PC 5228 Nov. 1, 2023

Outline:

- Order_finding (period of modular exponentiation)
- Shor's algorithm.

▷ Shor's algorithm → Classically transformed into "order-finding" problem
→ apply Quantum order-finding algorithm.

▷ Quantum order-finding algorithm { Quantum Phase Estimation → Inverse QFT
Continuous fractions algorithm

☒ Basics of number theory

(I) • For N integer

① 1

② prime number 2, 3, 5

③ composite number $p \times q$, $p, q \neq 1$

• For any integer N, we have the following decomposition.

$$N = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$ (fundamental theorem of arithmetic)

Example $N = 84$

$$\begin{array}{r|l} 2 & 84 \\ \hline 2 & 42 \\ \hline 3 & 21 \\ \hline & 7 \end{array} \qquad 84 = 2^2 3^1 7^1$$

Seive N check all prime $1 < p \leq \sqrt{N}$

• Factoring: Given $N = pq$, output p, q.

• gcd of N and M

▷ $a|b$ means b is divisible by a

Example $3|9$, $2|8$, ...

▷ Let $a|M$, $a|N$ a is called common divison of M and N, the largest such a is greatest common divisor $\gcd(M,N)$

$$\gcd(M,N)\,|\,M, \quad \gcd(M,N)\,|\,N$$

▷ If $\gcd(M,N)=1$, M, N coprime.

(II) Modular arithmetic (motivation of order-finding)

- Def Given integer $N>1$, called a modulus; two integer a, b are called congruent modulo N, if N is a divisor of their difference

$$N\,|\,(a-b) \text{ (or } \exists \text{ integer } k \text{ such that } a-b=k\cdot N\text{)}.$$

- Congruruence modulo N

$$a \equiv b \pmod N$$

▷ b is the remainder when dividing a by N

▷ Example ① $\frac{28}{5} = 5 \cdots 3$

$$5\times5+3$$

$$28 \equiv 3 \pmod 5$$

$$28-3 = 5\times5$$

② $\frac{19}{3} = 6 \cdots 1$

$$3\times6+1$$

$$19 \equiv 1 \pmod 3$$

- Modular arithmetic

▷ Fix $N>1$ integer, the remaider can only be

$0, 1, \cdots, N-1$

- Fix a, N

  $a \equiv 0 \pmod N$

  $a \equiv 1 \pmod N$

  $\vdots$

  $a \equiv N-1 \pmod N$

- Modular exponentiation
  - motivation:

$2^0 \bmod 7 = 1 \bmod 7,$

$2^1 \bmod 7 = 2 \bmod 7,$

$2^2 \bmod 7 = 4 \bmod 7,$

$2^3 \bmod 7 = 8 \bmod 7 = 1 \bmod 7,$

$2^4 \bmod 7 = 16 \bmod 7 = 2 \bmod 7,$

$2^5 \bmod 7 = 32 \bmod 7 = 4 \bmod 7,$

$2^6 \bmod 7 = 64 \bmod 7 = 1 \bmod 7,$

$2^7 \bmod 7 = 128 \bmod 7 = 2 \bmod 7,$

$2^8 \bmod 7 = 256 \bmod 7 = 4 \bmod 7,$

$\{0, 1, 2, 3, \cdots, 6\} = \mathbb{Z}_7$

<u>Def</u> Fix a and N (modulus), find the smallest $r > 0$ such that $a^r \equiv 1 \pmod N$

This r is called the or or a modulo N.

<u>Remark</u> ① $(\mathbb{Z}_N, +)$ is a group

② $(\mathbb{Z}_N, \cdot)$ is not a group in general.

$\mathbb{Z}_N^{\times}$ is a group of order $\varphi(N)$.

Claim: ① For a, N integers, and a, N comprime, $\gcd(a, N) = 1$.

There always exist an r such that

$a^r \equiv 1 \pmod N$.

② The order of a modulo N must satisfy $1 \leq r \leq N$.

