

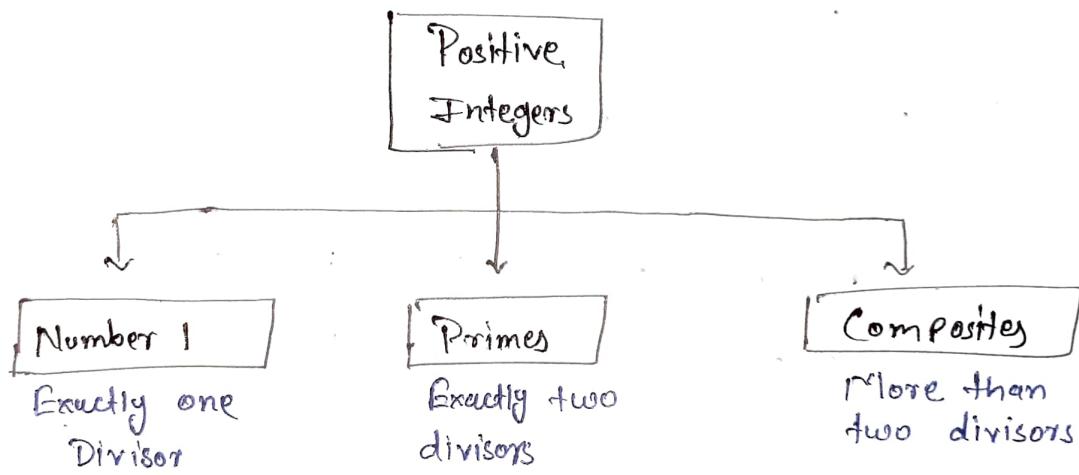
Chapter 9

Mathematics of cryptography

Primes :- Asymmetric - key cryptography uses Primes extensively.

A Positive integers can be divided into 3 groups

- ① number 1;
- ② Primes,
- ③ Composites,



Coprimes or relatively prime :- Two Numbers ~~a, b~~ a, b are coprime if the $\text{gcd}(a, b) = 1$

The number 1 is relatively prime to with any integer.

If P is prime the all the number 1 - P-1 are coprime to P

Z_n^* :- all member of this set is relatively Prime to n.

Checking for Primeness :- If the number 'n' is not divisible by all primes less than \sqrt{n} then 'n' is a prime.

Sieve of Eratosthenes :- This is a method to find all primes less than n.

first we write down all the numbers from 2 to n. & then divide all the numbers by prime numbers less than \sqrt{n} .

Example:- $n=10$ $\sqrt{n}=3\dots$

[Primes = 2, 3]

2 3 4 5 6 7 8 9 10

2, 3, 5, 7 are not divisible by 2 or 3 (except 2, 3)
(2, 3 is already prime)

Euler's Phi function:- Euler's phi function $\phi(n)$, which sometimes called the "Euler's totient function" plays a very important role in cryptography.

This function find the all the ~~all~~ numbers relatively prime to n & smaller then n .

In other word we have to find Z_n^* .
here we find Co-primes count

① The function is:-

$$\textcircled{1} \quad \phi(1) = 0$$

$$\textcircled{2} \quad \phi(p) = p-1 \quad \{ \text{if } p \text{ is prime} \}$$

$$\textcircled{3} \quad \phi(mn) = \phi(m) \times \phi(n) \quad \{ \text{where } m \& n \text{ are relatively prime} \}$$

$$\textcircled{4} \quad \phi(p^e) = p^e - p^{e-1} \quad \{ \text{If } p \text{ is prime} \}$$

NOTE :- The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of n .

Example :- $\phi(13) = 12$ (Rule 2)

$$\phi(10) = \phi(5) \times \phi(2) = 4 \times 1 = 4 \quad (\text{Rule 3})$$

$$\phi(240) = \phi(2^4) \times \phi(3) \times \phi(5)$$

$$= [2^4 - 2^3] \times 2 \times 4$$

$$= 8 \times 8 = 64 \quad (\text{Rule 4})$$

$$\phi(ug) = \phi(7) \times \phi(7) \cdot 36 \quad (\text{wrong way})$$

$$\phi(ug) = 6 \cdot 7^2 - 7 = 42 \quad (\text{Right way})$$

what is the numbers of element in $\mathbb{Z}_{\neq 14}$

$$\phi(14) = \phi(7) \times \phi(2) = 6.$$

Fermat's Little theorem : This theorem plays an important role in cryptography.

