Number Theory UNIT-2

Prime Number

An integer $p>1$ is called a prime number, or prime if its only (+ve) divisors are 1 and p. An integer greater than 1 that is not a prime is called composite.

$n=1$ is neither prime nor composite.

Theorem: If p is a prime and p/ab then p/a or p/b.

Proof: If p/a then nothing to prove.

if $p \nmid a$ and p is prime

$\because$ ~~then~~ $\gcd(p,a) = p$ or $\gcd(p,a)=1$,

$\Rightarrow p/a$ or $p \nmid a$

Since $p/ab \Rightarrow ab = np \quad n \in Z$

$\because \gcd(p,a)=1 \Rightarrow p/b$ (using Euclid's lemma)

$5 \nmid 3$
$\gcd(5,3)=1$
$5/15$

Euclid's Lemma: If a/bc with $\gcd(a,b)=1$ then a/c.

Proof: given $\gcd(a,b)=1 \Rightarrow \exists$ integers x & y s.t

$$ax+by=1 \quad \text{---(1)}$$

now $acx+bcy=c$ $\because$ (1)

given a/bc and trivially a/ac

$\Rightarrow a/(acx+(bc)y \Rightarrow a/c$

$\gcd(p,a)=1$
$\Rightarrow px+ay=1$
$bpx+bay=b$
$\because p/pb, p/ab$
$\Rightarrow p/(pbx+aby)$
$\Rightarrow p/b$ ✓

In general:

If p is a prime and $p/a_1 a_2 \cdots a_k \cdots a_n$ then p/a_k for some k, where $1 \le k \le n$.

Fundamental theorem of arithmetic:

Every positive integer $n>1$ can be expressed as a prod of product of primes. This is unique representation apart from the order in which the factors occur.

Euclid: There is an infinite number of primes.

Let $P_1=2$, $P_2=3$, $P_3=5$, $P_4=7$, ---- be the primes in ascending order and suppose that there is a last prime say P_n. now consider

a positive integer $q = P_1 P_2 \cdots P_n + 1$ —— ①

observe that $q>1$

$\Rightarrow$ q can be written as product of primes

say q is divisible by some prime p.

we assumed the only primes $P_1, P_2, \cdots, P_n$

then p is one of the P_i's, $i=1,2,\cdots,n$.

$\Rightarrow P / P_1 P_2 \cdots P_n$ — ② and P/q — ③

$\Rightarrow P/(q-(P_1 P_2 \cdots P_n))$

$\Rightarrow P/1$ (from ①)

$\Rightarrow\Leftarrow$ (but $P>1$ as p is prime)

our assumption is wrong. hence there is an infinite number of primes.

Miller Rabin Primality Test:

Steps: ①

check if 7 is a prime number?

$n = 7$

① $\boxed{n-1 = 2^s \times d}$ (d is odd no)

$7-1 = 2^5 \times d$

$6 = 2^5 \times d$

$2^1 \times 3 = 2^s \times d$ $\quad s=1,\ d=3$

② $\boxed{x \equiv a^d \bmod n}$ $\quad 2 \le a \le n-2$

$2 \le a \le 7-2$

$2 \le a \le 5$

$\Rightarrow a = 3, 4$

take $a=3$, $x \equiv 3^3 \bmod 7$

$\equiv 27 \bmod 7$

$x = 6$

③ $\boxed{x \equiv \pm 1 \bmod n}$

$6 \equiv \pm 1 \bmod 7$

$6 \equiv 1 \bmod 7$ ✗ , $6 \equiv -1 \bmod 7$ ✓

$\therefore$ $n = 7$ is probably a prime number.

Miller Rabin Algorithm:

① Let $n-1 = 2^s d$ where $d \in N$ and $s \in N$

② choose a random integer a with $2 \le a \le n-2$

③ Compute $x \equiv a^d \pmod n$

if $x \equiv \pm 1 \pmod n$ then n is probably prime.

else ~~s=s+1~~, $x \not\equiv \pm 1 \pmod n$ ~~then~~ and $s=1$ then n is not prime

O.W. set $r=1$ go to step ③

Q.1 Check if $n=15$ is prime number.

$n=15$

① $n-1 = 2^s d \Rightarrow 15-1 = 2^s d \Rightarrow 2^1 \times 7 = 2^s d$

$\therefore (s=1), d=7$

② Choose $2 \le a \le n-2$

$2 \le a \le 13$

say $a=3$

③ $x \equiv a^d \bmod n \Rightarrow x \equiv 3^7 \bmod 15 \equiv 12$

now withthen $x \equiv \pm 1 \bmod n$

$12 \equiv +1 \bmod 15$ ✗

$12 \equiv -1 \bmod 15$ ✗

$\therefore x \not\equiv a^d \bmod n$ but $s=1$, $\therefore n$ is not prime.

Q.2 $n=29$

$n-1 = 2^s d \Rightarrow 28 = 2^s d \Rightarrow 2^2 \times 7 = 2^s d \Rightarrow s=2, d=7$

$x \equiv a^d \bmod n \Rightarrow x \equiv 3^7 \bmod 29 \equiv 2187$

$x \equiv 12$

$2 \le a \le n-2$

$2 \le a \le 27$

$a=3$

now $x \equiv \pm 1 \bmod n$?? $12 \equiv 1 \bmod 29$ ✗

$12 \equiv -1 \bmod 29$ ✗

$\therefore \boxed{x \not\equiv \pm 1 \bmod n}$

now $s=1$? NO $\because s=2$

$\therefore s=2, d=7, a=3$

$r=1, r \le s-1, r = r+1$

for { $a^{2^r \times d} \bmod n \equiv \pm 1 \bmod n \rightarrow$ n is not prime

else $a^{2^r \times d} \bmod n \equiv -1 \bmod n \rightarrow$ n is prime

}

$r=1$, $a^{2d} \bmod n \equiv 3^{2\times 7} \bmod 29 \equiv 3^{14} \bmod 29 \equiv 28 \equiv 1 \bmod 29$ no

$28 \equiv -1 \bmod 29$ yes

$\therefore n=29$ is prime.

Miller Rabin Algorithm (Primality testing)

[1] Let $n-1 = 2^s d$ where $d \in N$, $s \in N$
Choose a random integer a with $2 \le a \le n-2$

[2] Compute $X \equiv a^d \pmod n$

if $X \equiv \pm 1 \bmod n$

then "n is probably a prime"

if $X \not\equiv \pm 1 \bmod n$

check s.

if $s = 1$ then "n is definitely a prime"

if $X \not\equiv \pm 1 \bmod n$ and $s \neq 1$

then go to step ③

[3] Compute $X \equiv a^{2^r d} \pmod n$ — if $X \not\equiv 1 \bmod n$
n is definitely not a prime

if $X \equiv -1 \bmod n$
n is probably a prime.

o.w set $r = r+1$ and
go to step ④

[4] If $r = s-1$, go to step ⑤
o.w go to step ③

[5] Compute $X \equiv a^{2^{s-1} d} \bmod n$

if $X \not\equiv -1 \bmod n$ then n is definitely not a prime

If $X \equiv -1 \bmod n$ then n is probably a prime.

Q $n=61$

$a=3$ $x=60$

Q. check $n=41$ is a prime no.