Claim (not crucial for us here):

① Fermat's little theorem : p prime, a is arbitrary integer

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

proof : Group theory

② Generalized Fermat's little theorem : a, N coprime,

then $a^{\varphi(N)} \equiv 1 \pmod N$ ⟿ order of a modulo N must divide $\varphi(N)$

☆ $\varphi(N)$ is the Euler function

the number of positive integers that is coprime with N

Example. ① $\varphi(p) = p-1$

② $\varphi(3) = 2$ $\quad a=1,\ N=3 \quad a=2,\ N=3 \quad \cancel{a=3},\ N=3$

③ $\varphi(10) = 4$

$a=1$	$a=2$	$a=3$	$a=4$	$a=5$	$a=6$
✓	✗	✓	✗	✗	✗

$a=7$	$a=8$	$a=9$	$a=10$
✓	✗	✓	✗

☆ For $N=7$, $a=2$ $\quad \varphi(7) = 6$

$2^6 \equiv 1 \pmod 7$

$$\varphi(N) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1) \qquad N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

↳ • $\varphi(ab) = \varphi(a)\cdot\varphi(b)$ if $\gcd(a,b) = 1$

• modular exponetiation period

▷ Claim : $\left.\begin{array}{l} a \equiv x \pmod N \\ b \equiv y \pmod N \end{array}\right\} \Rightarrow a\cdot b \equiv x\cdot y \pmod N$ ☆ !!!

$a = lN + x$

$b = kN + y$

$a\cdot b = (lN+x)\cdot(kN+y)$

$= klN^2 + lyN + xkN + xy$

▷ $a^0 \equiv x_0 \pmod N$ $\quad x_0 = 1$

$a^1 \equiv x_1 \pmod N$

$\vdots$

$a^{N-1} \equiv x_{N-1} \pmod N$

$a^r \equiv 1 \pmod N$

$a^{\varphi(N)} \equiv 1 \pmod N$ $\quad \Rightarrow \quad r \mid \varphi(N)$

otherwise $\quad \varphi(N) = kr + s \qquad 0 \le s < r$

$$a^{\varphi(N)} \equiv a^{kr} \cdot a^s \equiv 1 \pmod N$$
$$\equiv 1 \cdot a^s \pmod N$$
$$\Rightarrow \quad a^s \equiv 1 \pmod N \quad \text{contradiction.}$$

▷ Claim: there is a period $a^n \pmod N$ for n.
the period is the order r.

Proof: $\quad a^0 \equiv 1 \pmod N \qquad x_0 = 1$

$a^1 \equiv x_1 \pmod N$

$\vdots$

$a^{r-1} \equiv x_{r-1} \pmod N$

$a^r \equiv 1 \pmod N \qquad x_r = 1$

$a^{r+1} \equiv a^r \cdot a^1 \pmod N \equiv x_r \cdot x_1 \equiv x_1$

$a^{r+2} \equiv a^r \cdot a^2 \pmod N \equiv x_r \cdot x_2 \equiv x_2$

$a^{r+3} \equiv \cdots$

$\vdots$

period = order

▨ Quantum order-finding algorithm

(I) Problem: modular exponetiation period-finding problem.

Given a, N such that $\gcd(a, N) = 1$

Find the order r

$$a^r \equiv 1 \pmod N$$

(II) Classical solution:

Repeating square method

- input some n and calculate

$$a^n \equiv x_n \pmod N$$

Difficulty: calculating x_n

- Example. $91 = a$ $N = 131$, $n = 43$

$$91^{43} \equiv x_{43} \mod (131)$$

$$x_{43} = ?$$

$$\begin{aligned}43 &= 101011_2\\ &= 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0\\ &= 1\cdot 32 + 0\cdot 16 + 1\cdot 8 + 0\cdot 4 + 1\cdot 2 + 1\cdot 1.\end{aligned}$$

$$\begin{aligned}91^{43} \bmod 131 &= 91^{1\cdot 32+0\cdot 16+1\cdot 8+0\cdot 4+1\cdot 2+1\cdot 1} \bmod 131\\ &= 91^{1\cdot 32}91^{0\cdot 16}91^{1\cdot 8}91^{0\cdot 4}91^{1\cdot 2}91^{1\cdot 1} \bmod 131\\ &= \left(91^{32}\right)^1\left(91^{16}\right)^0\left(91^{8}\right)^1\left(91^{4}\right)^0\left(91^{2}\right)^1\left(91^{1}\right)^1 \bmod 131\end{aligned}$$

$91^1 \bmod 131 = 91 \bmod 131,$

$91^2 \bmod 131 = 8281 \bmod 131 = 28 \bmod 131,$

$91^4 \bmod 131 = (92^2)^2 \bmod 131 = 28^2 \bmod 131 = 784 \bmod 131 = 129 \bmod 131,$

$91^8 \bmod 131 = (92^4)^2 \bmod 131 = 129^2 \bmod 131 = 16641 \bmod 131 = 4 \bmod 131,$

