Quantum Computation

Lectures 15-16

Applications of the quantum Fourier transform

Order-finding quantum subroutine

Modular arithmetic:

Let x, N be positive integers.

x has a (unique) <u>multiplicative</u> <u>inverse</u> modulo N if and only if x and N have no common factor (except 1)

$\gcd(x,N) = 1$

x and N are <u>co-prime</u> or <u>relatively prime</u>.

For x and N co-prime, the <u>order</u> of x mod N is the smallest positive integer r such that $x^r = 1 \pmod N$

$N=5$

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$1 \cdot 1 = 1 \bmod 5$

$2 \cdot 3 = 1 \bmod 5$

$4 \cdot 4 = 1 \bmod 5$

$x=1$; $r=1$

$x=2$; $r=4$

$x=3$; $r=4$

$x=4$; $r=2$

$N=6$

X	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$1 \cdot 1 = 1 \bmod 6$

$5 \cdot 5 = 1 \bmod 6$

	1	5
1	1	5
5	5	1

$x=1$; $r=1$

$x=5$; $r=2$

$Z_N = \{1, 2, \ldots, N-1\}$ ← positive integers modulo N

$Z_N^+ = \{0, 1, 2, \ldots, N-1\}$ ← integers modulo N

$\gcd(x,N) \neq 1 \iff \exists\, n < N$ such that $nx = 0 \pmod N$

x doesn't generate Z_N^+

Z_N^+ is a group under addition modulo N. Any element of Z_N^+ generates a subgroup

$$x,\ 2x,\ 3x,\ \ldots,\ nx = 0 \pmod N \implies nx = kN$$

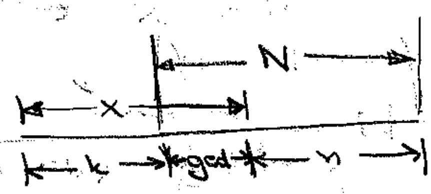
↑ smallest positive n such that $nx = 0 \pmod N$

$$\underbrace{(n-1)}_{\text{additive inverse of } x} x + x = 0 \pmod N$$

$$mx = 0 \pmod N \iff m \text{ is a multiple of } n.$$

N is a multiple of n.

$$\gcd(x,N) = \frac{N}{n} = \frac{x}{k}$$



prime factorization

$n = N,\ x = k$

① If $\gcd(x,N) = 1$, then x generates $Z_N^+ \Rightarrow$ there exists a (unique) m such that $mx = 1 \pmod N$, i.e., x has a (unique) multiplicative inverse modulo N.

② If x has a multiplicative inverse m modulo N, i.e., $mx = 1 \pmod N$, then the subgroup generated by x contains 1. The subgroup generated by 1 is the whole of Z_N^+, which means the subgroup generated by x is Z_N^+, so $\gcd(x,N) = 1$.

The integers x, $1 \le x \le N-1$, such that x is co-prime to N, are a group Z_N^* under multiplication modulo N. The order of the group is denoted $|Z_N^*| \equiv \varphi(N)$.

① $N = p$: All $x = 1, \dots, p-1$ are co-prime to p ($Z_p^* = Z_p$);
$\varphi(p) = p-1$.

② $N = p^\alpha$: All $x = 1, \dots, p^\alpha - 1$ are co-prime to p^α, except multiples of p, i.e., $p, 2p, \dots, (p^{\alpha-1}-1)p$;
$\varphi(p^\alpha) = p^\alpha - 1 - (p^{\alpha-1} - 1) = p^{\alpha-1}(p-1)$.

③ Arbitrary $N = p_1^{\alpha_1} \cdots p_M^{\alpha_M}$; $\varphi(N) = \prod_{j=1}^{M} \varphi(p_j^{\alpha_j}) = \prod_{j=1}^{M} p_j^{\alpha_j - 1}(p_j - 1)$

[Use: a, b co-prime $\Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$]

Any element of Z_N^* generates a subgroup

$$x, x^2, \dots, x^r = 1 \pmod N$$

order of x: smallest positive r such that $x^r = 1 \pmod N$.

$$x^{r-1} = x^{-1} \pmod N$$

$$x^s = 1 \pmod N \iff s \text{ is a multiple of } r.$$

[$x^s \pmod N$ is a periodic fcn. with period r.]
modular exponentiation

$$r = \begin{pmatrix} \text{order of subgroup} \\ \text{generated by } x \end{pmatrix} \Rightarrow r \mid \varphi(N) \le N-1$$

$$\Rightarrow x^{\varphi(N)} = 1 \pmod N$$

In the subgroup $x, x^2, \ldots, x^r = 1 \pmod N$, the arithmetic in the exponent of the modular exponentiation is mod-r addition.

