→ Primality And Factoring

→ Primality test

1) Primality test is a criterian for a number n ~~to~~ not prime. In ~~ca~~ n 'passes' a primality test, then it may be prime. If it passes whole lot of primality test, then it is very likely to be prime. On the other hand, if n fails any single test, then it is definetely compo[site]

→ But it leaves us with very difficult problem: i.e., finding prime factor of n.

→ In General it is much more time-consuming to factor a large number once it is known to be composite (bcz it fails test) than it is to find a prime number of same order of magnitude [Only a statement]

1.) <u>Pseudoprime</u>

→ let n be a large odd integer, and suppose that you want to determine whether or not n is prime.
The simplest primality test is 'trial divisio'

→ This means that you take an odd integer m and see whether or not it divides n. If $m \neq 1$, n and $m | n$, then n is composite; otherwise n passes the primality test "trial division by m".

- As m runs through the odd numbers starting with 3, if n passes all of trial ~~t~~ division test, then it becomes more and more likely that n is prime.
- We know for sure that n is prime, when m reaches $\sqrt{n}$.

-

⇒ ~~A~~

⇒ Acc. to Fermat little Theorem,
if n is prime then for any b such that $\gcd(b, n) = 1$ One has,

$$b^{n-1} \equiv 1 \bmod n \quad \text{--- (1)}$$

→ <u>Definition</u> → If n is an odd composite number and b is an integer such that $\gcd(n, b) = 1$ and (1) holds, then n is called <u>Pseudo prime</u> to the base b.

<u>Ex</u> → : $n = 91$
base, $b = 3$
↳ $3^{90} \equiv 1 \bmod 91$
↳ so $n = 91$ is Pseudoprime to base 3

but if $b = 2$
↳ $3^{90} = 64 \bmod 91$
↳ it is not Pseudoprime to base 2.

⇒ Euler Pseudoprime

→ let n be an odd integer and let $\left(\frac{b}{n}\right)$ denote the Jacobi Symbol.
Now if n is prime then,

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \bmod n \quad \text{——} (2)$$

for any integer b.

⇒ If n is an odd composite number and b is an integer such that $\gcd(n, b) = 1$, and (2) holds, then n is called the <u>Euler Pseudo prime</u> to base b.

⇒ ~~VI.4~~ If n is an Euler pseudoprime to base b then it is a pseudoprime to base b.

To prove ~~this~~ this, we have to show that if (2) holds ~~and~~ then (1) holds.

And this ~~to~~ can be done by simply squaring both sides of congruence (2),

Ex → Converse of above statement is not true.
Suppose $n = 91$ and we know that it is
Pseudoprime to base $b = 3$, However,

we get
for ~~Eurle~~ Eular Pseudoprime; $3^{45} \equiv 27 \mod 91$

So (2) doesn't hold for $n = 91$ & $b = 3$.

Solovay- Strassen Primality test :-

- Suppose n is +ve odd integer, we would like to know whether n is prime or composite.

→ Choose k integers $0 < b < n$ at random
- For each b first compute both sides of

$$b^{(n-1/2)} \equiv \left(\frac{b}{n}\right) \bmod n. \quad -\ (2)$$

It takes $O(\log^3 n)$ time [using repeated squaring method]

It takes $O(\log^3 n)$ time

→ If 2 sides are congruent, the n is composite and test stops.

→ Else move to next b, If (2) holds for all k random choices of b, then probability that n is composite despite passing all tests is at most $(1/2^k)$.

→ Thus, Solovay-Strassen test is a probabili
Algo., which leads to the Conclusion that
'n' is 'composite' or to Conclusion that it is
probably 'prime'.

Ex → $n = 221$ whether n is prime or not?

→ We write $= \frac{(n-1)}{2} = 110$

- We randomly select an b (> 1 & $< n$):
Now we compute,

- $b^{(n-1)/2} \bmod n = 47^{110} \bmod 221$
$= -1 \bmod 221$

- $\left(\frac{b}{n}\right) \bmod n = -1 \bmod 221$

→ Result → Either 221 is prime or b is Euler liar for 221

→ We take $b = 2$,

- $b^{(n-1)/2} \bmod n = 2^{110} \bmod 221$
$= \underbrace{30 \bmod 221}$

- $\left(\frac{b}{n}\right) \bmod n = \left(\frac{2}{221}\right) \bmod n$
$= \underbrace{-1 \bmod 221}$

- Hence we can see that 221 is composite

⇒ Strong Pseudo Prime

- Another type of Primality test, which is in one respect better than Solovay - Strassen test [based on Euler Pseudoprime]

- Suppose n is large +ve odd integer, & $b \in (\mathbb{Z}/n\mathbb{Z})^*$, suppose n is pseudo prime to base b i.e., $b^{n-1} \equiv 1 \bmod n$.

- The idea behind strong Pseudoprime criterion is that, if we successively "extract square roots" of congruence i.e., if we raise b to the,

$((n-1)/2)^{th}$, $((n-1)/4)^{th}$ - $((n-1)/2^s)^{th}$ powers [where $t = \frac{(n-1)}{2^s}$ is odd]

then the first residue class we get other than 1 must be -1 if n is prime, because ± 1 are the ~~oty~~ only square roots of 1 modulo a prime number.

→ In practice, we set $n-1 = 2^s t$ with t = odd, then compute $b^t \bmod n$ then ~~com~~ squaring to get $b^{2t} \bmod n$, then squaring again.. etc. until we get 1 as residue, if we get -1 before it, then it is prime Else, composite.

⇒ let n be an odd composite number, and write $(n-1) = 2^s t$ with t = odd, let $b \in (\mathbb{Z}/n\mathbb{Z})^*$
if n and b satisfy the condn either $b^t \equiv 1 \bmod n$
or
there exists r, $0 \leq r < s$, such that $b^{2^r t} \equiv -1 \bmod n$
then n is called strong pseudoprime to base b.

⇒ Miller-Rabin Primality test :-

→ Suppose $n \Rightarrow$ large +ve odd integer, whether it is prime or composite.

→ We write $(n-1) = 2^s t$ with t = odd and choose a random integer b, $0 < b < n$. First

→ First we compute $b^t \bmod n$,

If, we get ± 1 → it passes test(3) and moves to next b.

Else, we square ($b^t \bmod n$) then square that mod n, and so on, until we get -1.

if (we get -1) → n passes the test,

else if (we never reach -1)

→ n fails the test. and n is Composite.