Quantum Fourier Transforms and Shor's Algorithm (Parts 1 and 2)

Peter Høyer

University of Calgary

June 24, 2003

PIMS-MITACS Summer School on Quantum Information Science

Techniques

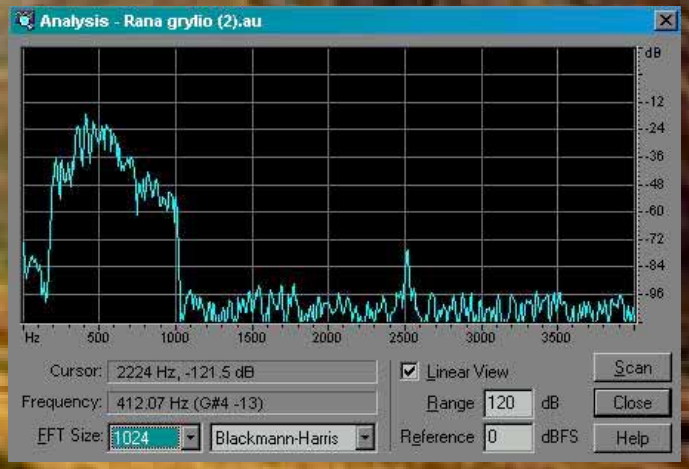
1. Amplitude Amplification

   Grover's Search algorithm

2. Fourier Transforms

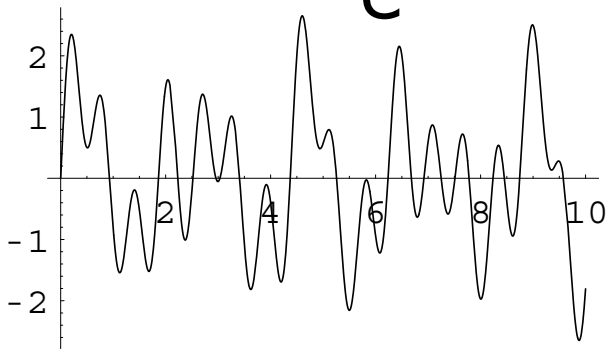
   Shor's Factoring algorithm

Frequency Analysis

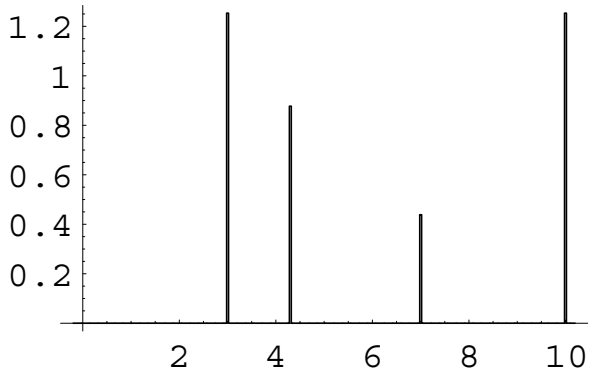


Fourier Transforms

Time



Frequency

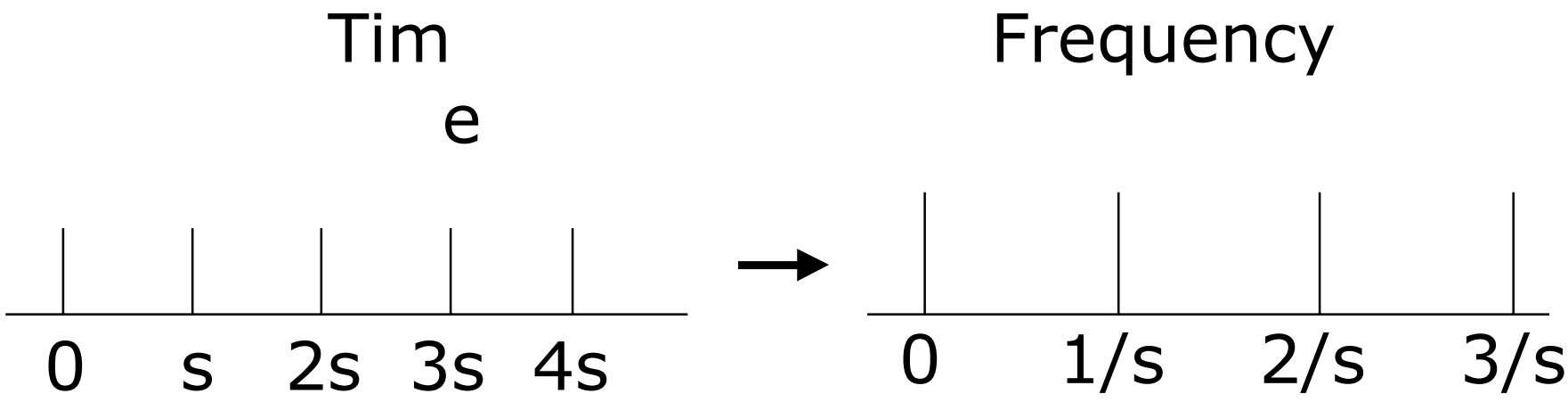


Sin[3t] + .7 Sin[4.2t] + .36 Sin[7t] + Sin[10t]

↓ Fourier Transform

_(3) + .7 _(4.2) + .36 _(7) + _(10)