We have 2 versions of this theorem.

First version :-

If p is prime & a is any integer & p is not divisible by a , then

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

Second version :-

$$a^p \bmod p \equiv a \bmod p$$

It removes the condition on a .

It is helpful in finding some Exponentiation.

Example: ① $6^{10} \bmod 11 \equiv 1$ (version 1)

$$\begin{aligned} \textcircled{2} \quad 3^{12} \bmod 11 &= (3^{11} \bmod 11 \times 3 \bmod 11) \bmod 11 \\ &= (3 \times 3) \bmod 11 \\ &= 9 \bmod 11 \end{aligned}$$

Multiplicative Inverse :- This theorem is useful in finding the multiplicative inverse very quickly.

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

where p is prime, a is integer & $(p \nmid a)$ p does not divide a .

Prove

$$= (axa^{-1}) \bmod p$$

$$\Rightarrow [a \bmod p \times a^{-1} \bmod p] \bmod p$$

$$= [a \bmod p \times a^{p-2} \bmod p] \bmod p$$

$$= (axa^{p-2}) \bmod p$$

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

$\equiv 1$ (By version 1 of fermat's little theorem)

Example:-

$$8^{-1} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$$

Euler's Theorem: It is a generalized form of fermat's little theorem.

The modulus in the fermat little theorem is a prime. But, the modulus in Euler's theorem is an integer.

Similarly we have 2 versions of this theorem.

first version: This version is similar to first version of fermat little theorem.

$$[(a^{\phi(n)} \bmod n) = 1 \bmod n]$$

where a & n are integers

But a & n must be coprime.

Second version: It is similar to second version of fermat's little theorem. \square

It removes the condition that a & n should be coprime

$$[a^{k \times \phi(n) + 1} \bmod n = a \bmod n]$$

where k is any integer.

Proof :-

$$\therefore a^{K \times \phi(n) + 1} \mod n$$

$$= (a^{\phi(n)} \mod n)^K \times a \mod n$$

$$= 1^K \times a \mod n$$

$$= a \mod n.$$

Example

Example

$$\text{find the result of } 6^{24} \bmod 35$$

$$= 6^{\phi(35)} \bmod 35$$

$$= 1$$

$$\text{find the result of } 20^{62} \bmod 77$$

$$\phi(77) = \phi(7) \times \phi(11)$$

$$= 6 \times 10$$

$$= 60$$

$$= 20^{62} \bmod 77$$

$$= 20^{\phi(77)+2} \bmod 77$$

$$= 20^{\phi(77)} \bmod 77 \times 400 \bmod 77$$

$$= 1 \times 400 \bmod 77$$

$$= 15 \cancel{+}$$

Multiplicative inverses It is useful in finding the multiplicative inverses.

If n & a are coprime then

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

Example

$$8^{-1} \bmod 77 = 8^{60-1} \bmod 77$$

$$= 8^{59} \bmod 77$$

$$= 29 \bmod 77$$

$$= 29 \cancel{+}$$

Generating Primes! Two mathematicians, Mersenne and Fermat, attempted to develop a formula that could generate Primes.

Mersenne Primes!

Mersenne defined the following formula

$$M_p = 2^P - 1$$

If p is prime the M_p was thought to be Prime.

NOTE! But all the number created using this formula is Not Prime.

Example

Example!

$$\begin{aligned} 2^2 - 1 &= 3 \quad (\text{Prime}) \\ 2^3 - 1 &= 7 \\ 2^5 - 1 &= 31 \\ 2^7 - 1 &= 127 \end{aligned}$$

$$2^{11} - 1 = 2047 \quad (\text{Not Prime}) \quad (23 \times 89)$$

Fermat Primes :-

Fermat tried to find a formula to generate Primes. The following is the formula for a Fermat number

$$F_n = 2^{2^n} + 1$$

{ It gives may or may not primes }

He tested F_4 up to F_4
& got F_5 not prime

Primality testing :- The above schemes are failed to generate large prime number.

But we can choose large number & check whether the number is prime or not.

