Lecture 17

What we will assume today

- PRIME is in NP (Primality certificate)

(Lehmer's thm).

If ∃a such that

① $a^{n-1} \equiv 1 \pmod{n}$

② ∀ prime factors g of $n-1$,

$$a^{\frac{n-1}{g}} \not\equiv 1 \pmod{n}$$

then n is a prime number.

Verify that $g_1 \dots g_k$ ~~are~~ all prime ~~a com~~ factors of $N-1$

$g_i \mid N-1$

$P(g_1) \dots P(g_k)$

$$\underbrace{N, \underbrace{a}_{①}, \underbrace{(g_1 \dots g_k)}}_{②}$$

$$T(N) = \boxed{\text{polylog}(N) + \sum_{i=1}^{k} T(g_i)} + \cancel{k}.$$

$\leq \text{polylog}(N)$

$\leq \text{polylog} N + \log N \cdot T(\frac{N}{2})$

$\leq \text{polylog} N.$

RSA public key encryption

- Crucially uses the fact that when N = pq, hard to deduce p and q

$$\boxed{221} = \underline{\underline{13}} \times \underline{\underline{17}}$$

Factoring

- $\underline{\text{FACTORING}}$={ ($\underline{N}$, $\underline{L}$, $\underline{U}$) : prime p between L and U such that divides N}

$\exists p$, prime, $L \le p < U$, $p \mid N$.

$(221, \underline{10}, \underline{15}) \in$ FACTORING .

$\parallel$

$\underline{\underline{13}} \times 17$.

$(221, 15, 20) \in$ FA ''

Suppose above is in P, then ?

Supp. FACTORING $\in P$, $\exists$ polytime machine $M_F \leq O(\text{polylog}(N))$ decides Factoring.

$N \rightarrow \boxed{\text{alg}} \rightarrow (p_1, k_1) \; --- \; (p_e, k_e) \rightarrow O(\text{polylog } N)$

such that

① $N = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_e^{k_e}$

② $p_1 \cdots p_e$ are all prime numbers.

$N \rightarrow \boxed{\text{alg}} \rightarrow p$. $\begin{cases} p \text{ is a prime.} \\ p \mid N. \end{cases}$ ✓

Primefactor.

$$O(\log N) * O(\text{polylog}(N)) \leq O(\text{polylog} N)$$

$N \rightarrow$ PRIME FACTOR $\rightarrow p$.

$N = p * \frac{N}{p}$

$\frac{N}{p}$

$O(\log N)$ call to PRIMEFACTOR.

$(N, 2, N) \rightarrow \boxed{M_F}$

Yes $\rightarrow (N, 2, \frac{N}{2})$

$\rightarrow (N, \frac{N}{2}, N)$

No $\rightarrow$ N is a prime. ✓

ask (N, L, U) if $\boxed{\text{YES}}$.

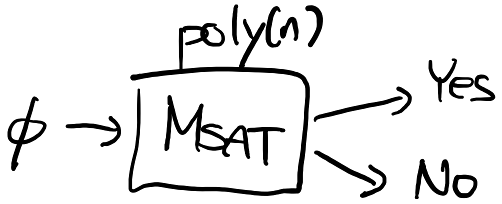
ask $(N, L, L+\frac{U-L}{2})$., ask $(N, L+\frac{U-L}{2}, U)$