$91^{16} \bmod 131 = (92^8)^2 \bmod 131 = 4^2 \bmod 131 = 16 \bmod 131,$

$91^{32} \bmod 131 = (92^{16})^2 \bmod 131 = 16^2 \bmod 131 = 256 \bmod 131 = 125 \bmod 131.$

$$\begin{aligned}91^{43} \bmod 131 &= (125)^1(16)^0(4)^1(129)^0(28)^1(91)^1 \bmod 131\\ &= 125\cdot 4\cdot 28\cdot 91 \bmod 131\\ &= 1274000 \bmod 131\\ &= 25 \bmod 131\end{aligned}$$

$$
\begin{aligned}
125 \cdot 4 \cdot 28 \cdot 91 \bmod 131 &= 125(4(28 \cdot 91)) \bmod 131 \\
&= 125(4(2548)) \bmod 131 \\
&= 125(4(59)) \bmod 131 \\
&= 125(236) \bmod 131 \\
&= 125(105) \bmod 131 \\
&= 13125 \bmod 131 \\
&= 25 \bmod 131.
\end{aligned}
$$

(III) Quantum order-finding algorithm.

Procedure: ① Quantum phase estimation $\theta = \frac{s}{r}$

② From phase to obtain the order r via continuous fractions

(a) Map the order into phase

☆ • Unitary operator:

Fix a, N construct a unitary operator $\gcd(a, N) = 1$

$U_{a,N} |y\rangle = |a \cdot y \pmod N\rangle$ $\quad y = 0, \cdots, N-1$

• Exercise: Show that $U_{a,N}$ is unitary

$N=5 \quad a=2$

$|0\rangle \longrightarrow |0\rangle$ $\quad 0$

$|1\rangle \longrightarrow |2\times 1\rangle = |2\rangle$ $\quad 2$

$|2\rangle \longrightarrow |2\times 2\rangle = |4\rangle$ $\quad 4$

$|3\rangle \longrightarrow |2\times 3\rangle = |6\rangle = |1\rangle$ $\quad 1$

$|4\rangle \longrightarrow |2\times 4\rangle = |8\rangle = |3\rangle$ $\quad 3$

one-to-one and orthogonal

Only need to show that $U_{a,N}$ is one-to-one.

▷ To show $U_{a,N}|y_1\rangle \neq U_{a,N}|y_2\rangle$ if $y_1 \not\equiv y_2 \pmod N$

assume that

$$a y_1 \equiv a y_2 \pmod N$$
$$a y_1 - a y_2 \equiv 0 \pmod N$$
$$\Leftrightarrow \quad N \mid a(y_1 - y_2)$$

since $\gcd(N, a) = 1$

$$\Rightarrow N \mid (y_1 - y_2)$$
$$\Leftrightarrow y_1 \equiv y_2 \pmod N$$

- Suppose the order is r

$$\begin{aligned}
U^0|1\rangle &= |1 \bmod N\rangle = |a^0 \bmod N\rangle, \\
U^1|1\rangle &= |a \bmod N\rangle = |a^1 \bmod N\rangle, \\
U^2|1\rangle &= |a^2 \bmod N\rangle, \\
U^3|1\rangle &= |a^3 \bmod N\rangle, \\
&\vdots \\
U^r|1\rangle &= |a^r \bmod N\rangle = |a^0 \bmod N\rangle.
\end{aligned}$$

☆ • Eigenstates of $U_{a,N}$

$$\begin{aligned}
|v_s\rangle &= \frac{1}{\sqrt{r}}\Big(e^{-2\pi i s(0)/r}|a^0 \bmod N\rangle + e^{-2\pi i s(1)/r}|a^1 \bmod N\rangle + \dots \\
&\quad + e^{-2\pi i s(r-2)/r}|a^{r-2} \bmod N\rangle + e^{-2\pi i s(r-1)/r}|a^{r-1} \bmod N\rangle\Big) \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi i s k/r}|a^k \bmod N\rangle.
\end{aligned}$$

eigenvalues : $\exp\left(\frac{2\pi i s}{r}\right)$

$s = 0, 1, \dots, r-1$

Proof :

