Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMUST
Department of Muster
Second row

Shor‘s algorithm: Order finding and factorization

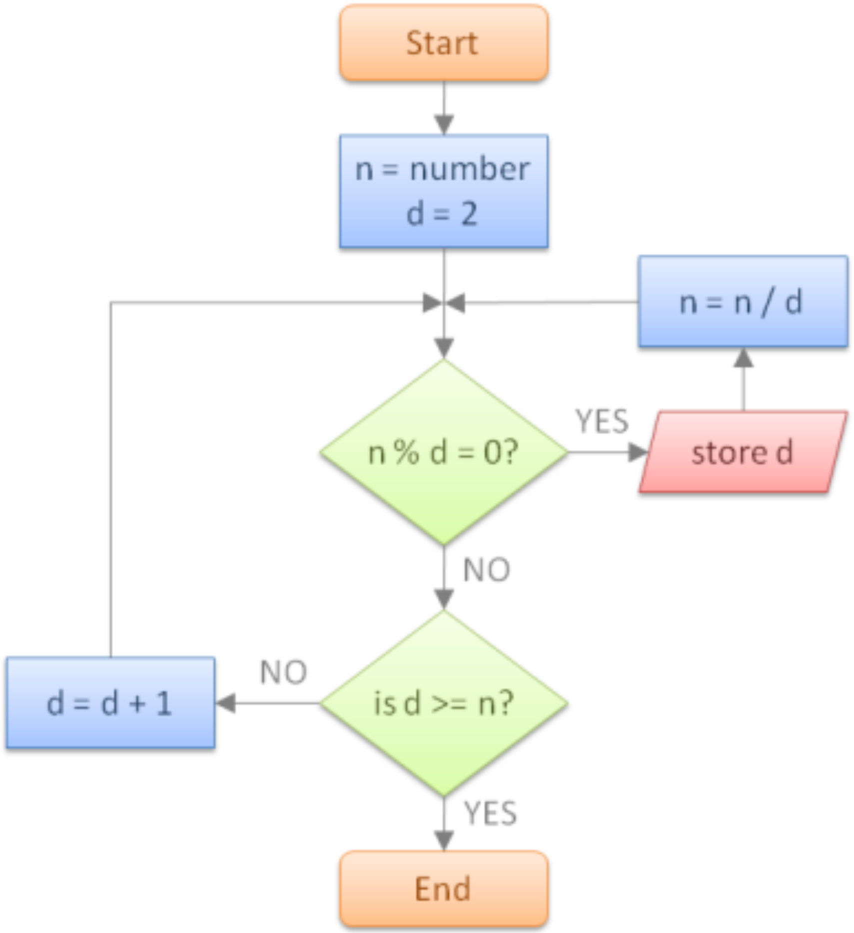
Ruben Dezeure & Manuel Schneider

Outline