Discrete Fourier Transforms

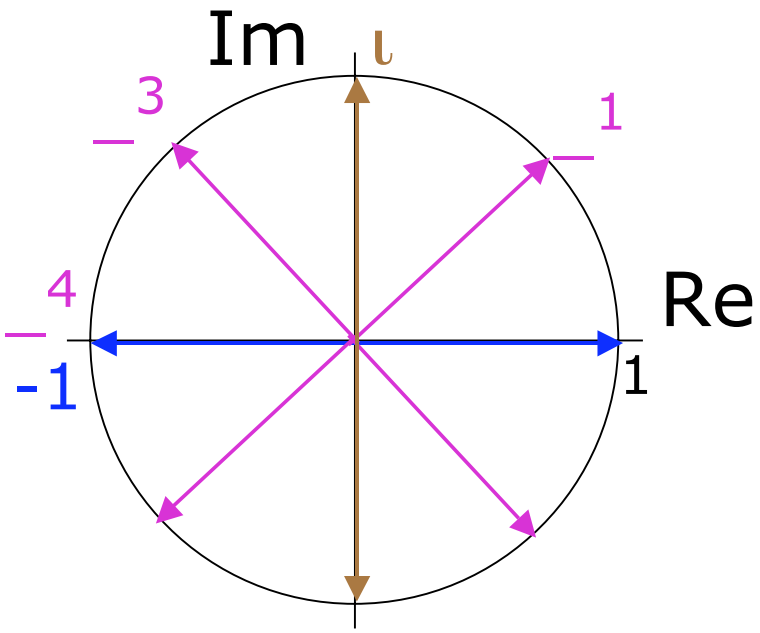


Period s

↓ Fourier Transform

Frequencies {0, 1/s, 2/s, 3/s,…}

Roots of unity



$X^2=1 \Leftrightarrow X\in\{+1,-1\}$

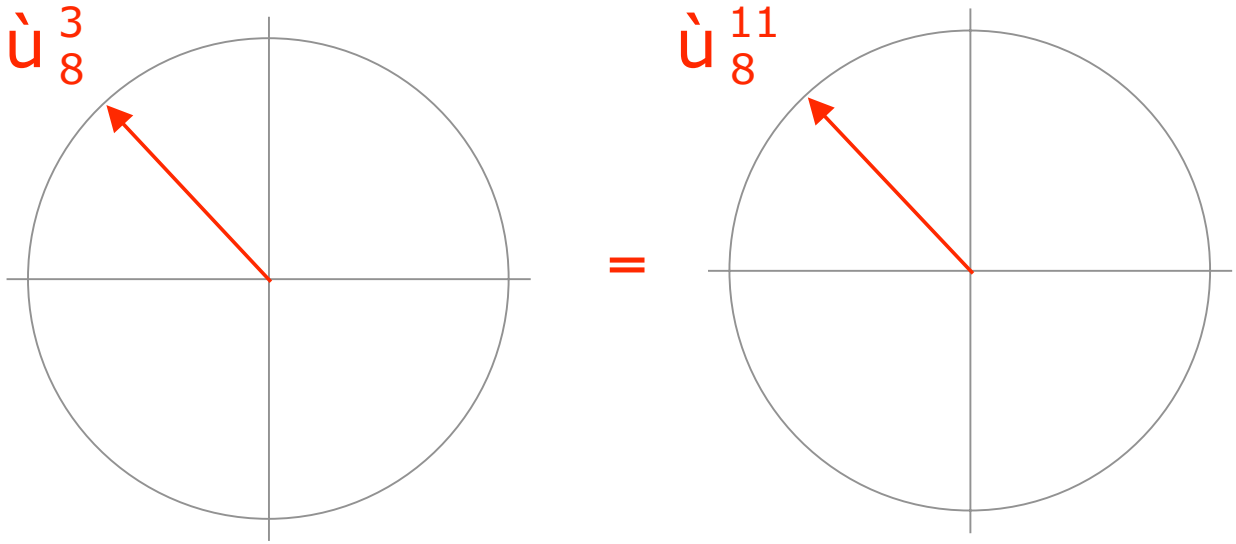
$X^4=1 \Leftrightarrow X\in\{+1,\iota,-1,-\iota\}$

$X^8=1 \Leftrightarrow$
$X\in\{\_^0,\_^1,\_^2,\_^3,\_^4,\_^5,\_^6,\_^7\}$

where $\_ = \__8 = \exp(2\pi\iota/8)$

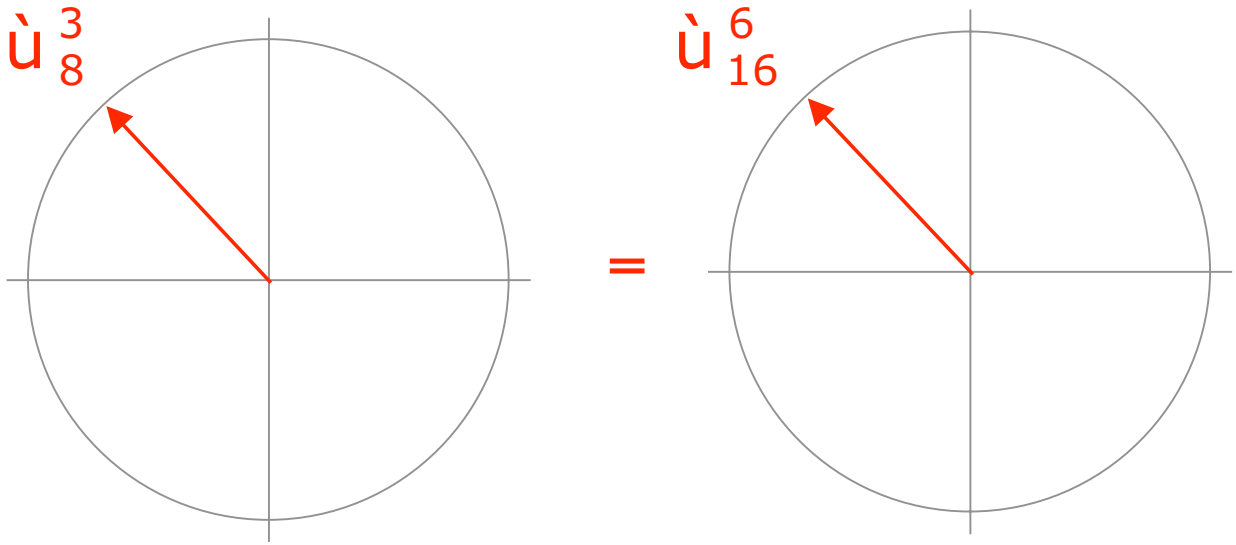
Def: n^{th} principal root is $\__n = \exp(2\pi\iota/n)$

Property I



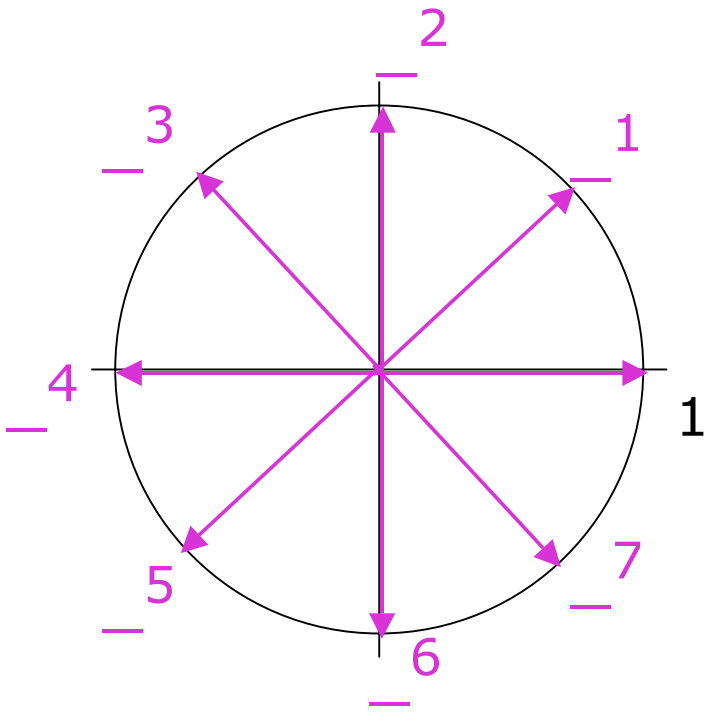
Def: n^{th} principal root is $\omega_n = \exp(2\pi\iota/n)$

Property II



Def: n^{th} principal root is $\omega_n = \exp(2\pi\iota/n)$

Destructive interference!



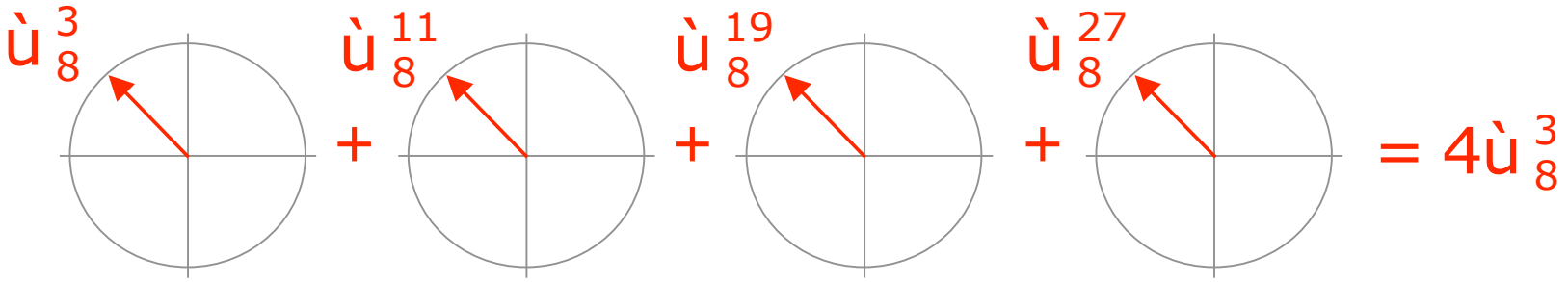
$$\sum_{j=0}^{n-1} \omega_n^j = 0$$

$$\sum_{j=0}^{n-1} \omega_n^{tj} = 0 \quad (0 < t < n)$$

Eg, t=5: $\{\omega_n^0, \omega_n^1, \omega_n^2, \omega_n^3, \omega_n^4, \omega_n^5, \omega_n^6, \omega_n^7\}$