Order of x^n: smallest positive integer s such that $(x^n)^s = 1 \bmod N$. ($s \le r$, ns is a multiple of r); i.e., s is the smallest positive integer such that $ns \equiv 0 \pmod r \Longrightarrow s = \frac{r}{\gcd(n,r)}$.

$N = p$: $x^{p-1} = 1 \pmod p$ for any x not a multiple of p.

$N = p^\alpha$: $x^{p^{\alpha-1}(p-1)} = 1 \pmod p$ for any x not a multiple of p

Fact: $\mathbb{Z}^*_{p^\alpha}$ is a cyclic group; i.e., there exists a generator x that generates the entire group $[r = \varphi(p^\alpha)]$.

We want to find the order of x

For any $x \in Z_N^*$, $Z_N^+ = \{0, 1, \ldots, N-1\}$ divides up into <u>disjoint</u> equivalence classes $\{x^k y \ (\mathrm{mod}\ N),\ k = 1, \ldots, r\}$.
If $y \in Z_N^*$, you get a coset of the subgroup generated by x, containing r members; if $y \notin Z_N^*$, you get a class whose number of members, $\bar{r}$, divides r.

$x^{\bar{r}} y = y \ (\mathrm{mod}\ N)$ ← smallest
$x^r y = y \ (\mathrm{mod}\ N)$

Put this in Hilbert space:

$$U_x|y\rangle \equiv \begin{cases} |xy \ (\mathrm{mod}\ N)\rangle, & y = 0, \ldots, N-1, \\ |y\rangle & , y = N, \ldots, 2^L - 1. \end{cases}$$

$L = \lceil \log N \rceil = \begin{pmatrix}\text{size of} \\ \text{problem}\end{pmatrix}$

U_x unitary: $xy = xy' \ (\mathrm{mod}\ N) \Rightarrow y = y' \ (\mathrm{mod}\ N)$
(x has an inverse)

Each equivalence class forms a cycle under U_x.

Eigenstates of U_x:

$$|u_s\rangle = \frac{1}{\sqrt{\bar{r}}} \sum_{k=0}^{\bar{r}-1} e^{-2\pi i ks/\bar{r}} |x^k y \ (\mathrm{mod}\ N)\rangle, \quad s = 0, \ldots, \bar{r}-1$$

$$U_x|u_s\rangle = \frac{1}{\sqrt{\bar{r}}} \sum_{k=0}^{\bar{r}-1} e^{-2\pi i ks/\bar{r}} |x^{k+1} y \ (\mathrm{mod}\ N)\rangle$$

$$= \frac{1}{\sqrt{\bar{r}}} \sum_{k=0}^{\bar{r}-1} e^{-2\pi i (k-1)s/\bar{r}} |x^k y \ (\mathrm{mod}\ N)\rangle$$

$$= e^{2\pi i s/\bar{r}} |u_s\rangle$$

$N = 15$: $\mathbb{Z}_N^*$ contains 1, 2, 4, 7, 8, 11, 13, 14

$x = 2$

$k =$	1	2	3	4 (0)	
$1x^k$:	2	4	8	1	$(r = 4)$
$7x^k$:	14	13	11	7	
$0x^k$:	0	0	0	0	
$3x^k$:	6	12	9	3	
$5x^k$:	10	5	10	5	

$x = 8$ gives same classes

$U_2|1\rangle = |2\rangle$
$U_2|2\rangle = |4\rangle$
$U_2|4\rangle = |8\rangle$
$U_2|8\rangle = |1\rangle$

