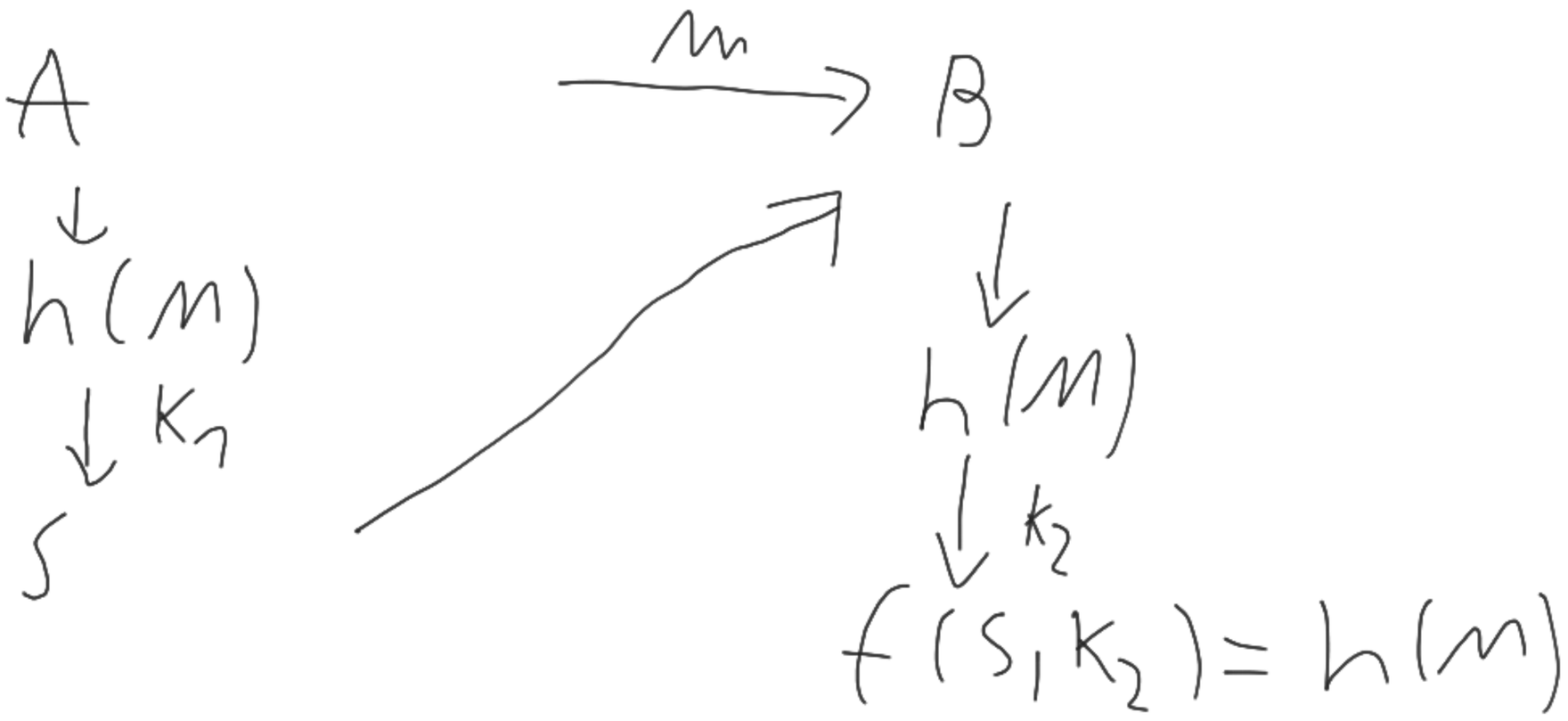
Shor's Algorithm



1. p, q Prime numbers $p = 11$, $q = 17$

2. $n = p \cdot q$ $n = 187$

   $LCM(p-1, q-1)$ $m = 80$

3. $e < m$ $e = 7$

   e doesn't divide m

4. Modular inverse of e w.r.t m. $e \cdot t \bmod m = 1$

   $t = 23$

   $23 \cdot 7 = 161$

   $161 \% 80 = 1$

5. Private Key (n, e)

   Public key (n, e)