$$
\begin{aligned}
U|v_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} U \left| a^k \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \Big(e^{-2\pi i s(0)/r} U \left| a^0 \bmod N \right\rangle + e^{-2\pi i s(1)/r} U \left| a^1 \bmod N \right\rangle + \dots \\
&\qquad + e^{-2\pi i s(r-2)/r} U \left| a^{r-2} \bmod N \right\rangle + e^{-2\pi i s(r-1)/r} U \left| a^{r-1} \bmod N \right\rangle \Big) \\
&= \frac{1}{\sqrt{r}} \Big(e^{-2\pi i s(0)/r} \left| a^1 \bmod N \right\rangle + e^{-2\pi i s(1)/r} \left| a^2 \bmod N \right\rangle + \dots \\
&\qquad + e^{-2\pi i s(r-2)/r} \left| a^{r-1} \bmod N \right\rangle + e^{-2\pi i s(r-1)/r} \underbrace{\left| a^r \bmod N \right\rangle}_{\left| a^0 \bmod N \right\rangle} \Big) \\
&= \frac{1}{\sqrt{r}} \Big(e^{-2\pi i s(r-1)/r} \left| a^0 \bmod N \right\rangle + e^{-2\pi i s(0)/r} \left| a^1 \bmod N \right\rangle \\
&\qquad + e^{-2\pi i s(1)/r} \left| a^2 \bmod N \right\rangle + \dots + e^{-2\pi i s(r-2)/r} \left| a^{r-1} \bmod N \right\rangle \Big).
\end{aligned}
$$

Multiplying by $1 = e^0 = e^{2\pi i s/r - 2\pi i s/r} = e^{2\pi i s/r} e^{-2\pi i s/r}$, this becomes

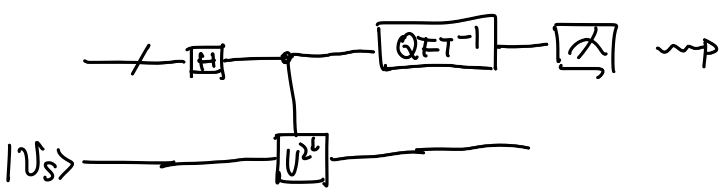
$$
\begin{aligned}
U|v_s\rangle = e^{2\pi i s/r} \frac{1}{\sqrt{r}} \Big(& e^{-2\pi i s(r)/r} \left| a^0 \bmod N \right\rangle + e^{-2\pi i s(1)/r} \left| a^1 \bmod N \right\rangle \\
& + e^{-2\pi i s(2)/r} \left| a^2 \bmod N \right\rangle + \dots + e^{-2\pi i s(r-1)/r} \left| a^{r-1} \bmod N \right\rangle \Big).
\end{aligned}
$$

Note the first coefficient $e^{-2\pi i s(r)/r} = e^{-2\pi i s} = 1$ since s is an integer, and since $e^{-2\pi i s(0)/r} = 1$, the is equation can be written as

$$
\begin{aligned}
U|v_s\rangle &= e^{2\pi i s/r} \frac{1}{\sqrt{r}} \Big(e^{-2\pi i s(0)/r} \left| a^0 \bmod N \right\rangle + e^{-2\pi i s(1)/r} \left| a^1 \bmod N \right\rangle \\
&\qquad + e^{-2\pi i s(2)/r} \left| a^2 \bmod N \right\rangle + \dots + e^{-2\pi i s(r-1)/r} \left| a^{r-1} \bmod N \right\rangle \Big) \\
&= e^{2\pi i s/r} |v_s\rangle.
\end{aligned}
$$

Thus, $|v_s\rangle$ is an eigenvector of U with eigenvalue $e^{2\pi i s/r}$.

(b) phase estimation of $U_{a,N}$, $|v_s\rangle$



$\rightsquigarrow$ $\varphi \simeq \frac{s}{r}$

$0.j_1 \cdots j_n$ binary number.

(c) Obtain the order r from $\varphi = 0.j_1 \cdots j_n \simeq \frac{r}{s}$

continued fractions (approximate arbitrary $\frac{p}{q}$)

$$[a_0, \ldots, a_M] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_M}}}}$$

- 0th order $[a_0] = a_0$
- 1st order $[a_0, a_1] = a_0 + \frac{1}{a_1}$
- 2nd order $[a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2}}$

$\vdots$

- Now, we have $\varphi = 0.j_1 \cdots j_n \simeq \frac{s}{r}$
  To find r, notice that $r < N$
  Find best expression of

$$\varphi = 0.j_1 \cdots j_n = \frac{\tilde{s}}{\tilde{r}} \qquad \tilde{r} < N$$