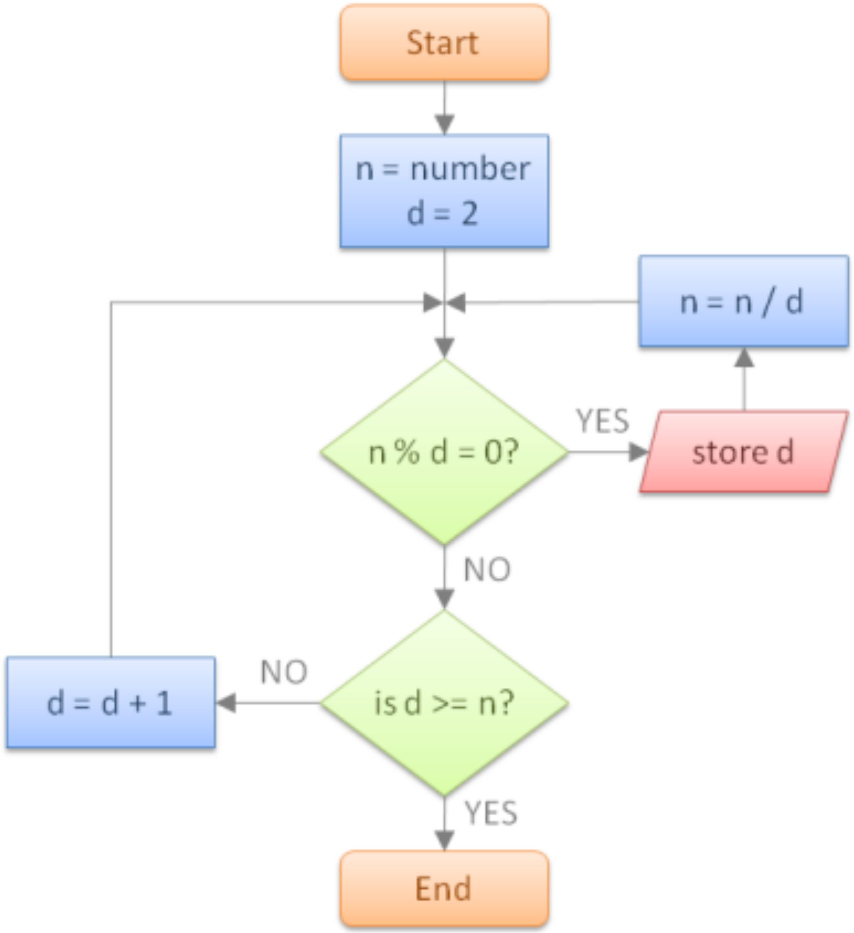
- Introduction
- Quantum Fourier Transform
- Phase Estimation
- Modular Exponentiation
- Order Finding
- Prime Factorization

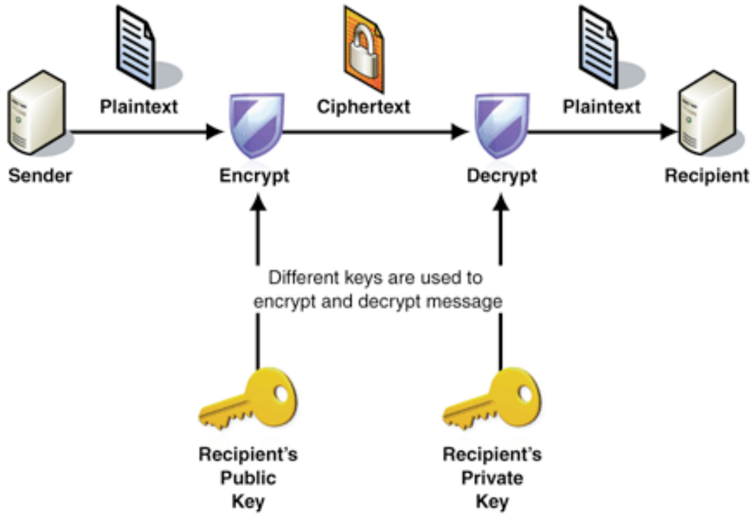
What is Shor‘s algorithm and why is it interesting?