Eigenstates: $\frac{1}{2}(|1\rangle + |2\rangle + |4\rangle + |8\rangle)$ 1

$\frac{1}{2}(|1\rangle - i|2\rangle - |4\rangle + i|8\rangle)$ i

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

$\frac{1}{2}(|1\rangle + i|2\rangle - |4\rangle - i|8\rangle)$ $-i$

$U_2|5\rangle = |10\rangle$
$U_2|10\rangle = |5\rangle$

Eigenstates: $\frac{1}{\sqrt{2}}(|5\rangle + |10\rangle)$ $+1$

$\frac{1}{\sqrt{2}}(|5\rangle - |10\rangle)$ -1

$x = 4$

$k =$	1	2 (0)	
$1x^k$:	4	1	$(r = 2)$
$2x^k$:	8	2	
$7x^k$:	13	7	
$11x^k$:	14	11	
$0x^k$:	0	0	
$3x^k$:	12	3	
$6x^k$:	9	6	
$5x^k$:	5	5	
$10x^k$:	10	10	

U_4 does 2-cycles

U_4 does 1-cycles

$x = 7$

k	1	2	3	4	
$1x^k$:	7	4	13	1	$(r = 4)$
$2x^k$:	14	8	11	2	
$0x^k$:	0	0	0	0	
$3x^k$:	6	12	9	3	
$5x^k$:	5	5	5	5	
$10x^k$:	10	10	10	10	

$x = 13$ gives same classes

$x = 11$ (r = 2)

	k = 1	2
$1x^k$:	11	1
$2x^k$:	7	2
$4x^k$:	14	4
$8x^k$:	13	8
$0x^k$:	0	0
$3x^k$:	3	3
$5x^k$:	10	5
$6x^k$:	6	6
$9x^k$:	9	9
$12x^k$:	12	12

$x = 14$ (r = 2)

	k = 1	2
$1x^k$:	14	1
$2x^k$:	13	2
$4x^k$:	11	4
$7x^k$:	8	7
$0x^k$:	0	0
$3x^k$:	12	3
$5x^k$:	10	5
$9x^k$:	6	9

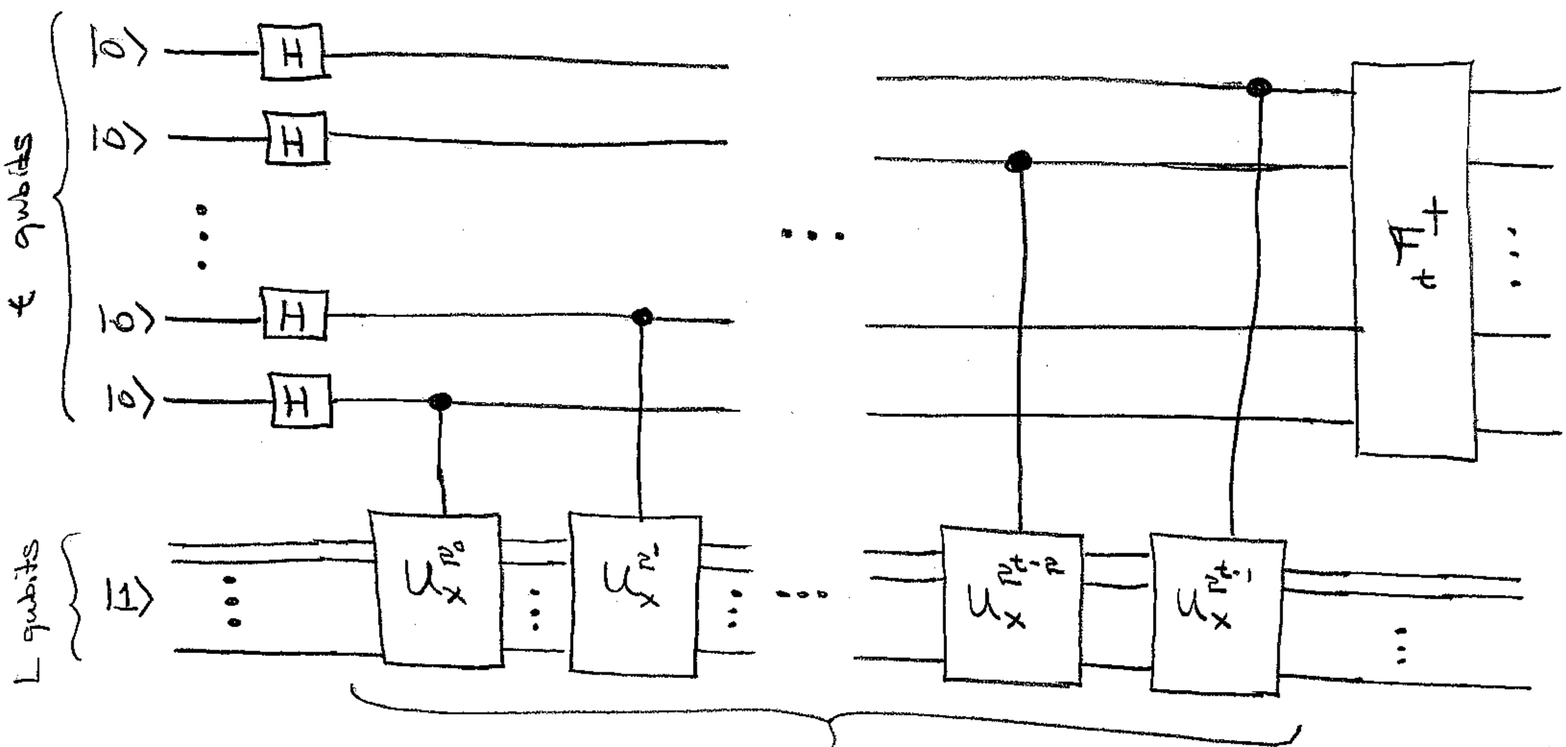
We are interested in the $y=1$ equivalence class:

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i k s/r} |x^k \pmod N\rangle$$

$$U_x |u_s\rangle = e^{2\pi i (s/r)} |u_s\rangle$$

phase ϕ_s we want to estimate; periodicity r/s

$$|x^k \pmod N\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i k s/r} |u_s\rangle, \quad k=0,\dots,r-1$$



This transformation:

$$|z\rangle|\psi\rangle \longrightarrow |z_1\rangle|z_2\rangle\dots|z_t\rangle \underbrace{U_x^{2^{t-1}z_1} U_x^{2^{t-2}z_2} \dots U_x^{2^1 z_{t-1}} U_x^{2^0 z_t}}_{U_x^{\sum_{j=1}^{t} 2^{t-j} z_j} = U_x^z} |\psi\rangle$$

$$|z\rangle|\psi\rangle \longrightarrow |z\rangle U_x^z |\psi\rangle$$

Including the Hadamards: $|0\rangle^{\otimes t}|\psi\rangle \longrightarrow \frac{1}{2^{t/2}} \sum_{z=1}^{2^t-1} |z\rangle U_x^z |\psi\rangle$

quantum parallelism

If $|\psi\rangle = |u_s\rangle$, $\quad |0\rangle^{\otimes t}|\psi\rangle \longrightarrow \left(\frac{1}{2^{t/2}} \sum_{z=1}^{2^t-1} e^{2\pi i z s/r}|z\rangle\right) \otimes |u_s\rangle$

(A) We can't put in $|u_s\rangle$ without knowing r

phase kickback

$U_x^z|y\rangle = |x^z y \pmod N\rangle$

(B) How do we do this?
$|z, y\rangle \longrightarrow |z, x^z y \pmod N\rangle$
Design a reversible classical circuit to calculate the function $x^z y \pmod N$; then do it in quantum parallel.

Modular exponentiation: Divide the z back into its bitwise components

$$x^z \pmod N = x^{\sum_{j=1}^{t} z_j 2^{t-j}} = \left((x^{2^{t-1}})^{z_1} \pmod N\right)\left((x^{2^{t-2}})^{z_2} \pmod N\right)$$
$$\times \cdots \times \left((x^{2^1})^{z_{t-1}} \pmod N\right)\left((x^{2^0})^{z_t} \pmod N\right)$$

Compute $x^2, x^4, \ldots, x^{2^{t-1}}$ $\qquad$ $t-1$ squaring operations, each using $O(L^2)$ elementary multiplications

Further t multiplications, each using $O(L^2)$ multiplications

$O(tL^2)$ operations

The modular exponentiation can be done efficiently. Making it reversible does not change the $O(tL^2)$ operations. Quantum parallelism calculates $x^z \pmod N$ in superposition and extracts the period r/s through the inverse FT. Classically, one would need to compute $r \sim O(\varphi(N)) \sim O(N) \sim O(2^L)$ values of $x^z \pmod N$ to extract r.