Signing: $h^t \bmod n = s$

$h = 5 \Rightarrow 5^{23} \bmod 187 = 180$

Checking: $s^e \bmod n = h$

$180^7 \bmod 187 = 5$

$\Rightarrow$ It is hard to decompose a large number into prime factors

Shor's algorithm: Find factors of n

Find solution to $(x^2 - 1) \bmod n = 0$

$\Rightarrow p = gcd(n, x-1)$

$q = gcd(n, x+1)$

$n = 15 \Rightarrow x = 4 \quad (4^2 - 1) \bmod 15 = 15 \bmod 15 = 0$

$p = gcd(15, 3) = 3$

$q = gcd(15, 5) = 5$

$n = 33 \Rightarrow x = 10$

$p = gcd(33, 9) = 3$

$q = gcd(33, 11) = 11$

$m = a \cdot b + r \quad \Rightarrow m \bmod b = r$

$m // b = a$

1. Pick a : $1 < a < n$

2. $d = \gcd(a, n)$

3. If $d \neq 1 \Longrightarrow$ done

Else: find r : $a^r \bmod n = 1$

r being the smallest positive solution

4. If r odd or $a^{r/2} \bmod n = -1$

$\Longrightarrow$ Back to step 1

5. Solutions: $\gcd(a^{r/2}+1, n)$ and $\gcd(a^{r/2}-1, n)$

Classical

Quantum

$n = 33$ $\quad a = 10 \Rightarrow 10^r \bmod 33 = 1$

$\Rightarrow r = 2$

$\Rightarrow \gcd(11, 33)$

$\gcd(9, 33)$

$a = 17 \Rightarrow r = 10 \Rightarrow a^{r/2} = 32$

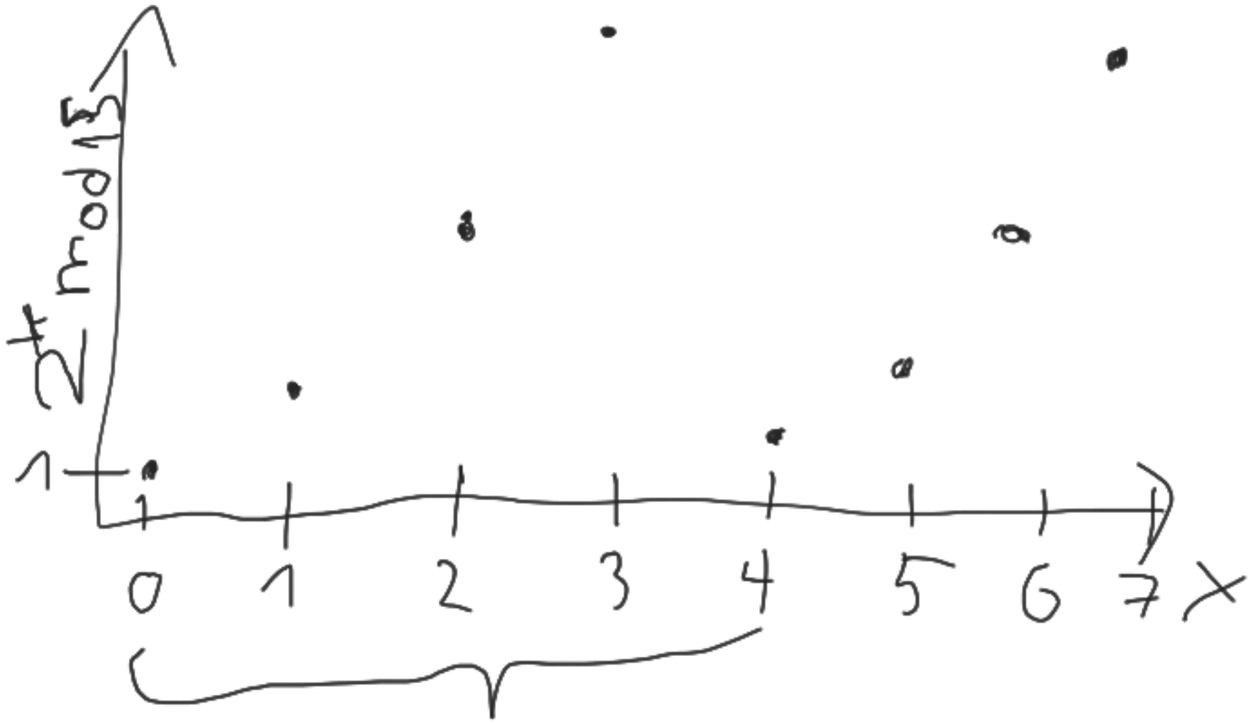
$32 \bmod 33 = -1$

$(32 + 1) \bmod 33 = 33 \bmod 33 = 0$

$\Rightarrow$ No solutions

Find: $a^x \bmod n = 1$

$\Rightarrow$ Period Finding



Period 4

States: $|y\rangle$

Binary: $|0\rangle = |00\rangle$

$|1\rangle = |01\rangle$

$|2\rangle = |10\rangle$

$|3\rangle = |11\rangle$

Unitary operator U

$U|1\rangle = |2\rangle$

$U|2\rangle = |4\rangle$

$U|4\rangle = |8\rangle$

$U|8\rangle = |1\rangle$

$U|y\rangle = |ay \bmod 15\rangle$

Eigenstates of U:

1. $|u_0\rangle = \frac{1}{\sqrt{x}} \sum_{k=0}^{x-1} |a^k \bmod n\rangle$

$$|u_0\rangle = \frac{1}{2}(|1\rangle + |2\rangle + |4\rangle + |8\rangle)$$

2. $|u_m\rangle = \frac{1}{\sqrt{x}} \sum_{k=0}^{x-1} e^{-\frac{2\pi i k m}{x}} |a^k \bmod n\rangle$