Introduction

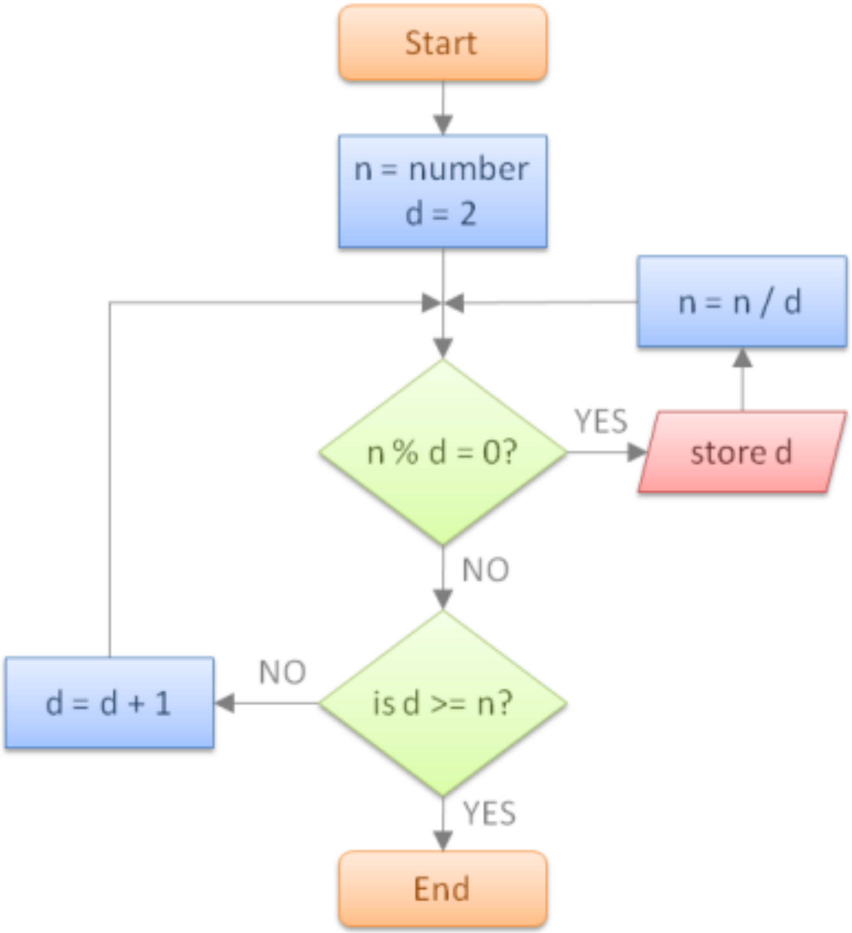


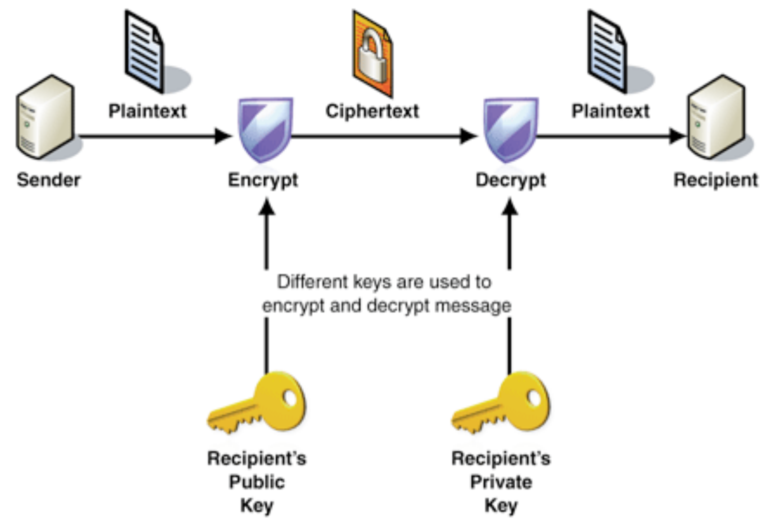
Introduction





Introduction



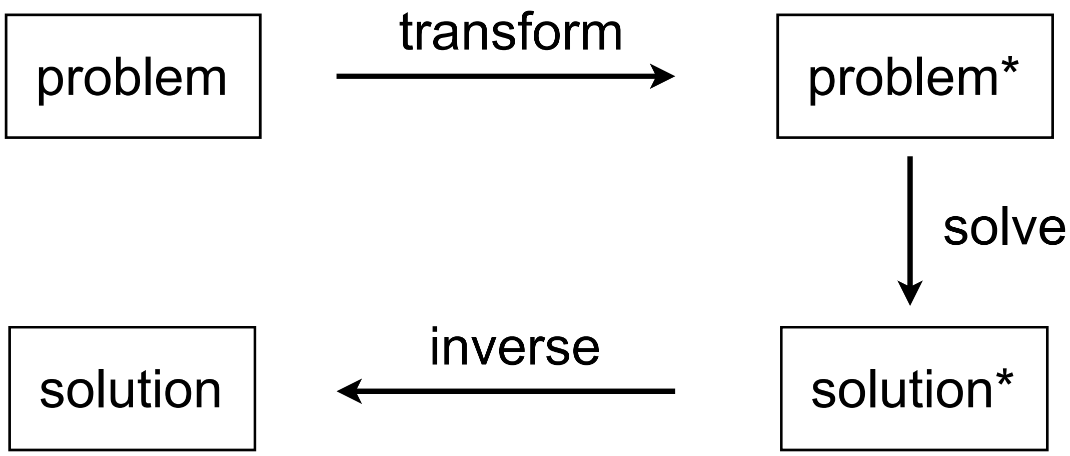


superpolynomial time on classical computers

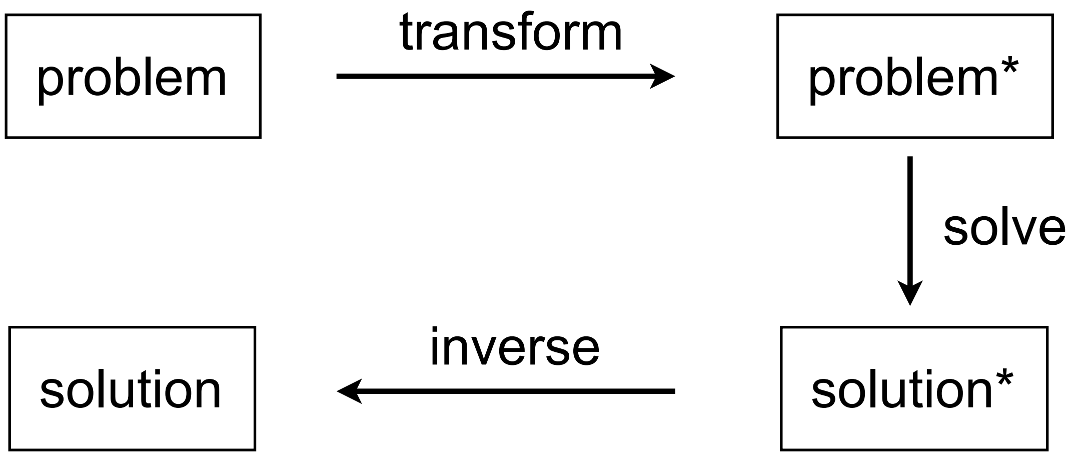
quantum polynomial time for Shor‘s algorithm!

Quantum Fourier Transform

Quantum Fourier Transform



Quantum Fourier Transform



discrete Fourier transform

Quantum Fourier Transform

classical

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}$$

Quantum Fourier Transform

classical

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$$

qm

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_j e^{2\pi ijk/N} |k\rangle$$

Phase Estimation

Phase Estimation

- general procedure
- key for many quantum algorithms

Phase Estimation

- general procedure
- key for many quantum algorithms

unitary operator	U
eigenvector	$\|u\rangle$
eigenvalue	$e^{2\pi i\varphi}$, unknown φ

Phase Estimation

1. $|0\rangle \, |u\rangle$ initial state

Phase Estimation

1. $|0\rangle\,|u\rangle$ — initial state

2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,|u\rangle$ — create superposition

Phase Estimation

1. $|0\rangle |u\rangle$ initial state

2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j |j\rangle |u\rangle$ create superposition

3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j |j\rangle U^j |u\rangle$ apply black box

Phase Estimation

1. $|0\rangle\,|u\rangle$ initial state

2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,|u\rangle$ create superposition

3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,U^j\,|u\rangle$ apply black box