$k=0,\ x^k = 1$

$$\text{Input } |\psi\rangle = |1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

$$|0\rangle^{\otimes N}|1\rangle \longrightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \underbrace{\left(\frac{1}{2^{t/2}} \sum_{z=0}^{2^t-1} e^{2\pi i z s/r}|z\rangle\right)}_{|\phi_s = s/r\rangle} \otimes |u_s\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \underbrace{|\phi_s = s/r\rangle}\otimes |u_s\rangle$$

Near-momentum eigenstate. $F_t^\dagger$ gives near position eigenstate (period r/s in z; read out one of these periods)

Measurement yields M-bit approximation to one of the {periods s/r, $s=0,\ldots,r-1$, with probability $1-\epsilon$, provided (repeat algorithm if get $s=0$) $t \geq M+1+\log(1+1/2\epsilon)$.} A continued-fraction procedure extracts the fraction s/r exactly, provided $M \geq 2L+1$.

$\Longrightarrow$ $t \geq 2L+2+\log(1+1/2\epsilon)$.

This is technicality.

Failure modes:

1. Poor approximation to s/r; run with ϵ small to make this probability negligible.
2. Get $s=0$ or ambiguity because s/r can be reduced. Run several times.

Resources:

1. Hadamards: $O(t) = O(L)$
2. FT: $O(t^2) = O(L^2)$
3. Modular exponentiation: $O(tL^2) = O(L^3)$

Note quantum parallelism and phase kickback.

Success probability p

Probability of first success on Nth trial: $P_N = (1-p)^{N-1} p$

Probability of success by Nth trial: $Q_N = \sum_{n=1}^{N} P_N$

$$Q_N = \sum_{n=1}^{N} (1-p)^{n-1} p = \frac{p(1-(1-p)^N)}{1-(1-p)} = 1-(1-p)^N$$

To have $Q_N \geq 1-\epsilon$, we need $(1-p)^N \leq \epsilon$, i.e.,

$$N \geq \frac{-\log\epsilon}{-\log(1-p)} = \frac{\log(1/\epsilon)}{\log(1/(1-p))}$$

Factoring:

Input: L-bit composite number N, not even or a prime power.

easily checked

Output: A nontrivial factor of N

Randomly choose x, $1 < x \le N-1$, and calculate $\gcd(x,N)$ by Euclid's algorithm. $O(L^3)$

if $\gcd(x,N) > 1$, output $\gcd(x,N)$

if $\gcd(x,N) = 1$, find order r of x ← crucial quantum step

if r is even and $y = x^{r/2} \neq \pm 1 \pmod N$ ← the upper sign is automatic; the rest occurs with probability $\ge 1 - 1/2^m$, where m is the number of distinct prime factors of N; otherwise, choose a new x, and start over

$y^2 = x^r = 1 \pmod N$

$y = 2, \dots, N-2 \pmod N$
$[y \neq 0, \pm 1 \pmod N]$

$y^2 - 1 = (y-1)(y+1) = 0 \pmod N$. So N divides $(y-1)(y+1) = x^r - 1$
$\Rightarrow$ N has a common factor with $y-1$ or $y+1$
This common factor cannot be N, so N has a nontrivial common factor with both $y-1$ and $y+1$.

Calculate $\gcd(y-1, N)$ or $\gcd(y+1, N)$ (Euclid's algorithm, $O(L^3)$) and output the gcd.