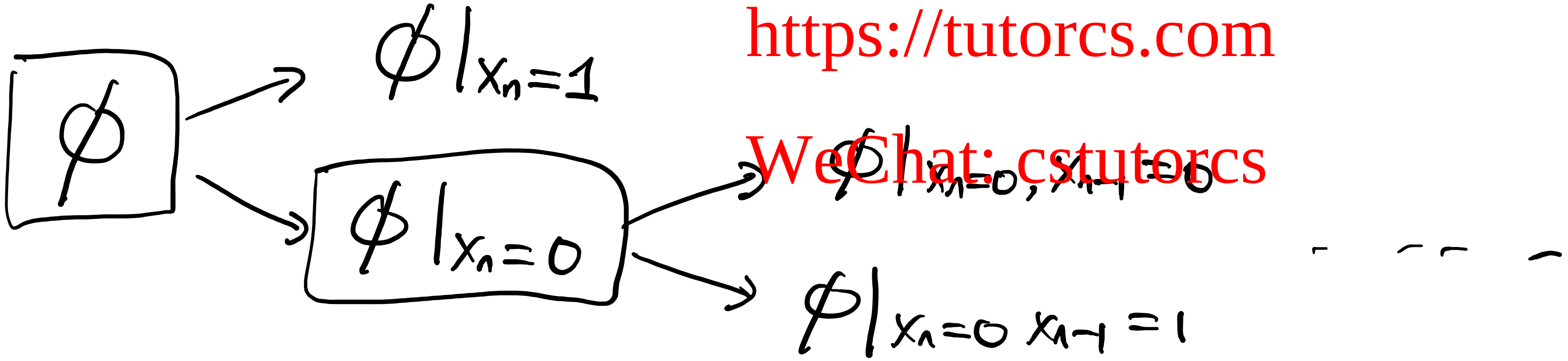
recursively ask on whichever says $\boxed{\text{YES}}$

Similar to finding SAT vs. deciding SAT

$x_1 \ldots x_n$
which satisfies ϕ

ϕ





$O(n) \cdot$

$O(n) \cdot poly(n) = poly(n)$

$\le \log^{c} N$

Why is FACTORING IN coNP ?

- $\overline{\text{FACTORING}} \in NP$. $p_i^{k_i}$ $\sum O(\lg k_i) \approx O(\lg k_1 \dots k_e) \le O(\lg N)$

(N, L, U), $(p_1, k_1) \dots (p_e, k_e)$

① $N = p_1^{k_1} p_2^{k_2} \dots p_e^{k_e}$.

~~$p_i \notin$~~ $\forall i$'s

② p_i's are all prime #.

$p_i \notin [L, U)$

for all i's attach the proof that p_i is a prime.

(N, L, U), $(p_1, k_1) \dots (p_e, k_e)$

$P(p_1)\, P(p_2) \dots P(p_e)$

PRIME $\in$ NP.

$O(\text{polylog}(p_i))$

#of prime(N)

$= \underbrace{\text{\#of prime}(p)}_{1} + \#\left(\frac{N}{p}\right)$

$\le O(\lg N)$

$$\sum_i O(\text{polylog}(p_i)) \le \sum_i \text{polylog}(N) \le \text{polylog}(N)$$

Why is FACTORING IN NP ?

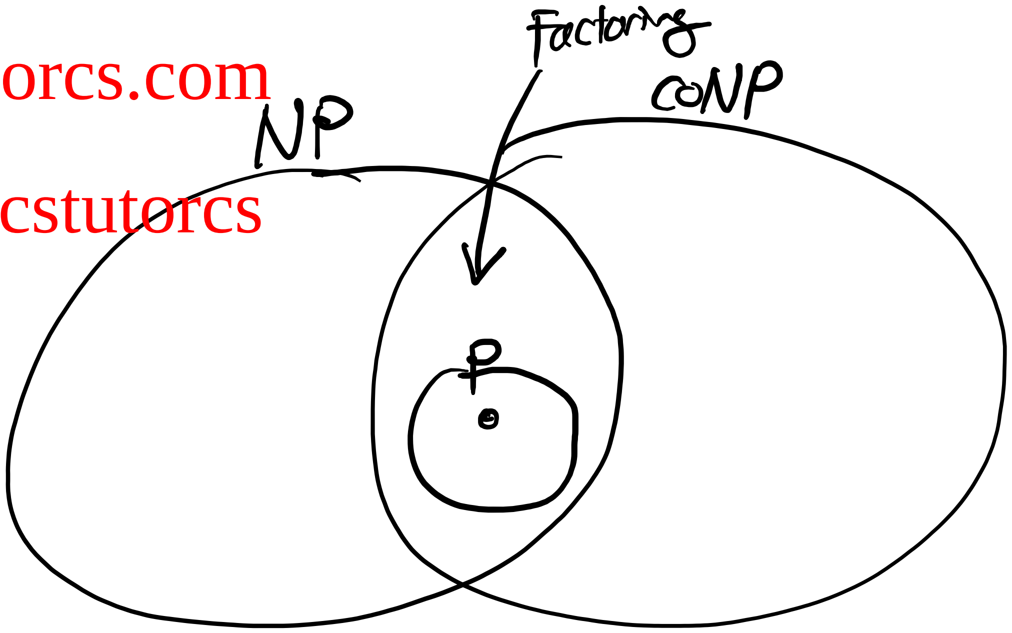
(N, U, L), $\boxed{p}$.