We have 2 types of algorithm for Primality testing:-

- ① Deterministic :- Gives always correct answer
- ② Probabilistic :- This gives correct answer most of the time. But Not all the time.

But Deterministic is less efficient compared to Probabilistic one's.

~~II~~. Deterministic Algorithms:

① Divisibility Algorithm: Divide the given number 'n' with all the primes less than \sqrt{n} . If any of these numbers is able to divide 'n' then 'n' is composite number.

The number of operation is $O(\sqrt{n})$

If we are performing operation on bits then the complexity is $O(2^{n_b/2})$

where n_b = Number of bits in 'n'.

This is Exponential time complexity.

② AKS algorithm: This algorithm says that He is able to find whether the no. is Prime or Not in Polynomial bit operation which is $O((\log_2 n_b)^{12})$

$$(n-a)^p \equiv (n^p - a) \pmod p \quad (\text{This algo. uses this fact})$$

Probabilistic Algorithm! - This algorithm give the prime in polynomial time complexity But it ~~is~~ is guaranteed that it always gives the Right answer.

Rule 1:- If the number is tested is actually a prime. the algorithm definitely returns a prime,

Rule 2:- If the number is composite. Then it returns a composite with probability $1-\epsilon$. But it may return Prime with Probability ϵ .

① Fermat test! - The first Probabilistic method we discuss is the Fermat Primality test

If n is prime then ..
 $a^n \mod n \equiv 1 \mod n$

If n is prime then the relationship hold

It does not mean that, If the congruence hold n is prime.

The integer can be a prime or composite

If n is prime $a^n \mod n \equiv 1 \mod n$

If n is composite , it is possible $a^n \mod n \equiv 1 \mod n$

A composite may pass the fermat test with probability ϵ .

Example: Does the number 561 pass the fermat test?

$$2^{561-1} \equiv 1 \pmod{561}$$

This Number Passes the fermat test but it is not a prime because $561 = 33 \times 17$.

② Square root test:

Before seeing this test, first we have to understand the concept of square root in modulo operation.

$$\text{If } [n^2 \equiv y \pmod{n}]$$

then the square root of y is n in mod n .

Example: find the square root of 4 is mod 5.

We know $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$$1^2 \pmod{5} = 1$$

$$2^2 \pmod{5} = 4$$

$$3^2 \pmod{5} = 4$$

$$4^2 \pmod{5} = 1$$

By above formula 2 & 3 are the square root of 4.

We use this concept for checking prime :-

Given the number 'n'. If it is a prime, then only $1^2 \bmod n = 1$ & $(n-1)^2 \bmod n = 1$. If we are getting 1 at other place, then the given number is not prime.

Example:-

This means that in case of prime the square root of 1 is 1 & $(n-1)$.

But in case of composite we get 0' square root of 1 other than 1 & $(n-1)$.

Example:-

$$n = 5, 7$$

$$\begin{aligned} 1^2 \bmod 5 &= 1 \\ 2^2 \bmod 5 &= 4 \\ 3^2 \bmod 5 &= 4 \\ 4^2 \bmod 5 &= 1 \\ \cancel{5 \bmod 5} &= \end{aligned}$$

$$\begin{aligned} 1^2 \bmod 7 &= 1 \\ 2^2 \bmod 7 &= 4 \\ 3^2 \bmod 7 &= 2 \\ 4^2 \bmod 7 &= 2 \\ 5^2 \bmod 7 &= 4 \\ 6^2 \bmod 7 &= 1 \end{aligned}$$

Square root of 1 is 1 & 3
So it is prime

Square root of 1 is 1 & 6
So 7 is prime

Example $\leftarrow n=8$

$$1^2 \bmod 8 = 1$$

$$2^2 \bmod 8 = 4$$

$$3^2 \bmod 8 = 1$$

$$4^2 \bmod 8 = 0$$

$$5^2 \bmod 8 = 1$$

$$6^2 \bmod 8 = 4$$

$$7^2 \bmod 8 = 1$$

the square root of 1 is 1, 3, 5, 7 other than
 $1 \& n-1$ so 8 is Not prime,

Note! It is Not guarantee that this test work every time,

Example:

$$n=6$$

$$1^2 \bmod 6 = 1$$

$$2^2 \bmod 6 = 4$$

$$3^2 \bmod 6 = 3$$

$$4^2 \bmod 6 = 4$$

$$5^2 \bmod 6 = 1$$

Square root of 1 is

$1 \& n-1$ so according to our test 6 is
Prime But it is Not.