$N = 15$

$$\left.\begin{array}{l} x = 2:\ r = 4,\ y = 4 \\ x = 4:\ r = 2,\ y = 4 \\ x = 7:\ r = 4,\ y = 49 \equiv 4 \pmod{15} \\ x = 8:\ r = 4,\ y = 64 \equiv 4 \pmod{15} \end{array}\right\} \longrightarrow y - 1 = 3,\ y + 1 = 5$$

$x = 11:\ r = 2,\ y = 11,\quad y - 1 = 10,\ y + 1 = 12$

$x = 13:\ r = 4,\ y = 169 \equiv 4 \pmod{15}$

$x = 14:\ r = 2,\ y = 14,\ \longleftarrow\ y = N - 1$, so start over

$\uparrow$

r even in all cases

Period finding:

$f: \{0,1\}^L \to \{0,1\}^L$

$f(z+r) = f(z)$ (Range of f) $= \{f(0), \ldots, f(r-1)\}$

$U|f(z)\rangle = |f(z+1)\rangle$

$U|y\rangle = |y\rangle$, $y \neq f(z)$ for any z

$U^z|f(0)\rangle = |f(z)\rangle$

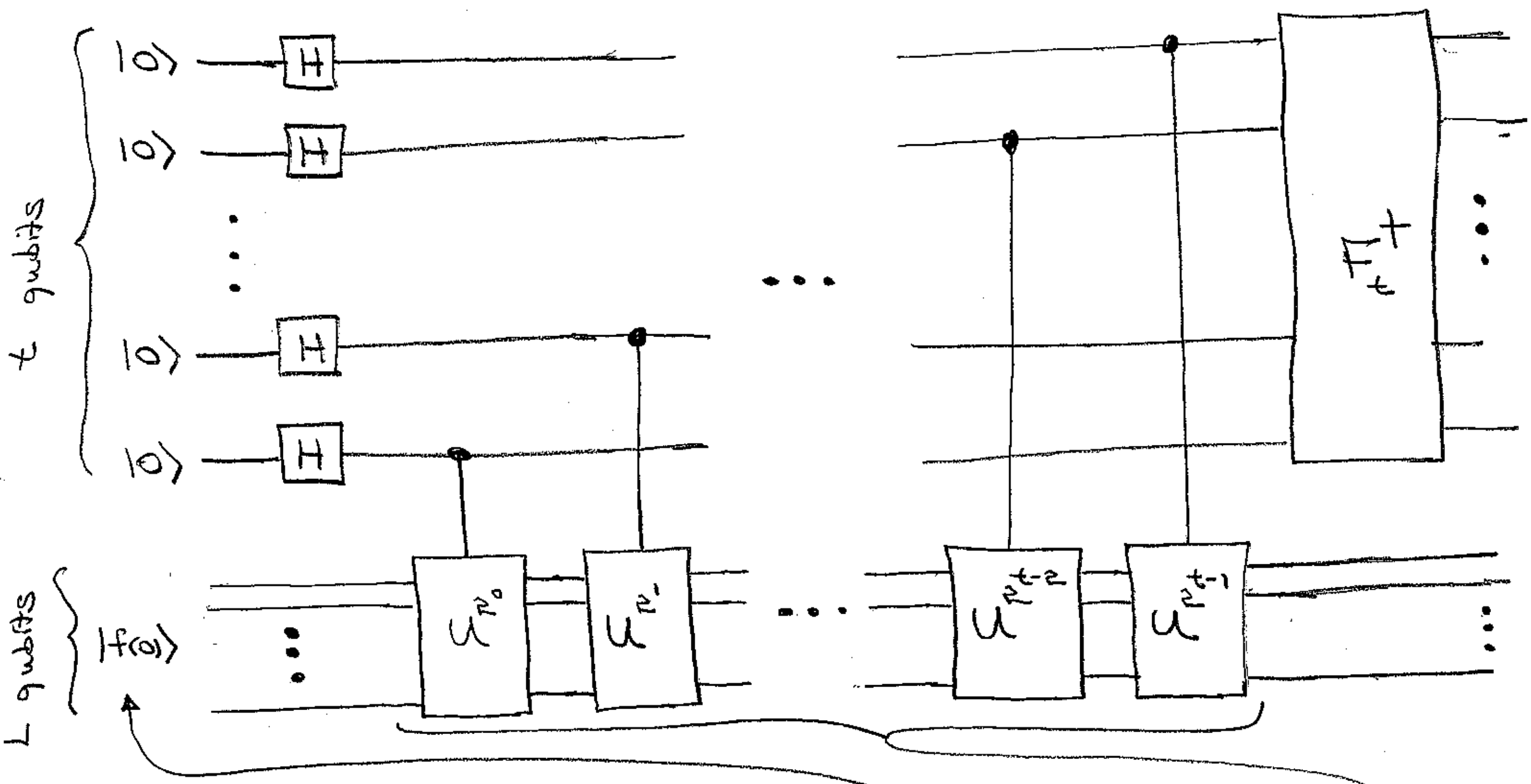
Order finding as a special case.

