Number Theory

Lecture seven

Assist Prof. Dr. Saja Jasem Mohammed
2025-2024

Prime numbers
Greater Common Divisor
Euler totient function
Multiplicative Inverse

Prime numbers

- Any integer a > 1 can be factored in a unique way as: $a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$

where p1 < p2 < …..<pt are prime numbers and where each ai is a positive integer

$$\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}$$

- A **prime** is a number divisible only by itself and one.
- Prime numbers play a critical role in number theory.

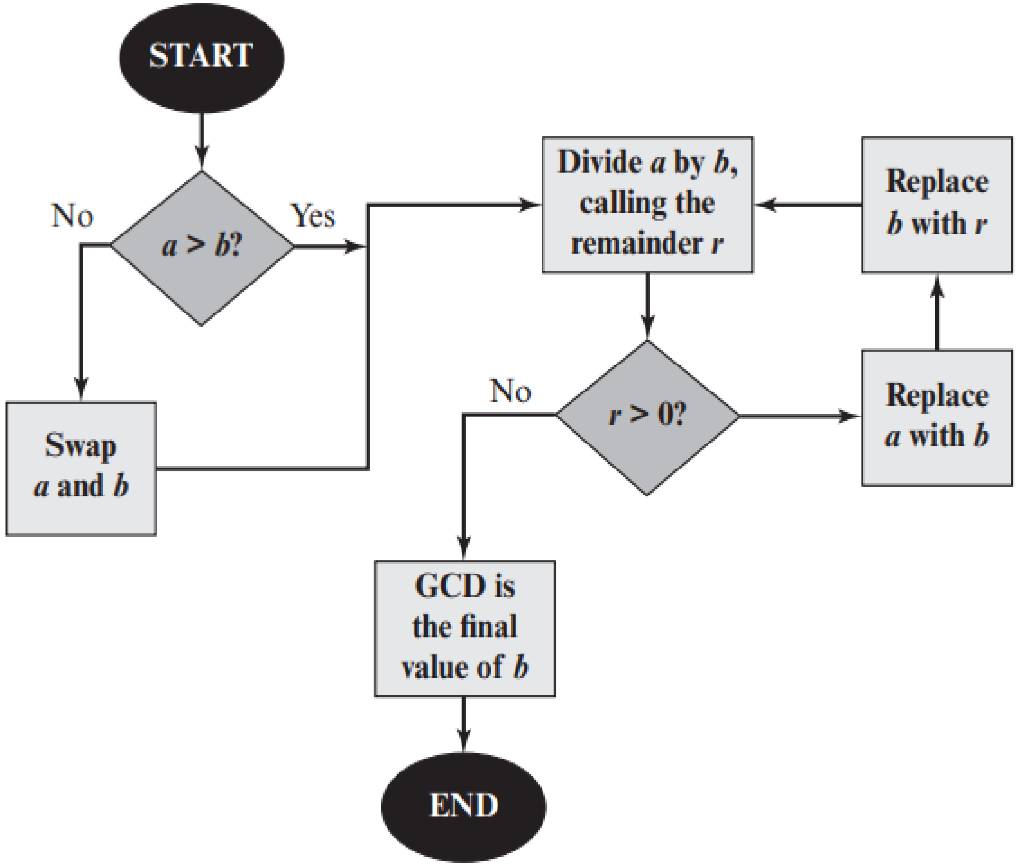
list of prime number less than 200 is: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199.

- Two numbers are said to be **Relatively prime** <u>if their only common positive integer factor is 1(GCD of them is 1 **only**).</u> Ex. (4,13) are relatively prime, where (15,21) are not.
- Many primality test are uses to test the primality of an integer such as **Miller Rabin.**

Greatest Common Divisor (GCD)

- GCD (a,b) of a and b <u>is the largest number that divides evenly into both a and b</u>.
- GCD(60,24) = 12
- The factors of 24 are: 1, 2, 3, 4, 6, 8, 12, 24 The factors of 60 are: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.
- **Euclidean Algorithm** is used to find the GCD between two integers.

The function details:



gcd (a,b)➔ a=x*b+r

Same GCD

GCD GCD

$710 = 2 \times 310 + 90$

$310 = 3 \times 90 + 40$

$90 = 2 \times 40 + 10$

$40 = 4 \times 10$

gcd(710, 310)

- **Examples GCD(33,77), GCD(4,13)**
- **H.W. GCD(244,117)**

Euler's Totient function

This function, written Ø(n), is defined as the number of positive integers less than n and relatively prime to n. By convention, Ø(1) = 1.

Example :

Determine Ø(37) and Ø(35).

1. Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus Ø(37) = 36.
2. To determine Ø(35), we list all of the positive integers less than 35 that are **relatively prime to it**:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34
There are 24 numbers on the list, so Ø(35) = 24

Euler Totient Function ø(n)

Case 1:

(n is prime): ➔ Ø(n)= n-1

Ex.

Ø(37) = (n-1) = (37-1) = 36

Ø(29) = ?

Case 2:

n^r (n is prime) n^{r-1} *(n-1)

Ex.

Ø(9) $=3^2$ ===> (n^{r-1} * (n-1)) = 3^{2-1}*(3-1) = 3*2 = 6

Ø(25) = ?