$$U|u_m\rangle = e^{\frac{2\pi i m}{x}} |u_m\rangle$$

$$\frac{1}{\sqrt{x}} \sum_{m=0}^{x-1} |u_m\rangle = |1\rangle$$

Quantum Phase Estimation (QPE)

U and Eigenstate $|\psi\rangle$

$U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$

↑ QPE gives us θ

$U|u_m\rangle = e^{2\pi i\frac{m}{x}}|u_m\rangle$ ⇒ QPE gives us $\theta = \frac{m}{x}$

Do QPE $|\eta\rangle$ ⇒ $\theta = \frac{m}{x}$ with random m

$$|\psi_0\rangle = \underbrace{|0\rangle^{\otimes t}}_{\text{counting register}} \otimes |\psi\rangle$$

1. Hadamard on counting register

$$|\psi_1\rangle = \frac{1}{2^{t/2}} (|0\rangle + |1\rangle)^{\otimes t} \otimes |\psi\rangle$$

2. $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle \qquad U^{2^j}|\psi\rangle = e^{2\pi i\theta \cdot 2^j}|\psi\rangle$

Controlled version U

$$cU\left((|0\rangle + |1\rangle) \otimes |\psi\rangle\right) = |0\rangle \otimes |\psi\rangle + e^{2i\pi\theta} |1\rangle \otimes |\psi\rangle$$

cU^{2^j} : for $0 \le j \le t-1$ for each qubit in counting register

$$|\psi_2\rangle = \frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i \theta}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \theta \cdot 2}|1\rangle\right)$$

$$\otimes \ldots \otimes \left(|0\rangle + e^{2\pi i \theta 2^{t-1}}|1\rangle\right) \otimes |\psi\rangle$$

$$= \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \theta k} |k\rangle \otimes |\psi\rangle$$

QFT of $|x\rangle$ with $x = 2^t\theta$

$$\Rightarrow U_{QFT}^{-1} |\psi_2\rangle = \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} \sum_{k=0}^{2^t-1} e^{-\frac{2\pi i k}{2^t} x} e^{\frac{2\pi i k}{2^t}(2^t\theta)}$$

$$= \sum e^{-\frac{2\pi i k}{2^t}(x - 2^t\theta)} \quad |x\rangle \otimes |\psi\rangle$$

← measuring gives $|x\rangle$