③ Miller-Rabin test :- This test combines the Fermat test and the Square root test in a very elegant way.

Algorithm :-

Step 1 :- Find $n-1 = 2^k \times m$

Step 2 :- Choose 'a' such that $1 < a < n-1$

Step 3 :- Compute $b_0 = b^m \text{ mod } n$.

if $b_0 = 1$ then n is ~~prime~~ composite
else if $b_0 = -1$ then n is probably prime we have to stop here

* But if b_0 is ± 1 then we have to compute

$$b_i = b_{i-1}^2 \text{ mod } m$$

then again we check above conditions.

Example :- Is 561 is prime?

$$n = 561$$

Step 1 :- $n-1 = 2^k \times m$

$$560 = 2^4 \times 35$$

$$k=4, m=35$$

Step 2 :- $a = 2$

Step 3 :- $b_0 = 2^{35} \bmod 561 = 263$

$$b_1 = (263)^2 \bmod 561 = 166$$

$$b_2 = (166)^2 \bmod 561 = 67$$

$$b_3 = (67)^2 \bmod 561 = 1$$

means 561 is Not Prime if it is composite.

Chinese Remainder Theorem

The Chinese Remainder theorem is used to solve a set of congruent equations with one variable but different moduli which are relative prime.

$$n \equiv a_1 \pmod{m_1}$$

$$n \equiv a_2 \pmod{m_2}$$

$$n \equiv a_K \pmod{m_K}$$

$$X = \left(a_1 M_1 m_1^{-1} + a_2 M_2 m_2^{-1} + \dots + a_K M_K m_K^{-1} \right) \pmod{M}$$

$$M = a_1 \times a_2 \times \dots \times a_K$$

$$M_1 = \frac{M}{m_1}$$

$$M_2 = \frac{M}{m_2}$$

$$M_K = \frac{M}{m_K}$$

m_i^{-1} = Multiplicative Inverses of m_i found using Extended Euclidean algorithm.

Note: Solution is possible only when m_1, m_2, \dots, m_K are coprime.

Example 1

(1) $n \equiv 2 \pmod{3}$
 $n \equiv 3 \pmod{5}$
 $n \equiv 2 \pmod{7}$

~~def~~ $a_1 = 2, a_2 = 3, a_3 = 2$
 $m_1 = 3, m_2 = 5, m_3 = 7$

$$M = 3 \times 5 \times 7 = 105$$

$$m_1 = \frac{105}{3} = 35, \quad m_1^{-1} = 2$$

$$m_2 = \frac{105}{5} = 21, \quad m_2^{-1} = 1$$

$$m_3 = \frac{105}{7} = 15, \quad m_3^{-1} = 1$$

$$n = (2 \times 35 \times 2 + \cancel{3 \times 21 \times 1} + 2 \times 15 \times 1) \pmod{105}$$

$$= 233 \pmod{105}$$

$$\boxed{n = 23}$$

Modular Exponentiation ↴

Example 1 ↴ Solve ~~$88^7 \mod 187$~~

$$88^7 \mod 187$$

$$88^1 \mod 187 = 88$$

$$88^2 \mod 187 = 88^1 \times 88^1 \mod 187 = 7744 \mod 187 \\ = 77$$

$$88^4 \mod 187 = (88^2 \times 88^2) \mod 187 = (77 \times 77) \mod 187 \\ = 5929 \mod 187 = 132$$

$$88^7 \mod 187 = (88^4 \times 88^2 \times 88^1) \mod 187 \\ = (132 \times 77 \times 88) \mod 187 \\ = (894432) \mod 187 \\ = 11$$

Example 2 :-

what is the last two digits of $2^9^5 \equiv ?$

or

$$\text{Find } 2^{9^5} \bmod 100$$

$$2^{9^1} \bmod 100 \equiv 2^9$$

$$2^{9^2} \bmod 100 \equiv (2^{9^1} \times 2^9) \bmod 100 \equiv 41$$

$$2^{9^3} \bmod 100 \equiv (2^{9^2} \times 2^9) \bmod 100 \equiv (41 \times 41) \bmod 100 \\ \equiv 1681 \bmod 100 \\ \equiv 81$$

$$2^{9^4} \bmod 100 \equiv (2^{9^3} \times 2^9) \bmod 100 \equiv (81 \times 81) \bmod 100 \\ \equiv 49$$