$= \{\omega_n^0, \omega_n^5, \omega_n^{10}, \omega_n^{15}, \omega_n^{20}, \omega_n^{25}, \omega_n^{30}, \omega_n^{35}\}$

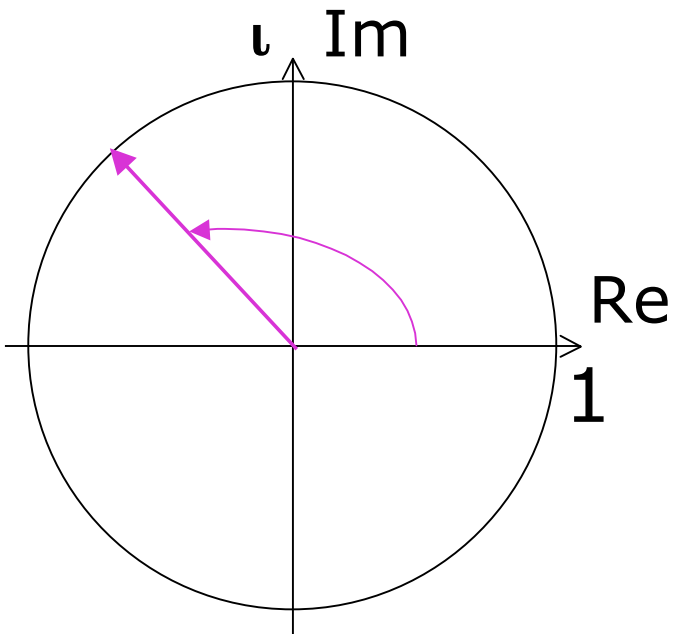
Constructive interference



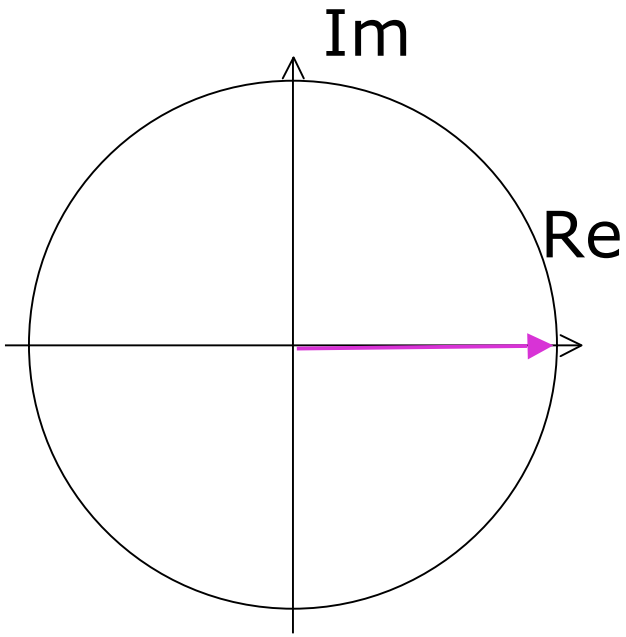
Back to Frequency Analysis

—

Rotating vector

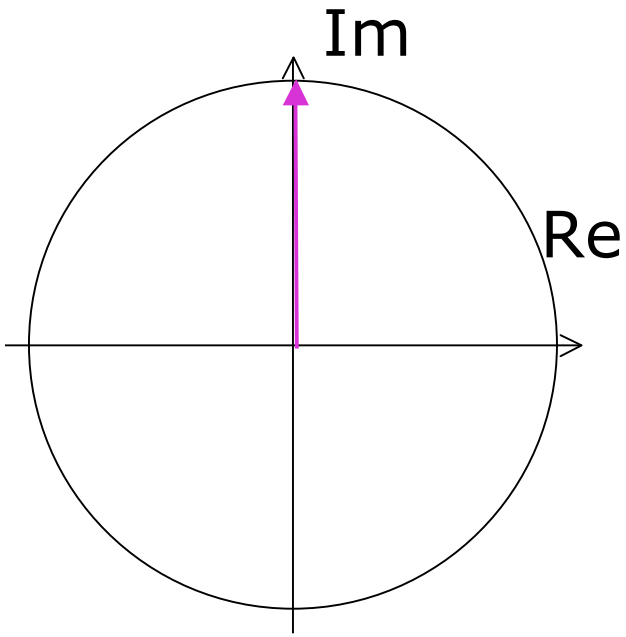


Rotating vector



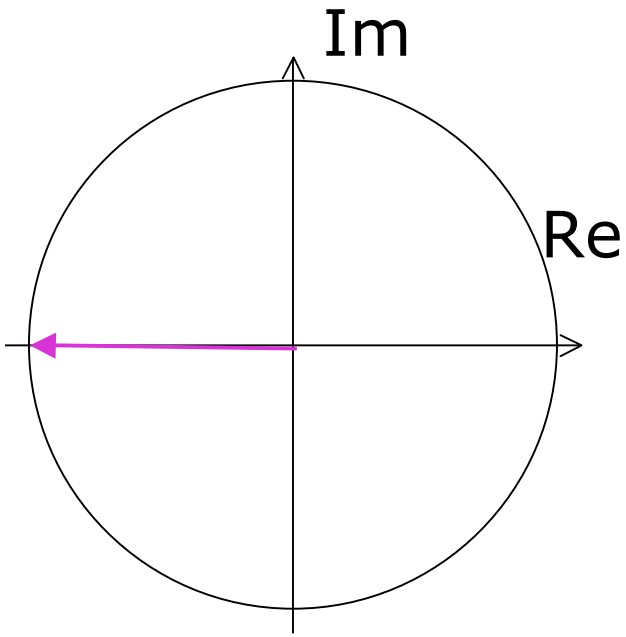
$f_2 = 1$

Rotating vector



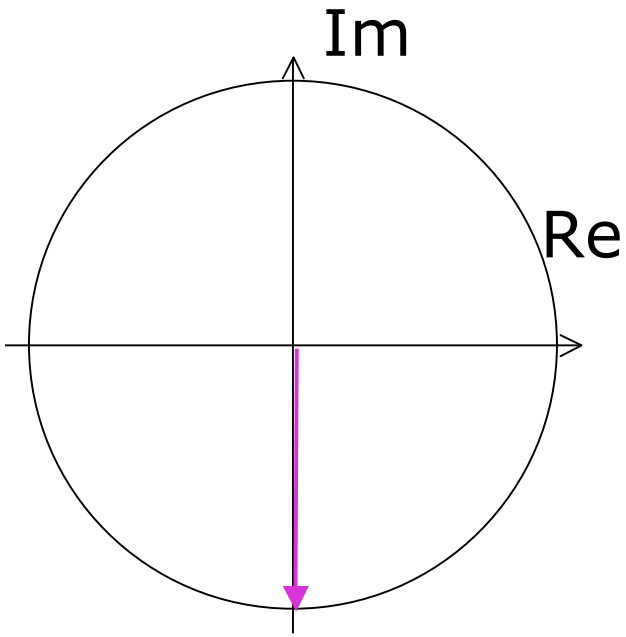
$f_2 = 1 , \iota$

Rotating vector



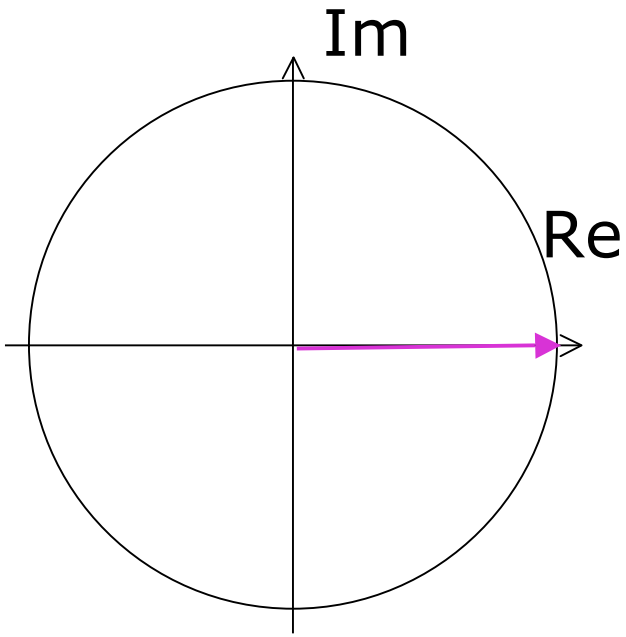
$f_2 = 1 , \imath , -1$

Rotating vector



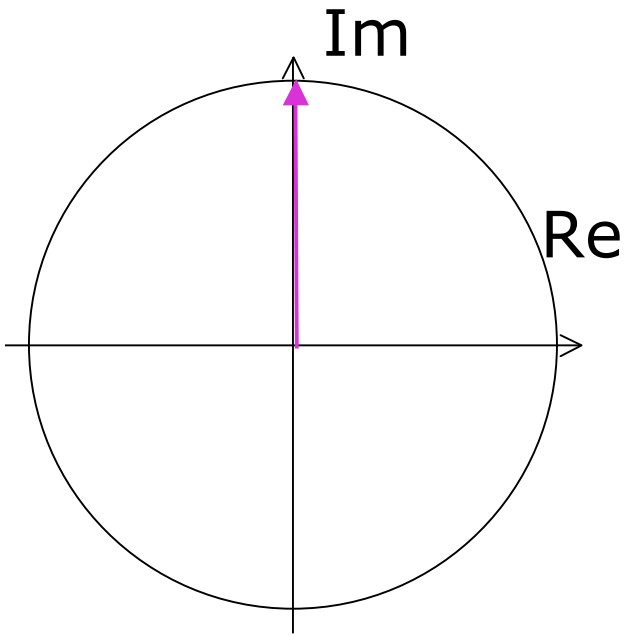
$f_2 = 1 , \iota , -1 , -\iota$

Rotating vector



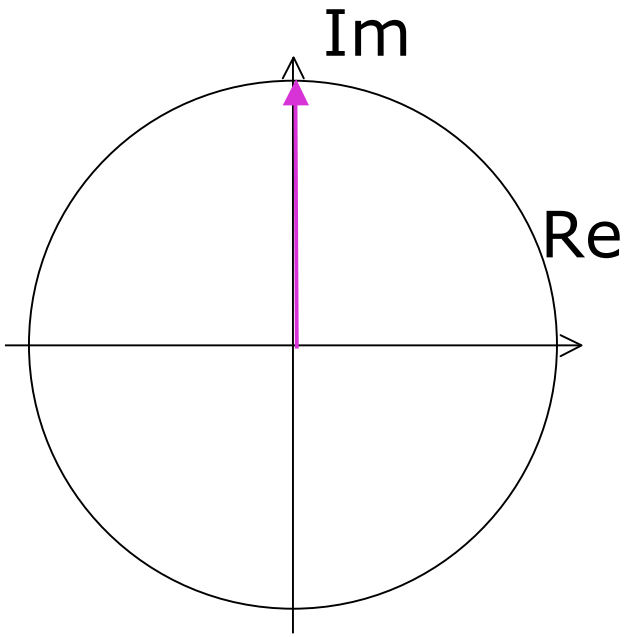
$f_2 = 1, \imath, -1, -\imath, 1$

Rotating vector



$f_2 = 1, \imath, -1, -\imath, 1, \imath$