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j e^{2\pi i j \varphi_u}\,|j\rangle\,|u\rangle$$

Phase Estimation

1. $|0\rangle\,|u\rangle$ — initial state

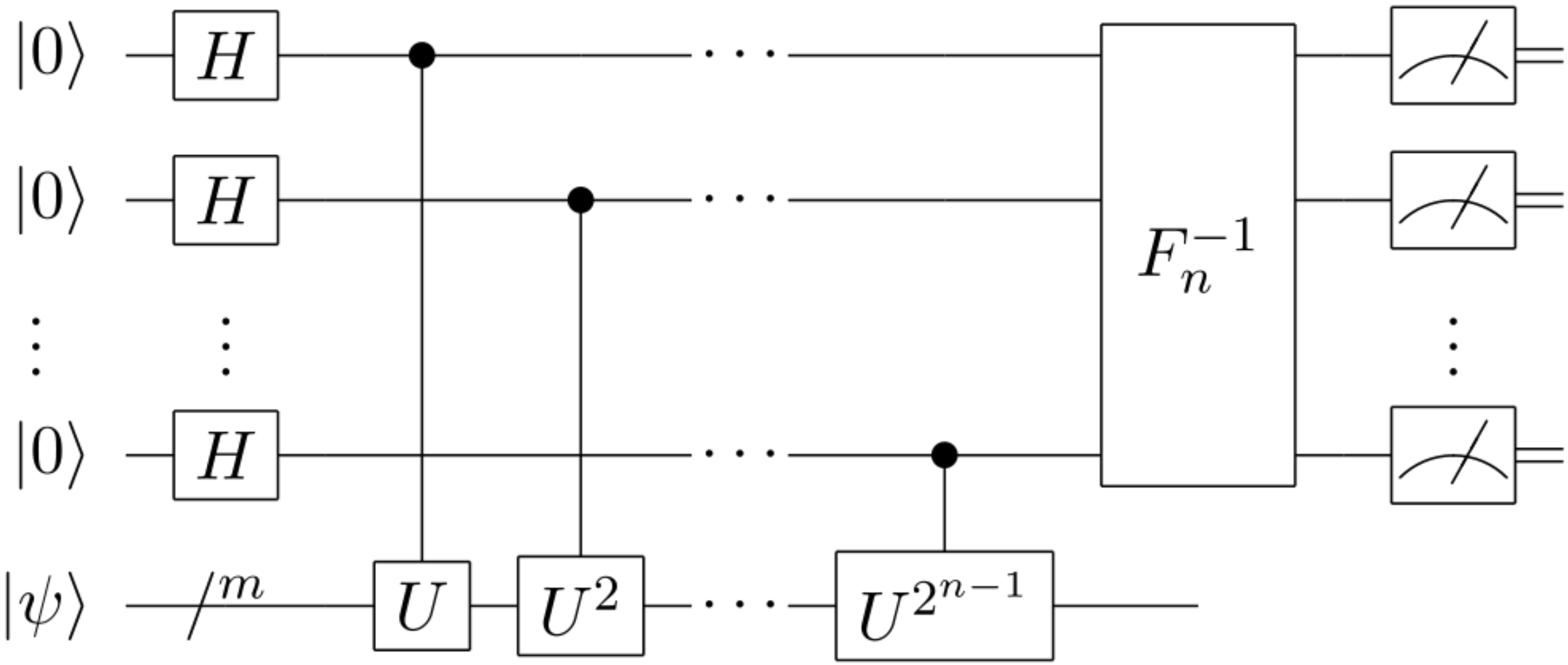
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,|u\rangle$ — create superposition

3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,U^j\,|u\rangle$ — apply black box

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j e^{2\pi i j \varphi_u}\,|j\rangle\,|u\rangle$$

4. $\rightarrow |\varphi\rangle\,|u\rangle$ — apply inverse FT

Phase Estimation



Modular Exponentiation

Modular Exponentiation

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{t-1} x_j \left| j \right\rangle U^{2^j} \left| u \right\rangle$$