① $L \le p < U$

② $p \mid N$

$\boxed{③\ p \text{ is a prime}}$ attach the proof that p is a prime.

FACTORING ∈ NP.



Why Factoring unlikely to be NP-complete?

If $L \in NP \cap coNP$ then $\bar{L} \in NP \cap coNP$.

- Suppose Factoring is NP-complete, any L in NP reduces to FACTORING

$L \leq_p \underline{FACTORING} \in coNP \Rightarrow NP \subseteq coNP.$

- Any L in coNP reduces to FACTORING as well

$L \leq_p \overline{FACTORING} \in NP. \Rightarrow coNP \subseteq NP.$

- Therefore any language in NP is in coNP, coNP in NP

$NP = coNP.$ → unlikely.

$NP \overset{?}{=} coNP.$

Factoring in Quantum Computer

- Can be done ! (Shor's Algorithm)

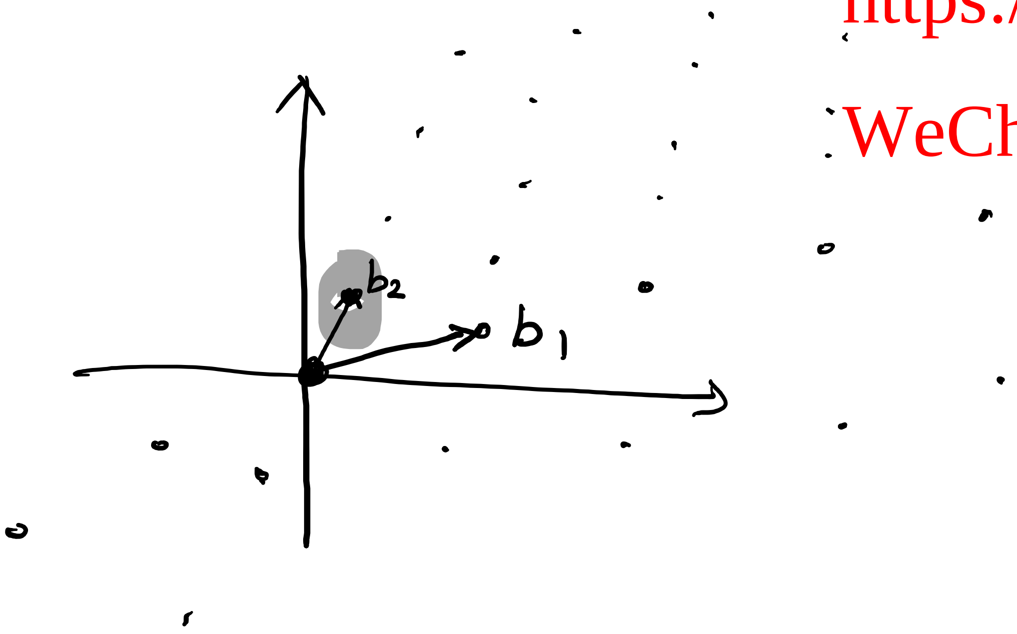
90's .

→ post Quantum Cryptography .

Lattice Problem

- What is a Lattice ? $\mathbb{R}^d$, $B = \{b_1, ..., b_d\}$ linearly independent

$$\mathcal{L}(B) = \left\{ \sum_{l=1}^{d} \alpha_l b_l \mid \alpha_l \in \mathbb{Z} \right\} .$$



Shortest Vector Problem

Given $\mathcal{L}(B)$. find the shortest non-zero vector.

↳ this problem is hard for Quantum Computer.