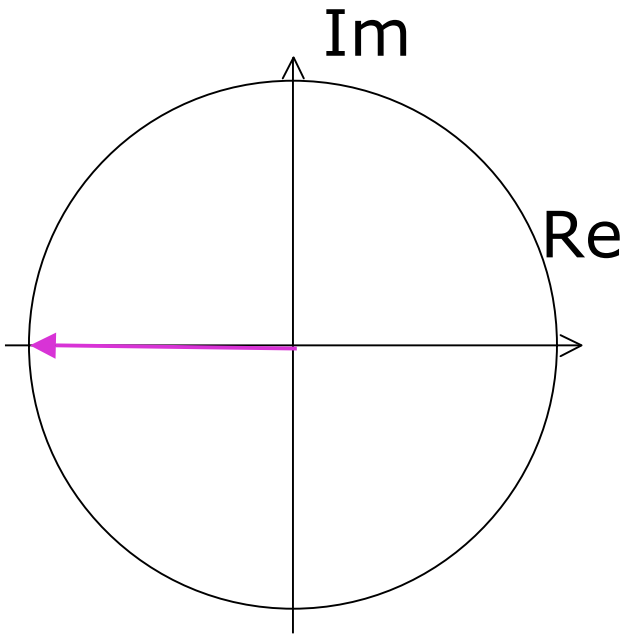
Rotating vector



TIME

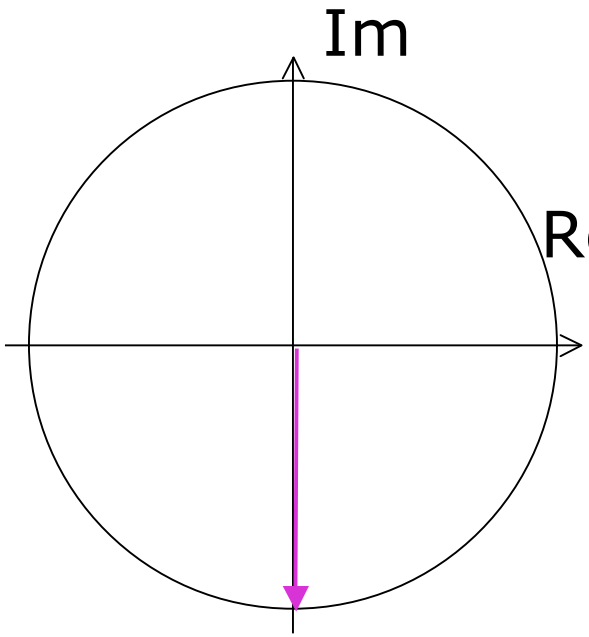
f_2	1	ι	-1	-ι	1	ι	-1	-ι

Rotating vector



f_2	1	ι	-1	$-\iota$	1	ι	-1	$-\iota$
f_4	1	-1	1	-1	1	-1	1	-1

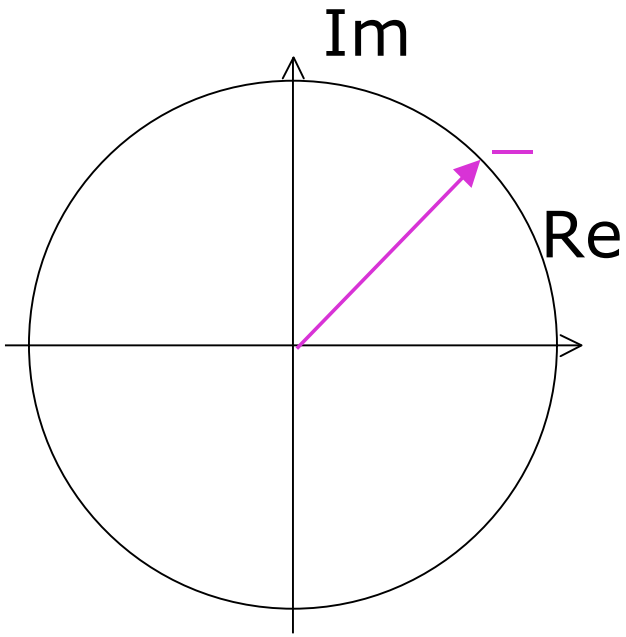
Rotating vector



FREQUENCY

f_2	1	ι	-1	-ι	1	ι	-1	-ι
f_4	1	-1	1	-1	1	-1	1	-1
f_6	1	-ι	-1	ι	1	-ι	-1	ι

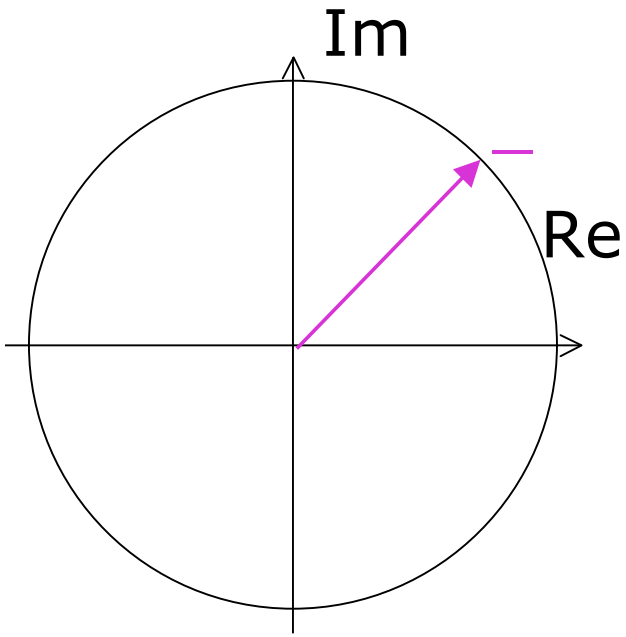
Rotating vector



$\iota = \_^2$

f_1	1	_						
f_2	1	ι	-1	$-\iota$	1	ι	-1	$-\iota$
f_4	1	-1	1	-1	1	-1	1	-1
f_6	1	$-\iota$	-1	ι	1	$-\iota$	-1	ι

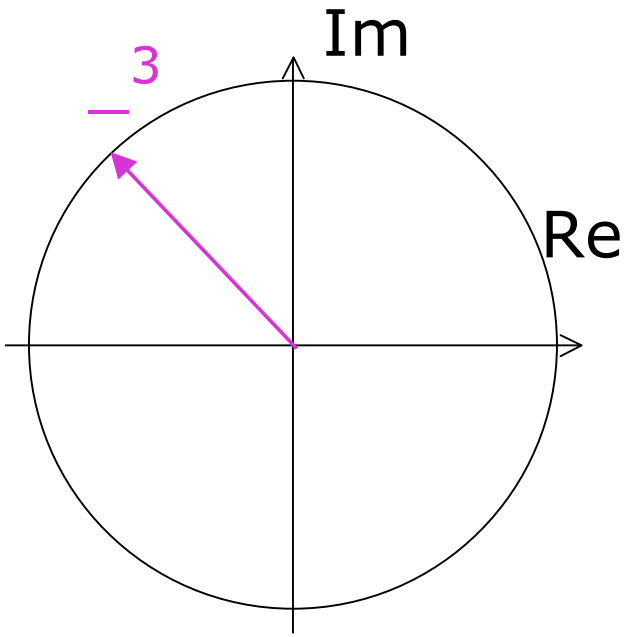
Rotating vector



$\iota = \_^2$

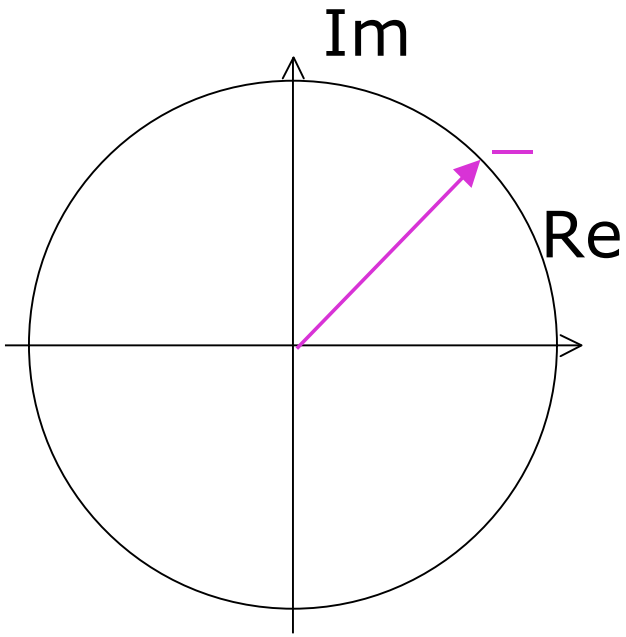
f_1	1	$\_$	$\_^2$	$\_^3$	$\_^4$	$\_^5$	$\_^6$	$\_^7$
f_2	1	ι	-1	$-\iota$	1	ι	-1	$-\iota$
f_4	1	-1	1	-1	1	-1	1	-1
f_6	1	$-\iota$	-1	ι	1	$-\iota$	-1	ι