$f_x(z) = x^z \pmod N$

$f_x(z+r) = f_x(z)$

$U_x|y\rangle = |xy \pmod N\rangle$

$U_x^z|1\rangle = |x^z \pmod N\rangle$



$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{z=0}^{r-1} e^{-2\pi i s z/r} |f(z)\rangle$$

$$|f(0)\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

$$U|u_s\rangle = e^{2\pi i \underbrace{s/r}_{\text{phase } \phi}} |u_s\rangle$$

Determine one of the phases, s/r; extract the period, r.

$$|f(z)\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{+2\pi i s z/r} |u_s\rangle$$

What does this part of the circuit do?

$$|z\rangle|\psi\rangle \longrightarrow |z\rangle\, U^{\underbrace{z_1 2^{t-1} + z_2 2^{t-2} + \dots + z_{t-2} 2^1 + z_{t-1} 2^0}_{\sum_{j=1}^{N} z_j 2^{t-j} = z}} |\psi\rangle = |z\rangle U^z |\psi\rangle$$

$$|z\rangle|f(0)\rangle \longrightarrow |z\rangle U^z |f(0)\rangle = |z\rangle|f(z)\rangle$$

So we could replace this part of the circuit with the standard unitary for reversible function evaluation:

$$|z\rangle|y\rangle \longrightarrow |z\rangle|y \oplus f(z)\rangle$$

Now choose the initial state of the k ancilla qubits to be $|0\rangle$.

$$|z\rangle|0\rangle \longrightarrow |z\rangle|f(z)\rangle .$$

Including the Hadamards, the transformation becomes

$$|0\rangle^{\otimes t}|0\rangle^{\otimes L} \longrightarrow \frac{1}{2^{t/2}}\sum_{z=0}^{2^t-1} |z\rangle|f(z)\rangle \longleftarrow \text{quantum parallelism}$$

phase kickback

$$= \frac{1}{2^{t/2}}\frac{1}{\sqrt{r}}\sum_{z=0}^{2^t-1}\sum_{s=0}^{r-1} e^{2\pi i s z/r}|z\rangle|u_s\rangle$$

$$= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\underbrace{\left(\frac{1}{2^{t/2}}\sum_{z=0}^{2^t-1} e^{2\pi i z(s/r)}|z\rangle\right)}_{|\phi = s/r\rangle}|u_s\rangle$$

Near-momentum eigenstate with $p\phi = s/r$.

Measurement after $F_t^\dagger$ yields one of the s/r. Must repeat algorithm if get $s=0$.

Ⓐ

RSA cryptosystem

① Select two large prime numbers, p and q.

② Compute $N = pq$. →

③ Select a small (odd) integer, e, that is co-prime to $\varphi(N) = (p-1)(q-1)$.

④ Find the multiplicative inverse d of e modulo $\varphi(N)$. $[ed \equiv 1 (\text{mod } \varphi(N))]$

The positive integers $\leq N$ and co-prime to N (i.e., sharing no factor with N except 1) are a group Z_N^* under multiplication modulo N. The integers not co-prime to N are multiples of p or q. The $1 \leq x < N$ not co-prime are np, $n = 1, \ldots, q-1$, and mq, $m = 1, \ldots, p-1$. These lists contain no elements in common; i.e., the only multiples of both p and q are multiples of N. There being $p-1+q-1 = p+q-2$ integers in the lists, the order of Z_N^* is $pq - 1 - (p+q-2) = pq - p - q + 1 = (p-1)(q-1)$.

Public key: (e, N)

Secret key: (d, N)

$\lceil \log M \rceil \leq \lfloor \log N \rfloor < \log N \Rightarrow 1 \leq M < N$

Message M Encode using public key as $M' = M^e (\text{mod } N)$. Decode using secret key as $M'' = (M')^d (\text{mod } N) = M^{ed} (\text{mod } N)$.

