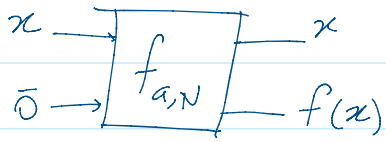
Modular Exponentiation

Tuesday, October 3, 2023 5:24 PM

Modular Exponentiation

1] To compute $f(x) = a^x \pmod N$



Use the repeated squring method

2] Mod-Exponentiation (fast exp)

$f_{a,N}(x) \longrightarrow a^x \bmod N$

Let $x = (d_n\ d_{n-1}\ d_{n-2} \cdots d_1)_2$

1. $f = 1$
2. $p \equiv a \pmod N$
3. For $i = 1$ to n

   if $d_i = 1$

   $f = f * p \pmod N$

   $p = p * p$
4. Return (f)

e.g. $x = 19 = 10011$ (d_i)

$p = a^1$

$p = p \times p = a^2$ ✗

$p = p \times p = a^4$

$p = a^8$

$p = p \times p = a^{16}$ ✗

$f = a^1 \cdot a^2 \cdot a^{16}$

$= a^{19}$

3] e.g. $14^{19} \pmod{11}$

$19 = 10011$

d_i	$f = 1$	$p = 14 \equiv 3$
1	3	9
1	$27 = 5$	4
0	5	$16 \equiv 5$
0	5	$25 \equiv 3$
1	$15 \equiv 4$	9

$f = 4$

F.L.T $a^{p-1} \equiv 1$

14^{19}

$\equiv 3^{10} \cdot 3^{10} \cdot 3^{-1}$

$\equiv 1 \cdot 1 \cdot 3^{-1}$

$\equiv 4$

4] Complexity and number of bits

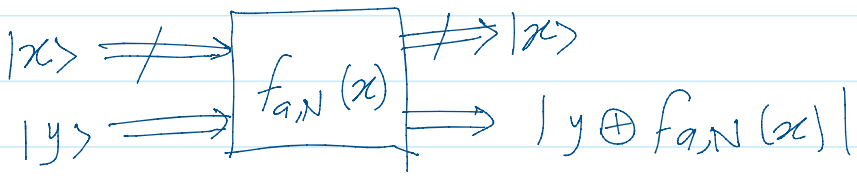
The algorith needs $\log_2(N)$ steps

number of bits $= \log_2(x)$

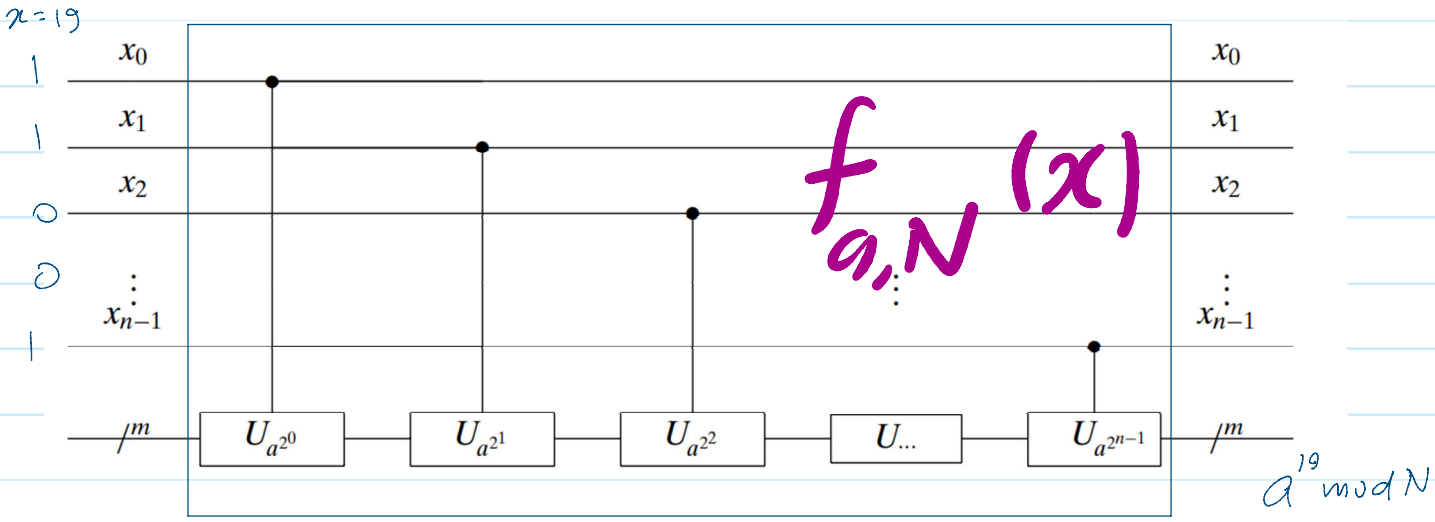
Time complexity is $O(\log N)$

5] Quantum modular exponentiation

$f_{a,N}(x)$



6] Implementation



$a^2 \bmod N$

7] Find the period = $\text{ord}(a)$ in $\mathbb{Z}_N^*$

r ? such that $a^r \equiv 1 \pmod{N}$

8] In this implementation, we need m q-bits for $|x\rangle$ and n q-bits for $|y\rangle$ where

n = number of bits in $N = \log_2(N)$

$m = \log_2(N^2) = 2\log_2 N = 2n.$

To factorize a 1000 bit integer ($\simeq$ 300 digits) we need 3000 q-bits in total.