Rotating vector



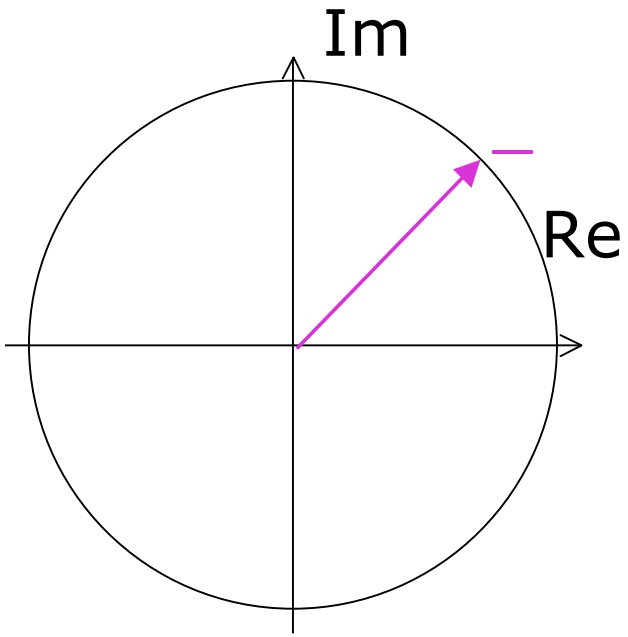
$\iota = \_^2$

f_0	1	1	1	1	1	1	1	1
f_1	1	_	$\_^2$	$\_^3$	$\_^4$	$\_^5$	$\_^6$	$\_^7$
f_2	1	ι	-1	$-\iota$	1	ι	-1	$-\iota$
f_3	1	$\_^3$	$\_^6$	_	$\_^4$	$\_^7$	$\_^2$	$\_^5$
f_4	1	-1	1	-1	1	-1	1	-1
f_5	1	$\_^5$	$\_^2$	$\_^7$	$\_^4$	_	$\_^6$	$\_^3$
f_6	1	$-\iota$	-1	ι	1	$-\iota$	-1	ι
f_7	1	$\_^7$	$\_^6$	$\_^5$	$\_^4$	$\_^3$	$\_^2$	_



f_0	1	1	1	1	1	1	1	1
f_1	1	$\_$	$\_^2$	$\_^3$	$\_^4$	$\_^5$	$\_^6$	$\_^7$
f_2	1	$\_^2$	$\_^4$	$\_^6$	$\_^0$	$\_^2$	$\_^4$	$\_^6$
f_3	1	$\_^3$	$\_^6$	$\_$	$\_^4$	$\_^7$	$\_^2$	$\_^5$
f_4	1	$\_^4$	$\_^0$	$\_^4$	$\_^0$	$\_^4$	$\_^0$	$\_^4$
f_5	1	$\_^5$	$\_^2$	$\_^7$	$\_^4$	$\_$	$\_^6$	$\_^3$
f_6	1	$\_^6$	$\_^4$	$\_^2$	$\_^0$	$\_^6$	$\_^4$	$\_^2$
f_7	1	$\_^7$	$\_^6$	$\_^5$	$\_^4$	$\_^3$	$\_^2$	$\_$

Fourier Transform!



