Primality Testing → To check whether a no. is prime or not.

↳ Fermat's little theorem.

↳ $a^p \bmod p = a$

$a^p \equiv a \pmod{p}$

$a^p \equiv a \pmod{p}$

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

if p is a prime

no.

By using this result

can we do primality testing ??

Fermat's pseudo prime number.

$$\left(2^{340} \bmod 341\right) = 1$$

$p' = 341$

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

$p' \rightarrow$ pseudo prime

341 → Composite →

↳ $341 = 11 \times 31$

* Euclid's lemma, → Consider we have 2 no's x & y then if a prime no. p, divides the product of the 2 no's i.e. $(x \times y) \% p == 0$ then this prime p should completely divide at least one of the given no.s (x & y)

(2×7) % 14 == 0

↳ factorized

(6×12) % 9 == 0

if a composite no. divides $(x \times y)$ completely then it doesn't necessarily divides atleast one of them.

But if we have a prime no, then it cannot be factorised.

Miller Rabin's Primality Testing.

↳ (1) $n = 1$ ⟶ Not a prime

(2) $n = 2$ ⟶ Yes a prime

(3) $(n \% 2 == 0)$ → Not a prime

What is left??

n is odd and $n \geq 3$

Now acc to fermat's little theorem, if n is prime then

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

n → odd

if n is odd, then n-1 is always even.

Any even no. can be represented as

$$d \times 2^s$$

d → odd no.

s → some power of 2

$n-1 = d \times 2^s$ → because $n-1$ is even.

Now, for a random value of a,

$$a^d \bmod n = 1$$

$a^{n-1} \mod n = 1$

$n-1 = d \times 2^s$

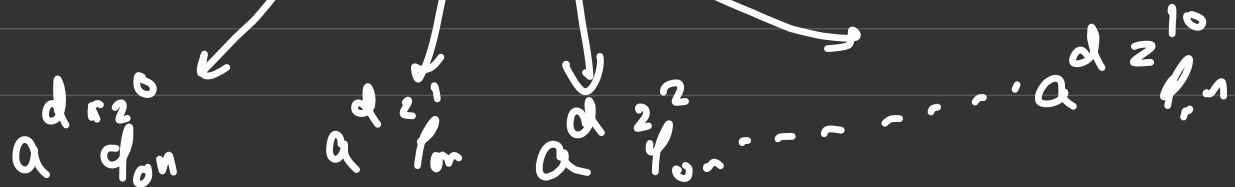
$a^{d \times 2^s} \mod n = 1$

Say, $s = 10$

$a^{d \times 2^{10}} \mod n = 1$

$x \Rightarrow a^{d 2^9}$

$s = 10$



$a^{d z^1}$ $a^{d z^2}$ $a^{d z^3}$ ----

$(a^y)^2$

$a^{d \times 2 \times 2}$

$(a^{2d})^2$

$d = 6$ $s = 2$

$a^{s \times 2 \times 2}$ → $(a^{10})^2$

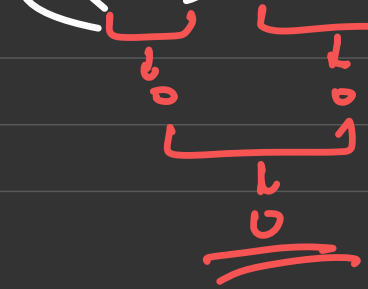
say $a^y = x$

x^2

Now $x^2 \phi(n) = 1$ if n is prime

$(x^2 - 1)\,\phi(n) = 0$

$((x-1)(x+1))\,\phi(n) = 0$



$(x-1)\,q_{on} = 0$

$x\,q_{on} = 1$ — (1)

$a^{d_{2^0}} \dots\dots\dots a^{d_{2^{s-1}}}$

$(x+1)\,q_{on} = 0$

$x\,q_{on} = (-1)$ or $x\,q_{on} = (n-1)$ — (2)

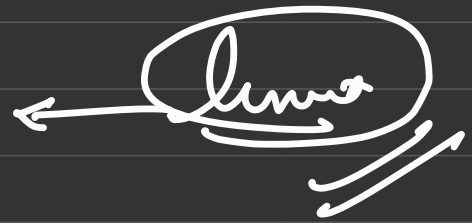
legendre

↳ So for n to be a prime the no.s of the form $a^{d_{2^s}}$ should satisfy the above 2 eq^n s

for some random a $\in [2, n-2]$

Q ∈ Top x prime no.

$x = 9$

$n \rightarrow 3 \times 10^{18}$ ← 

Mobius function

for any positive number, (integer n), we define $\mu(n)$ as the sum of the primitive n^{th} root of unity. It's values are either -1, or 0 or 1