Example 3 :-

Solve

$$3^{100} \bmod 29$$

$$3^1 \bmod 29 \equiv 3$$

$$3^2 \bmod 29 \equiv 9$$

$$3^3 \bmod 29 \equiv 27 \bmod 29 = 27$$

$$3^4 \bmod$$

Examples :-

$$\text{Solve } 3^{100} \pmod{29}$$

$$3^1 \pmod{29} = 3$$

$$3^2 \pmod{29} = (3^1 \times 3^1) \pmod{29} = 9$$

$$3^4 \pmod{29} = (3^2 \times 3^2) \pmod{29}$$

$$= (9 \times 9) \pmod{29}$$

$$= 81 \pmod{29}$$

$$= 23 \quad 00 - 6$$

$$3^8 \pmod{29} = (3^4 \times 3^4) \pmod{29}$$

$$= (-6 \times -6) \pmod{29}$$

$$= 36 \pmod{29}$$

$$= 7 \quad \cancel{-12}$$

$$3^{16} \pmod{29} = (3^8 \times 3^8) \pmod{29}$$

$$= (7 \times 7) \pmod{29}$$

$$= 49 \pmod{29}$$

$$= 20 \quad \cancel{-19} \text{ or } -9$$

$$3^{32} \pmod{29} = (3^{16} \times 3^{16}) \pmod{29}$$

$$= (-9 \times -9) \pmod{29}$$

$$= 81 \pmod{29}$$

$$= 23 \quad \text{or } -6$$

$$\begin{aligned}
 3^{64} \bmod 29 &= (3^{32} \times 3^{32}) \bmod 29 \\
 &= (-6 \times -6) \bmod 29 \\
 &= 36 \bmod 29 \\
 &= 7 \bmod 29 \\
 &= 7
 \end{aligned}$$

$$\begin{aligned}
 3^{100} &= (3^{64} \times 3^{32} \times 3^4) \bmod 29 \\
 &= (7 \times -6 \times -6) \bmod 29 \\
 &= (7 \times 36) \bmod 29 \\
 &= (7 \times 7) \bmod 29 \\
 &= 49 \bmod 29 \\
 &= 20.
 \end{aligned}$$

Example :- $23^{16} \bmod 30$

$$(-7)^{16} \bmod 30$$

$$(-7)^1 \bmod 30 = -7$$

$$(-7)^2 \bmod 30 = 19 \quad \text{or} \quad -11$$

$$\begin{aligned}
 (-7)^4 \bmod 30 &= ((-7)^2 \bmod 30 \times (-7)^2 \bmod 30) \bmod 30 \\
 &= (-11 \times -11) \bmod 30 \\
 &= 121 \bmod 30
 \end{aligned}$$

$$= 1$$

$$\begin{aligned}
 (-7)^8 \bmod 30 &= ((-7)^4 \times (-7)^4) \bmod 30 \\
 &= 1 \bmod 30
 \end{aligned}$$

$$\begin{aligned}(-7)^{16} \bmod 30 &= ((-7)^8 \bmod 30 \times (-7)^8 \bmod 30) \bmod 30 \\&= (1 \times 1) \bmod 30 \\&= 1\end{aligned}$$

Practice set :-

find the result of following using
fermat's little theorem

① $5^{15} \bmod 13$

② $15^{18} \bmod 17$

③ $456^{17} \bmod 17$

④ $145^{102} \bmod 101$

⑤ $5^{-1} \bmod 13$

⑥ $15^{-1} \bmod 17$

⑦ $27^{-1} \bmod 41$

⑧ $70^{-1} \bmod 101$

find the result of following using
"Euler's theorem".

$$\textcircled{1} \quad 12^{-1} \bmod 77$$

$$\textcircled{2} \quad 16^{-1} \bmod 323$$

$$\textcircled{3} \quad 20^{-1} \bmod 403$$

$$\textcircled{4} \quad 44^{-1} \bmod 667$$