TIME

FREQUENCY

1	1	1	1	1	1	1	1
1	$\_$	$\_^{2}$	$\_^{3}$	$\_^{4}$	$\_^{5}$	$\_^{6}$	$\_^{7}$
1	$\_^{2}$	$\_^{4}$	$\_^{6}$	$\_^{0}$	$\_^{2}$	$\_^{4}$	$\_^{6}$
1	$\_^{3}$	$\_^{6}$	$\_$	$\_^{4}$	$\_^{7}$	$\_^{2}$	$\_^{5}$
1	$\_^{4}$	$\_^{0}$	$\_^{4}$	$\_^{0}$	$\_^{4}$	$\_^{0}$	$\_^{4}$
1	$\_^{5}$	$\_^{2}$	$\_^{7}$	$\_^{4}$	$\_$	$\_^{6}$	$\_^{3}$
1	$\_^{6}$	$\_^{4}$	$\_^{2}$	$\_^{0}$	$\_^{6}$	$\_^{4}$	$\_^{2}$
1	$\_^{7}$	$\_^{6}$	$\_^{5}$	$\_^{4}$	$\_^{3}$	$\_^{2}$	$\_$

Quantum Fourier Transforms

$$F_M = \frac{1}{\sqrt{\hat{I}}} \begin{bmatrix} 1 & 1 & 1 & L & 1 \\ 1 & ù & ù^2 & & ù^{M-1} \\ 1 & ù^2 & ù^4 & & ù^{2(M-1)} \\ M & & & O & M \\ 1 & ù^{M-1} & ù^{2(M-1)} & L & ù^{(M-1)(M-1)} \end{bmatrix} = \sum_{i,j=0}^{M-1} \_^{ij} |i\rangle\langle j|$$

1) QFT is unitary: $\sum_j \_^{-j} \_^{2j} = 0$

2) Superpos of everything: $F_M |0\rangle = \sum_j |j\rangle = F_M^{-1} |0\rangle$

3) Computable in time $O(\log^2 M)$

Computable in $O(\log^2 M)$

1	1	1	1	1	1	1	1
1	$\binom{}{}$	$\binom{2}{}$	$\binom{3}{}$	$\binom{4}{}$	$\binom{5}{}$	$\binom{6}{}$	$\binom{7}{}$
1	$\binom{2}{}$	$\binom{4}{}$	$\binom{6}{}$	$\binom{0}{}$	$\binom{2}{}$	$\binom{4}{}$	$\binom{6}{}$
1	$\binom{3}{}$	$\binom{6}{}$	$\binom{}{}$	$\binom{4}{}$	$\binom{7}{}$	$\binom{2}{}$	$\binom{5}{}$
1	$\binom{4}{}$	$\binom{0}{}$	$\binom{4}{}$	$\binom{0}{}$	$\binom{4}{}$	$\binom{0}{}$	$\binom{4}{}$
1	$\binom{5}{}$	$\binom{2}{}$	$\binom{7}{}$	$\binom{4}{}$	$\binom{}{}$	$\binom{6}{}$	$\binom{3}{}$
1	$\binom{6}{}$	$\binom{4}{}$	$\binom{2}{}$	$\binom{0}{}$	$\binom{6}{}$	$\binom{4}{}$	$\binom{2}{}$
1	$\binom{7}{}$	$\binom{6}{}$	$\binom{5}{}$	$\binom{4}{}$	$\binom{3}{}$	$\binom{2}{}$	$\binom{}{}$

F_M is an
M x M matrix

Computable in $O(\log^2 M)$

1	1	1	1	1	1	1	1
1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
1	ω^2	ω^4	ω^6	ω^0	ω^2	ω^4	ω^6
1	ω^3	ω^6	ω	ω^4	ω^7	ω^2	ω^5
1	ω^4	ω^0	ω^4	ω^0	ω^4	ω^0	ω^4
1	ω^5	ω^2	ω^7	ω^4	ω	ω^6	ω^3
1	ω^6	ω^4	ω^2	ω^0	ω^6	ω^4	ω^2
1	ω^7	ω^6	ω^5	ω^4	ω^3	ω^2	ω

$F_4 \cdot \mathrm{diag}($

1	ω	ω^2	ω^3

$) =$

1	1	1	1
1	ω^2	ω^4	ω^6
1	ω^4	ω^0	ω^4
1	ω^6	ω^4	ω^2

1	ω	ω^2	ω^3
1	ω^3	ω^6	ω
1	ω^5	ω^2	ω^7
1	ω^7	ω^6	ω^5

$T(M) = T(M/2) + \log M \quad \Rightarrow \quad T(M) = \log^2 M$

Summary - QFTs

$$F_M = \sum_{i,j=0} \omega^{ij} |i\rangle\langle j|$$

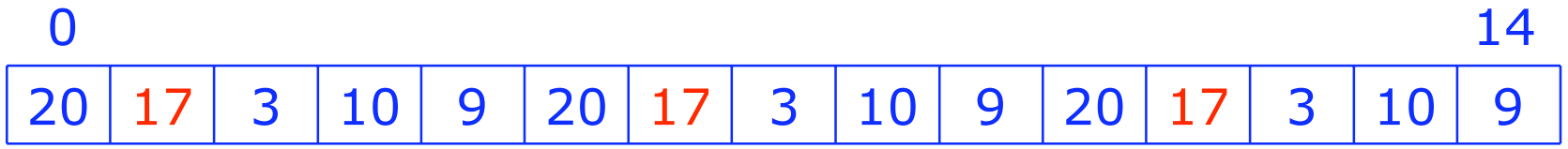
- Unitary
- Computed in $O(\log^2 M)$
- Finds periodicities

Simon's Problem for $\mathbb{Z}_M$

Given: function $f: \mathbb{Z}_M \rightarrow A$ (Arbitrary set)
with period s:

$$f(x)=f(x+s)=f(x+2s)=\ldots$$

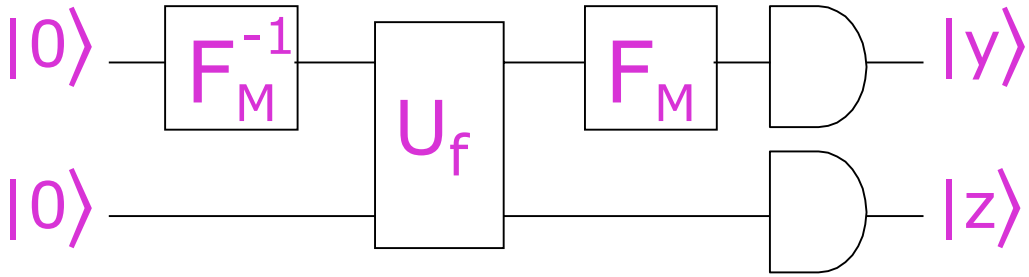
f is unique within each period



Period s = 5

We assume s divides M

Quantum algorithm

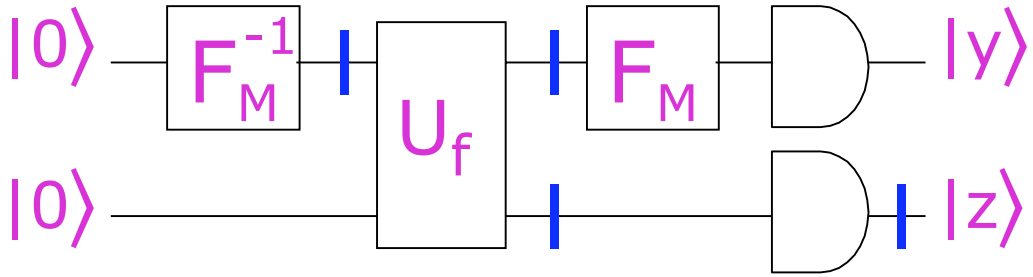


Theorem: $y \in_{random} \{0, M/s, 2M/s, \ldots, (s-1)M/s\}$

Corollary: We can find period s using only 10 queries

- Repeat 10 times. Obtain $y_1, y_2, \ldots, y_{10}$.
- Compute $d = GCD(y_1, y_2, \ldots, y_{10})$.
  Then with high prob., $d = M/s$.
- Output M/d.