Euler Totient Function ø(n)

Case 3:

$n=p*q$ (p & q are primes) $(p-1)*(q-1)$

Ex.

Ø(21) = (p-1)*(q-1) = (7–1)x(3–1) = 6*2 = 12

Ø(55) =?

Case 4:

$n=\prod_{i=1}^{t} p_i^{ei}$ (p_i primes) ➔ $Ø(n)=\Pi^{t}_{i=1} p_i^{ei-1} * (p_i-1)$

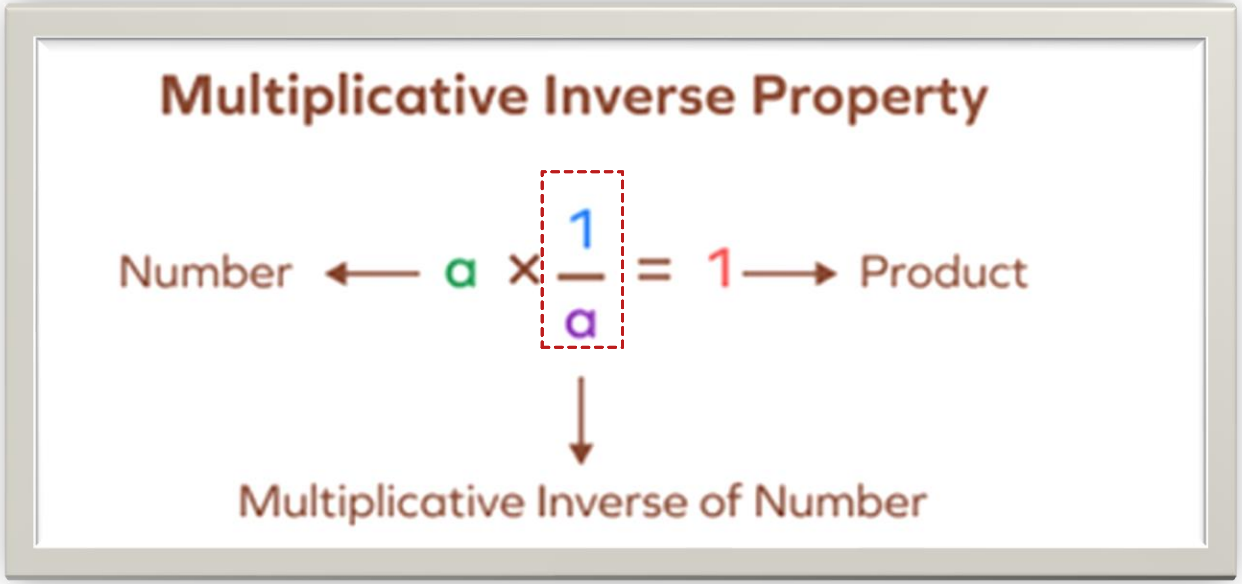
- $Ø(20) = (\Pi^{t}_{i=1} p_i^{ei-1} * (p_i-1)) = 4*5 = 2^2*5^1$

  $= 2^{2-1}*(2-1) * 5^{1-1}*(5-1) = 2 * 4 = 8$

H.W. : Ø(11), Ø(60), Ø(45), Ø(77)

The multiplicative inverse

- In mathematics, a **multiplicative inverse** for a number *x*, denoted by 1/*x* or x^{-1}, <u>is a number which when multiplied by *x* yields the multiplicative identity element, 1.</u>
- where the **additive inverse** for a number *x*, denoted by -*x* , <u>is a number which added to *x* yields the addtive identity element, 0.</u>



The General Method:

- To calculate the multiplicative inverse of any number **(a)** in modulo **(n)** when: (**n** is prime or not prime) and **(GCD(n , a)=1)** then the Inverse X is:

$$\boxed{X = a^{\phi(n)-1} \bmod n}$$

- **Case 1:**
  (n is prime) and (GCD(n , a)=1)

$$4^{-1}\ mod\ 3 = ?$$

If n=3, a=4, find the Inverse?

$X = 4^{\phi(3)-1} \bmod 3$

$X = 4^{2-1} \bmod 3$

$X = 4 \bmod 3$

$X = 1$

$a * X \bmod n = 1$

$4 * 1 \bmod 3 = 1$

$4 \bmod 3 = 1$

Case 2: (**n is even**) and (**GCD(n, a)=1**)

$$3^{-1}\, mod\, 4 = ?$$

If n=4, a=3, find the Inverse?

$X = 3^{ø(4)-1} \bmod 4$

$X = 3^{2-1} \bmod 4$

$X = 3 \bmod 4$

$X = 3$

a * X mod n = 1

3 * 3 mod 4 = 1

9 mod 4 =1

Case 3:

(**n is odd and is not prime**) and (**GCD(n,a)=**1)

$$4^{-1}\, mod\, 9 = ?$$

If n=9, a=4, find the Inverse?

$X = 4^{ø(9)-1} \bmod 9$

$X = 4^{6-1} \bmod 9$

$X = 1024 \bmod 9$

$X = 7$

a * X mod n = 1

4 * 7 mod 9 = 1

28 mod 9=1

Note: not all numbers have an inverse in particular mod.