① Why does this work? Because $M^{\varphi(N)} \equiv 1 (\text{mod } N)$ if M is co-prime to N.

$$M^{ed} (\text{mod } N) = M(M^{\varphi(N)})^k (\text{mod } N)$$

$$ed \equiv 1 (\text{mod } \varphi(N)) \Rightarrow ed = 1 + k\varphi(N)$$

(a) M co-prime to $N \Rightarrow M^{\varphi(N)} = 1 \pmod N$

$\Rightarrow M^{ed} = M \pmod N$

(b) M not co-prime to $N \Rightarrow$ M is a multiple of p or a multiple of q, but not both, so say it's a multiple of p.

(rare case)

M a multiple of p

$M = 0 \pmod p \Longrightarrow \boxed{M^{ed} = 0 \pmod p}$

$M^{q-1} = 1 \pmod q \Longrightarrow M^{\varphi(N)} = M^{(p-1)(q-1)} = 1 \pmod q$

so $\boxed{M^{ed} = M \pmod q}$

M not a multiple of q

$M^{ed} = M \pmod N$ is a solution.
By the Chinese remainder theorem, it is the unique solution.

What we have shown is that encoding, $M^e \pmod N$, is a 1-1 function from $\{1, \ldots, N-1\}$ to itself; decoding, $M^d \pmod N$, is the inverse function.

Messages like this are hazardous, because the encoded message can be used to find the secret key.

M co-prime to $N \Leftrightarrow M^e$ is co-prime to N.

$\Rightarrow$ Immediate consequence of the group $\mathbb{Z}_N^*$

ⓒ

$\Leftarrow$ M^e has a multiplicative inverse x.

$$M^e x = 1 \pmod N \Rightarrow M \underbrace{(M^{e-1}x)}_{\text{inverse of } M} = 1 \pmod N$$

$$\Rightarrow M \text{ is co-prime to } N$$

This says that the messages not co-prime to N (multiples of p or q) are encoded as numbers not co-prime to N. In this case, Euclid's algorithm applied to $M^e \pmod N$ and N would reveal p or q, thus allowing the extraction of the secret key.

② Can it be done efficiently?

ⓐ Generating the prime numbers:

$$\begin{pmatrix}\text{probability that an} \\ \text{L-bit \# is prime}\end{pmatrix} \sim \frac{1}{\log(2^L)} \sim \frac{1}{L}$$

$O(L^3)$ operations to test for primality

$O(L^4)$ operations to get an L-bit prime

ⓑ Getting e and d: Euclid's algorithm; $O(L^3)$ operations

ⓒ Encoding and decoding: Modular exponentiation; $O(L^3)$ operations

(5) (D)

Is it secure?

efficiency becomes the key to security

(a) If you could factor N (efficiently), thereby obtaining $\varphi(N) = (p-1)(q-1)$, you could find d efficiently using Euclid's algorithm, just as the party who set up the keys did. You would then have the secret key for decoding.

(b) Suppose M^e is co-prime to N. (If it's not, the gcd to M^e and N is p or q, which you can find by Euclid's algorithm, thereby going back to (a)). If you can find the order of M^e modulo N, i.e., the smallest positive integer s such that $(M^e)^s = 1 \pmod N$, then you can extract the message M in the following way. Let r be the order of M, i.e., the smallest positive integer r such that $M^r = 1 \pmod N$; We know that $s = r/\gcd(e,r)$. Since $r \mid \varphi(N)$ and e is co-prime to $\varphi(N)$, e is also co-prime to $r \Leftrightarrow \gcd(e,r) = 1 \Rightarrow s = r$. Now let d' be multiplicative inverse of e modulo $s = r$, i.e., $ed' = 1 \pmod r \Rightarrow ed' = 1 + kr$. Now extract the message by

$$M^{ed'} \pmod N = M(M^r)^k \pmod N = M \pmod N.$$

$ed = 1 + k\varphi(N) = 1 + klr \Rightarrow d = d' \pmod r$

For different messages m, you would find different d', whereas d works for all messages.

(E)

(c) Other attacks?