Modular Exponentiation

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{t-1} x_j \left|j\right\rangle U^{2^j} \left|u\right\rangle$$

$$\Big\downarrow \; \left|z\right\rangle \left|y\right\rangle$$

Modular Exponentiation

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{t-1} x_j \left|j\right\rangle U^{2^j} \left|u\right\rangle$$

$$\Big\downarrow \; \left|z\right\rangle \left|y\right\rangle$$

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{t-1} x_j \left|z\right\rangle U^{z_j 2^j} \left|y\right\rangle$$

Modular Exponentiation

$$U\,|y\rangle \;\equiv\; |xy(\mathrm{mod}N)\rangle$$

Modular Exponentiation

$$U|y\rangle \equiv |xy(\mathrm{mod}N)\rangle$$

$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{t-1} x_j |z\rangle \left| x^{z_j 2^j} y(\mathrm{mod}N)\right\rangle$$

$$= \quad |z\rangle |x^z y(\mathrm{mod}N)\rangle$$

Order-finding

- Find least positive r for specified x and N such that:

$$x^r = 1 (\mathrm{mod}\ N)$$

- No classical algo exists polynomial in O(L)

$$L \equiv \lceil \log_2 (N) \rceil$$

Order-finding: Quantum algorithm

- Phase estimation applied to operator U

$$U|y\rangle \equiv |xy(\bmod N)\rangle \qquad y \in \{0,1\}^L$$

- Then eigenstates of U are:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle \qquad 0 \le s \le r-1$$

Order-finding: Quantum algorithm

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle \qquad 0 \le s \le r-1$$

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^{k+1} \bmod N\rangle$$

$$= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle$$

Obtain estimate s/r using phase estimation procedure

Order r can be obtained with a little bit more work.

Order-finding: requirements

- Need efficient procedure for U for any

$$U|y\rangle \equiv |xy(\text{mod}\,N)\rangle$$

→satisfied by using modular exponentiation

- Must be able to prepare $|u_s\rangle$

→trickier, need r

exists clever fix for that

then we only obtain estimate $\varphi \approx s/r$

Order-finding: continued fraction expansion

- Now have estimate $\varphi \approx s/r$ would like to get r

Theorem: Suppose s/r is a rational number such that

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2}$$

Then s/r is a convergent of the continued fraction for φ.

→ Can use the continued fraction algorithm

Order-finding: continued fraction expansion

- The continued fraction algorithm

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}.$$

Can get s‘ and r‘ such that

$$\frac{s'}{r'} = \frac{s}{r}$$

➔ find correct r with probability > 1/4

Factoring algorithm

- Factoring can be reduced to order-finding

Theorem: *if x non trivial solution of*

$$x^2 = 1 (\mathrm{mod}\, N)$$

Then at least either gcd(x-1,N) or gcd(x+1,N) is a non-trivial factor of N. Can be computed using $O(L^3)$ *operations.*

Theorem: $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$

x chosen at random $1 \leq x \leq N-1$ *and co-prime with N. r is order of x mod N.*

Then p(r is even and $x^{r/2} \neq -1 (\mathrm{mod}\, N)$*)* $\geq 1 - \frac{1}{2^m}$

Factoring algorithm

1. Determine if N trivially factorisable
2. Randomly choose x >0 and < N. if gcd(x,N)>1 return it
3. Order-finding to find r $x^r = 1(\mathrm{mod}\, N)$
4. If r even and $x^{r/2} \neq -1(\mathrm{mod}\, N)$ then compute gcd($x^{r/2}$-1,N) and gcd($x^{r/2}$+1,N)

➔Each of these 2 can be a nontrivial factor of N

If not: repeat 3-4

Conclusions

- Quantum algorithm factorizes in polynomial time

- Critical components:
  - Quantum FT
  - Modular exponentiation
  - Order finding