n = (a−b) mod n
      3) [(a mod n) × (b mod n)] mod n = (a×b) mod n

3

Euclidean Algorithm

It is a basic technique or method for calculation of GCD of two positive integers.

Suppose we have 2 integers a, b such that d = gcd(a,b)
Assume a > b > 0

Now dividing a by b, we can state that:

$a = q_1 b + r_1 \quad 0 \le r_1 < b$

Where q_1 → quotient , r_1 → remainder

Suppose that $r_1 \neq 0$ because $b > r_1$, we can divide b by r_1 & apply division to obtain:

$b = q_2 r_1 + r_2 \quad 0 \le r_2 < r_1$

if $r_2 = 0$, then $d = r_1$ & if $r_2 \neq 0$, then $d = \gcd(r_1, r_2)$.

The division process continues till the remainder is 0.

5

Fermat's Theorem

Fermat's Theorem plays an important role in Cryptography. To understand this theorem, one needs to have basic knowledge of GCD, Prime numbers & Prime Factorisation.

Theorem: For any prime number p, 'a' is the integer which is not divisible by p, then

$a^{p-1} \equiv 1 \pmod p \longrightarrow (1)$

A variant of this theorem is:-

If p is a prime no. & a is a coprime to p (i.e gcd(a,p) = 1), then

$a^p \equiv a \pmod p \longrightarrow (2)$

Basically this theorem is useful in public key cryptography such as RSA

Example 2

3. Euclidean Algorithm

Q. Calculate GCD of 54 & 888

Sol: 54) 888 (16 ← Quotient
(888 = Dividend, 54 = Divisor)
54
348
324
24 ← Remainder

If the remainder is less than the divisor, continue the process with the remainder as the new divisor & the old divisor as the dividend

24) 54 (2
48
6) 24 (4
24
0

At some point of time, if we keep on continuing the division, we will eventually get 0 as the remainder.

The divisor for that operation will be the required GCD, i.e 6

Hence, we can show the complete operation as follows:-

888 ⇒ 54(16) + 24

54 ⇒ 24(2) + 6

24 ⇒ 6(4) + 0

This also always

$b = aq + r$

How to Solve Large Mod. Operations

Q.1: $5^{15} \bmod 23$

$5 \bmod 23 = 5$

$\Rightarrow 5^2 \bmod 23 = 25 \bmod 23 = 2$

$\Rightarrow 5^4 \bmod 23 = 4 \bmod 23 = 4$

$\Rightarrow 5^8 \bmod 23 = 16 \bmod 23 = 16$

As $5^{15} = 5^{8+4+2+1}$
$(5^8\ 5^4\ 5^2\ 5^1)$

$\therefore 5^{15} \bmod 23$

$\Rightarrow [(5^8 \bmod 23)(5^4 \bmod 23)(5^2 \bmod 23)(5^1 \bmod 23)] \bmod 23$

$\Rightarrow (16 \times 4 \times 2 \times 5) \bmod 23$

$\Rightarrow (64 \times 10) \bmod 23$

$\Rightarrow (640) \bmod 23$

$\Rightarrow 19$

4

Euclid (x,y)
1. x → x , y → y
2. If y=0 , return x = gcd(x,y)
3. R = x mod y
4. x ← y
5. y ← R
6. Go to Step 2

———— x ————

Q.1: GCD of (40,20)

Sol: We know that :-

$\gcd(x,y) = \gcd(y, x \bmod y)$

$\therefore \gcd(40,20) = \gcd(20, 40 \bmod 20)$

$= \gcd(20,0)$

$\because$ Now y = 0,

if y=0 , return

x = gcd (20,0) = 20

$\therefore$ GCD (40,20) = 20

Q.2: GCD of (36,10)

$\gcd(36,10) \Rightarrow \gcd(10, 36 \bmod 10)$

$\Rightarrow \gcd(10,6)$

$\therefore \gcd(10,6) \Rightarrow \gcd(6, 10 \bmod 6)$

$\Rightarrow \gcd(6,4)$

$\therefore \gcd(6,4) \Rightarrow \gcd(4, 6 \bmod 4)$

$\Rightarrow \gcd(4,2)$

$\therefore \gcd(4,2) \Rightarrow \gcd(2, 4 \bmod 2)$

$\Rightarrow \gcd(2,0)$

$\because y = 0,$

Hence GCD (36,10) = 2

———— x ————

Q.3: GCD of (48,30)

$\gcd(48,30) = \gcd(30, 48 \bmod 30)$

$= \gcd(30,18)$

$\therefore \gcd(30,18) = \gcd(18, 30 \bmod 18)$

$= \gcd(18,12)$

$\gcd(18,12) = \gcd(12, 18 \bmod 12)$

$= \gcd(12,6)$

$\therefore \gcd(12,6) = \gcd(6, 12 \bmod 6)$

$= \gcd(6,0)$

$\therefore$ GCD of 48,30 is 6

———— x ————

Q.4 GCD of 105,80

As $\gcd(105,80) = \gcd(80, 105 \bmod 80)$

$= \gcd(80,25)$

$\therefore \gcd(80,25) = \gcd(25, 80 \bmod 25)$

$= \gcd(25,5)$

$\therefore \gcd(25,5) = \gcd(5, 25 \bmod 5)$

$= \gcd(5,0)$

$\therefore$ GCD (105,80) = 5

6

Examples on Fermat's Theorem

① Let's have a = 3 , p = 5

Eg. 1 & 2 , both are satisfied. So we will test both the equations with these values.

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

$\Rightarrow 3^4 \Rightarrow 81$

$\because 81 \bmod 5 = 1$

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

$\because a^p \equiv a \pmod p$

$\therefore 3^5 \Rightarrow 243$

Also $3 \pmod 5 = 3$

Now, if we take 243 mod 5, it will give same result

$\therefore 243 \equiv 3 \pmod 5$

$\therefore (243) \bmod 5 \equiv (3 \bmod 5) \bmod 5$

$\Rightarrow 3 = 3$ $\therefore$ LHS = RHS

② Solve: $6^{10} \bmod 11$

Sol: Acc. to Fermat's Theorem

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

Hence p − 1 = 10 , a = 6

$\therefore p = 11$

Hence $6^{10} = 1 \bmod 11$

Now, $6^{10} \Rightarrow (6^8 \bmod 11)\ (6^2 \bmod 11) \bmod 11$

$\Rightarrow (4 \times 3) \bmod 11$

$\Rightarrow 1$

$\therefore 6^{10} \bmod 11 = 1$

Q.3 Solve $3^{10} \bmod 11$

Homework Question

$6^2 \bmod 11 = 36 \,\%\, 11 = 3$

$6^4 \bmod 11 = (3)^2 \,\%\, 11 = 9$

$6^8 \bmod 11 = (9)^2 \,\%\, 11 = 81 \,\%\, 11 = 4$