Analysis



$$|0\rangle \rightarrow \sum_{j=0}^{M-1} |j\rangle \rightarrow \sum_{j=0}^{M-1} |j\rangle\,|f(j)\rangle \rightarrow \sum_{r=0}^{M/s-1} |k+rs\rangle\,|z\rangle$$

$$|\psi_k\rangle := \sum_{r=0}^{M/s-1} |k+rs\rangle$$

Lemma: $F_M\,|\psi_k\rangle = \sum_{t=0}^{s-1} \omega_s^{tk}\,|t\ M/s\rangle$

Main proof

$|\psi_k\rangle := \sum_{r=0}^{M/s-1} |k+rs\rangle$

Lemma: $F_M |\psi_k\rangle = \sum_{t=0}^{s-1} \omega_s^{tk} |t\ M/s\rangle$

Pf: $F_M |\psi_k\rangle = \sum_{i,j=0}^{M-1} \omega^{ij} |i\rangle\langle j| \sum_{r=0}^{M/s-1} |k+rs\rangle$

$= \sum_{i=0}^{M-1} |i\rangle \ (\sum_{r=0}^{M/s-1} \sum_{j=0}^{M-1} \omega^{ij} \langle j|k+rs\rangle)$

$= \sum_{i=0}^{M-1} |i\rangle \ (\sum_{r=0}^{M/s-1} \omega^{i(k+rs)})$

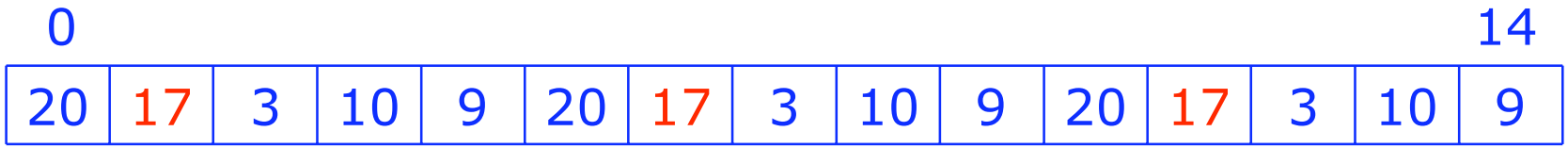
$= \sum_{i=0}^{M-1} \omega^{ik} |i\rangle \ (\sum_{r=0}^{M/s-1} \omega^{irs})$

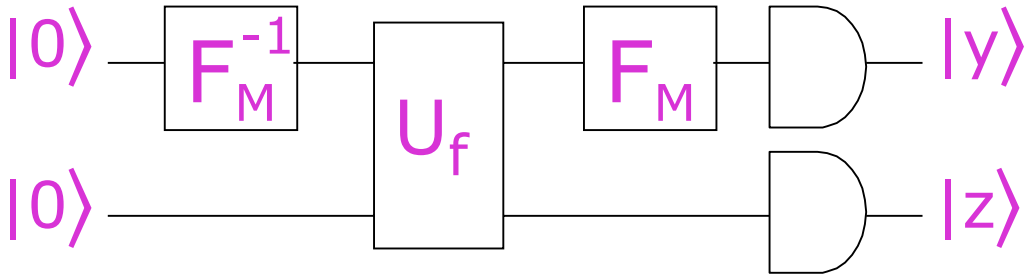
$= \sum_{i=0}^{M-1} \omega^{ik} |i\rangle \ (\sum_{r=0}^{M/s-1} \omega_{M/s}^{ir})$

$= \sum_{i=tM/s} \omega^{ik} |i\rangle$ ω

Summary

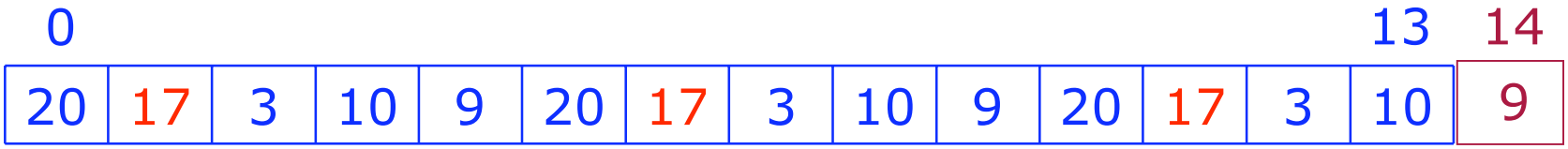
$$F_M = \sum_{i,j=0} \omega^{ij} |i\rangle\langle j|$$





Variation of **Hidden Periodicity**

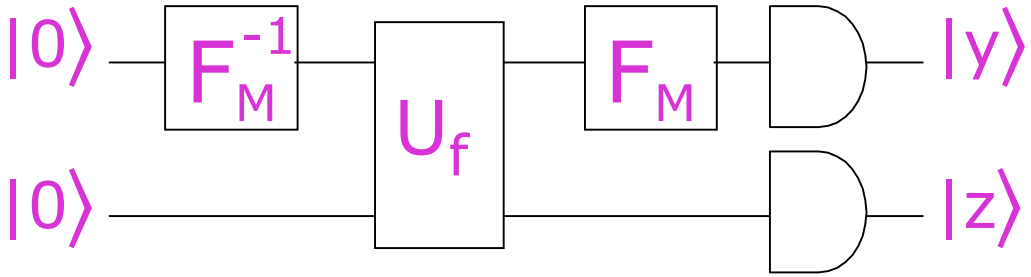
Given: function $f: \mathbb{Z}_M \rightarrow A$ (Arbitrary set)
with period s:
f(x)=f(x+s)=f(x+2s)=…
Unique within each period



Period s = 5

do NOT assume s divides M

Quantum algorithm



Theorem: $y/M \approx t/s$ for some integer $t \in \{0, 1, 2, ..., s-1\}$

$y = y_{random}$ for some integer $t \in \{0, M/s, 2M/s, ..., (s-1)M/s\}$

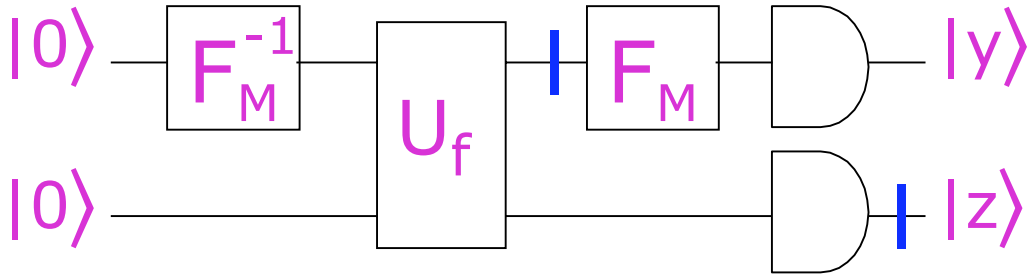
Corollary: We can find period s using only 10 queries

- Repeat 10 times. Obtain $y_1, y_2, \ldots, y_{10}$.
- Compute $s = GCD(y_1, y_2, \ldots, y_{10})$.
- Then with high probability $s = LCM(s_1, s_2) = LCM(s_2, s_4, s_7)$.
- Output the LCM.

Find integers t_1 and s_1 such that $y_1/M \approx t_1/s_1$.