- Example. $\varphi = 0.1562 = \frac{1562}{10000} = 0 + \frac{1562}{10000}$

$$= 0 + \cfrac{1}{\frac{10000}{1562}}$$

$$= 0 + \cfrac{1}{6 + \frac{628}{1562}}$$

$$= 0 + \cfrac{1}{6 + \cfrac{1}{\frac{1562}{628}}}$$

$$= 0 + \cfrac{1}{6 + \cfrac{1}{2 + \frac{306}{628}}}$$

$$0.1562 = 0 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{19 + \frac{1}{8}}}}}.$$

$$\simeq \frac{s}{r}$$

Now suppose that $N = 7$ we have $r < N$.

$$\text{0th convergent} = [0] = 0,$$

$$\text{1st convergent} = [0,6] = 0 + \frac{1}{6} = \frac{1}{6},$$

$$\text{2nd convergent} = [0,6,2] = 0 + \cfrac{1}{6 + \frac{1}{2}} = \frac{2}{13},$$

$$\text{3rd convergent} = [0,6,2,2] = 0 + \cfrac{1}{6 + \cfrac{1}{2 + \frac{1}{2}}} = \frac{5}{32},$$

$$\text{4rd convergent} = [0,6,2,2,19] = 0 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{19}}}} = \frac{97}{621},$$

$$\text{5th convergent} = [0,6,2,2,19,8] = 0 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{19 + \frac{1}{8}}}}} = \frac{781}{5000}.$$

Shor's algorithm

(I) RSA cryptosystem. (Rivest, Shamir, Adleman)

$N = pq$ Euler function $\varphi(N) = (p-1)(q-1)$

- Choose $e < \varphi(N)$ and $\gcd(e, N) = 1$

  public key (e, N)

- Euler theorem: If $\gcd(x, N) = 1$ $\exists\, y$ such that

  $xy \equiv 1 \pmod N$

- Since $\gcd(e, \varphi(N)) = 1$

  secret key $d = e^{-1}$

  (d, N) $d \cdot e \equiv 1 \pmod{\varphi(N)}$

- encryption: $a^e \equiv b \pmod N$ a is secret message

  decryption: $b^d \equiv a^{ed} \equiv a^{k\varphi(N)+1} \pmod N$

  $\equiv a \pmod N$

If for arbitrary $N = pq$, we can find p, q, then we can directly hack it!! (Shor's algorithm)

(II) Shor's algorithm

- Problem. Input $N = p \cdot q$

  Output p, q

- Shor's algorithm.

  (a) Classically transform the factoring problem into an order-finding prob.

① Pick arbitrary $1 < a < N$.

calculate $\gcd(a, N)$

If : (i) $\gcd(a, N) = p \neq 1$ done!

(ii) $\gcd(a, N) = 1$ step ②

②. Find order of a modulo N.

If : (i) r is odd, go back to step ①

and choose different a

(ii) r is even, calculate $a^{\frac{r}{2}} \pmod N$

$\begin{cases} \text{if " } = N-1 \text{ " go back to step ①} \\ \text{if " } \neq N-1 \text{ " go to step ③} \end{cases}$

The reason will become clear later.

③. r even

$$a^r \equiv 1 \pmod N$$

$$(a^r - 1) \equiv 0 \pmod N$$

$$a^r - 1 = kN = kpq$$

$$(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) = kpq$$

Since p, q are prime numbers,

1. $\underbrace{(a^{r/2}-1)}_{c}\underbrace{(a^{r/2}+1)}_{dpq} = kpq,$

2. $\underbrace{(a^{r/2}-1)}_{cp}\underbrace{(a^{r/2}+1)}_{dq} = kpq,$

3. $\underbrace{(a^{r/2}-1)}_{cpq}\underbrace{(a^{r/2}+1)}_{d} = kpq.$

Since $(a^{\frac{r}{2}} - 1) \not\equiv 0 \pmod N$

$(a^{\frac{r}{2}} + 1) \not\equiv 0 \pmod N$

1 and 3 are impossible

Proof. suppose $(a^{\frac{r}{2}} - 1) \equiv 0 \pmod{N}$

$\Leftrightarrow \quad a^{\frac{r}{2}} \equiv 1 \pmod{N}$

contradiction with the definition of r

suppose $(a^{\frac{r}{2}} + 1) \equiv 0 \pmod{N}$

$\Leftrightarrow \quad a^{\frac{r}{2}} \equiv -1 \pmod{N}$

$\equiv N-1 \pmod{N}$

This is not true because in step ③

we have assume that this in not true.

④ $p = \gcd(a^{\frac{r}{2}} - 1, N)$

$q = \gcd(a^{\frac{r}{2}} + 1, N)$