Compute M/d.

Analysis



$$|0\rangle \rightarrow \sum_{j=0}^{M-1} |j\rangle \rightarrow \sum_{j=0}^{M-1} |j\rangle\,|f(j)\rangle \rightarrow \sum_{r=0}^{\lfloor (M-k-1)/s \rfloor} |k+rs\rangle\,|z\rangle$$

$$|\psi_k\rangle := \sum_{r=0}^{\lfloor (M-k-1)/s \rfloor} |k+rs\rangle$$

Lemma: $F_M\,|\psi_k\rangle \approx \sum_{t=0}^{s-1} {}_{-s}^{tk} \{\,|\,\lfloor t\,M/s \rfloor\,\rangle + |\,\lceil t\,M/s \rceil\,\rangle\}$

Technicality: we require that $M > s^2$

Finding a **Hidden Periodicity**

Given: function f: $\mathbb{Z}_M \rightarrow A$ (Arbitrary set)
with period s:
f(x)=f(x+s)=f(x+2s)=…

Assume: - Unique within each period
- $M > s^2$

Theorem: Can find s using 10 queries to f

Reducing Factoring

Factoring

Order Finding

Hidden Periodicity

Order Finding

$\mathbb{Z}_N = \{0,1,\ldots, N-1\}$

$\mathbb{Z}_N^* = \{ a \in \mathbb{Z}_N : \mathrm{GCD}(a,N)=1 \}$

eg, $\mathbb{Z}_{21}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$

order(a) := min{ s > 0 : $a^s \equiv 1 \pmod N$}

$\mathbb{Z}_{21}^*$	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9
a=2	2	4	8	16	11	1	2	4	8
a=5	5	4	20	16	17	1	5	4	20
a=8	8	1	8	1	8	1	8	1	8

Integer Factorization

Input:	Output:
N=21	$N = 3 \cdot 7$
N=4399	$N = 53 \cdot 83$
N=9831	$N = 87 \cdot 113$

RSA awards you for a successful factorization:

$10,000:

188198812920607963838697239461650439807163563379417382700763356422988597152346654853190606065047430453173880113033967161996923212057340318795506569962213051687593076502570 59

Input size = number of digits in N

Factoring → Order Finding

We want to factorize N. Let $a \in \mathbb{Z}_N^*$, s = order(a).

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

$$\Rightarrow \quad a^s - 1 \equiv 0 \pmod N$$

$$\Rightarrow \quad (a^{s/2} + 1)(a^{s/2} - 1) \equiv 0 \pmod N \qquad \text{if s even}$$

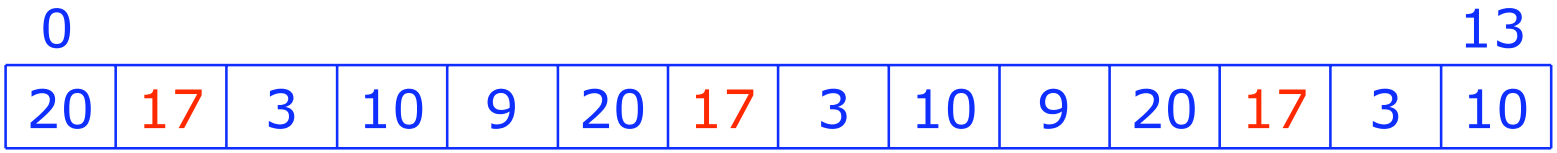
$\Rightarrow$ Each factor of N divides $(a^{s/2} + 1)$ or $(a^{s/2} - 1)$

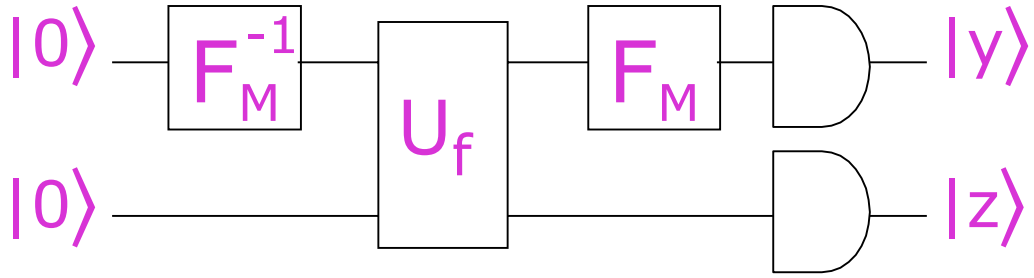
$\Rightarrow$ GCD(N, $a^{s/2} + 1$) is a proper factor of N - if lucky

Fact: if we choose $a \in \mathbb{Z}_N^*$ uniformly, then s is even and we are lucky, with probability at least 1/2.

Summary

$$F_M = \sum_{i,j=0} \omega^{ij} |i\rangle\langle j|$$





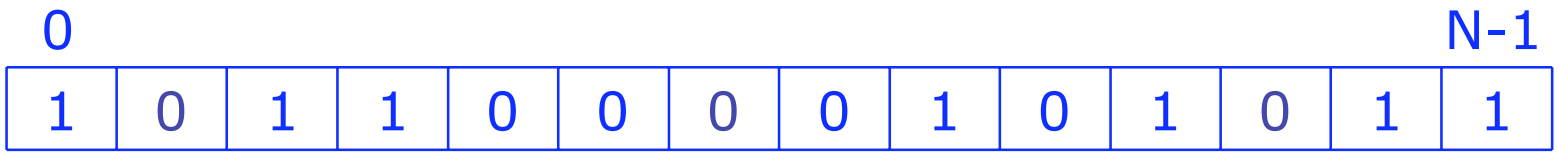
Factoring → Order Finding

→ Hidden Periodicity

Other applications of QFTs

- Phase Estimation

- Quantum Counting



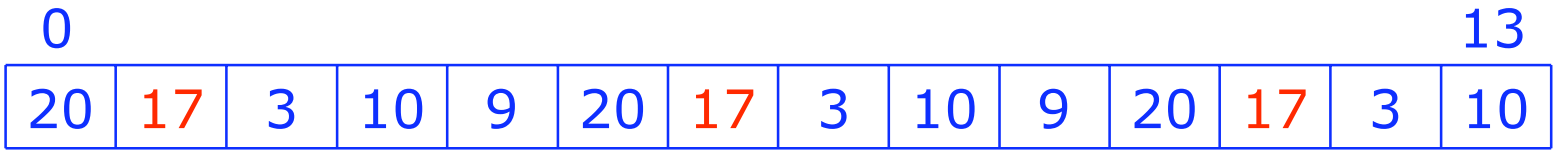
- Discrete Logarithms modulo a prime p

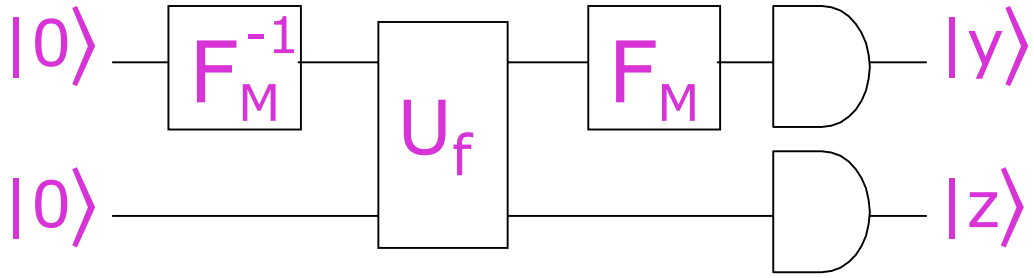
  Order finding: $a^s \equiv 1 \pmod N$

  Discrete logs: $g^r \equiv x \pmod p$

Summary

$$F_M = \sum_{i,j=0} \omega^{ij} |i\rangle\langle j|$$





Factoring → Order Finding

→ Hidden Periodicity