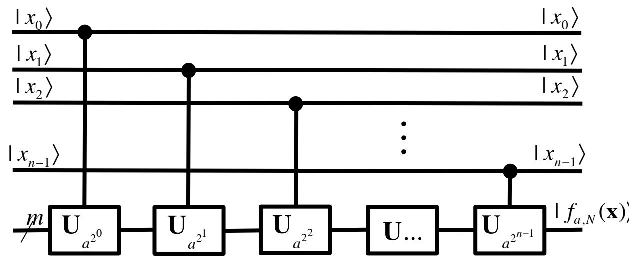
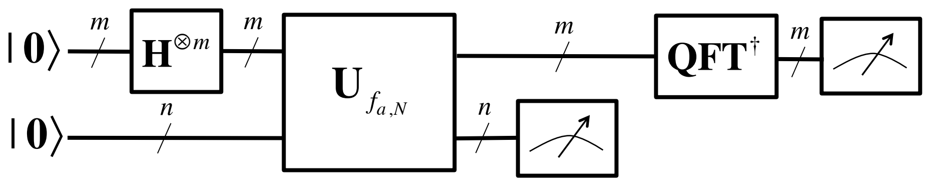
Shor's Factoring Algorithm





Shor's Factoring Algorithm

- Factoring Composite Numbers Very Important and Used for Security (Encryption)
- Method Reduces Factoring Problem to Finding Period of Function
- Deterministic Polynomial Algorithm Exists for Determining if a Value is Prime
  - Agrawal, Kayal, and Saxena, 2004
- Assumed Number is Already Checked for Primality

Modular Operation

- Modular Arithmetic
- Notation Where k, j, and r are Integers

$$|k|_j = r$$

- Denotes the Congruence:

$$k \equiv r \pmod{j} \Rightarrow k \pmod{j} = r \pmod{j}$$

- Such that:

$$j > 0 \qquad 0 \le r \le j-1$$

- Examples:

$|7|_{15} = 7$ $\quad |199|_{15} = 4$ $\quad |23374|_{371} = 1$

$|99|_{15} = 9$ $\quad |5317|_{371} = 123$ $\quad |1446|_{371} = 333$

Euclid's Algorithm

- Method for Computing the Greatest Common Divisor (GCD)
- GCD of Two Numbers is the Largest Number that Divides Both WITH a Zero-Valued Remainder
- Principle is GCD of Two Numbers Does Not Change if Smaller Number is Subtracted from Larger Number:

$$GCD(252,105) = 21$$

$$GCD(252,105) = GCD(252-105,105) = GCD(147,105) = 21$$

$$= GCD(147,105) = GCD(147-105,105) = GCD(42,105)$$

$$GCD(42,105) = GCD(63,42) = GCD(42,21) = GCD(21,0) = 21$$

CoPrimes

- Coprime Definition:
- Two Numbers a and b are Coprime if:

$$GCD(a,b) = 1$$

- When Searching for Factor of Number N:
  - Randomly Choose some value a Where $a<N$
  - Invoke Euclid's Algorithm for $\mathrm{GCD}(a, N)$
  - If $\mathrm{GCD}(a, N)\neq 1$, Then Factor of N is Found
  - If $\mathrm{GCD}(a, N)=1$, Then a is Coprime to N and can be Used
- Next, we Find Powers of a Modulo N:

$$|a^0|_N, |a^1|_N, |a^2|_N, |a^3|_N, ...$$

Modular Powers Function

- Finding Powers of a Modulo N Equivalent to Finding Values of Function:

$$f_{a,N}(x) = a^x (\mathrm{mod}\ N) = |a^x|_N$$

- EXAMPLE: $N=15$ and $a=2$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{2,15}(x)$	1	2	4	8	1	2	4	8	1	2	4	8	1	…

- EXAMPLE: $N=15$ and $a=4$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{4,15}(x)$	1	4	1	4	1	4	1	4	1	4	1	4	1	…

Modular Powers Function

- Finding Powers of a Modulo N Equivalent to Finding Values of Function:

$$f_{a,N}(x) = a^x (\text{mod } N) = | a^x |_N$$

- EXAMPLE: N=15 and a=13:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{13,15}(x)$	1	13	4	7	1	13	4	7	1	13	4	7	1	…

Modular Powers Function

- Useful Identities:

if $a \equiv a' (\text{mod } N)$ and $b \equiv b' (\text{mod } N)$

then $a \times b \equiv a' \times b' (\text{mod } N)$

$$| a \times b |_N = \left| | a |_N \times | b |_N \right|_N$$

$$| a^x |_N = | a^{x-1} \times a |_N = \left| | a^{x-1} |_N \times | a |_N \right|_N$$

- Since $a<N$ and $|a|_N=a$, Above Reduces to:

$$| a^x |_N = \left| | a^{x-1} |_N \times a \right|_N$$

- This Identity Allows Larger Values to be Used

Modular Powers Function

$$f_{a,N}(x) = a^x (\text{mod } N) = | a^x |_N$$

- EXAMPLE: N=371 and a=2:

x	0	1	2	3	4	5	6	7	…	78	…	155	156	157	158	…
$f_{2,371}(x)$	1	2	4	8	16	32	64	128	…	211	…	186	1	2	4	…

- EXAMPLE: N=371 and a=6:

x	0	1	2	3	4	5	6	7	…	13	…	25	26	27	28	…
$f_{6,371}(x)$	1	6	36	216	183	356	281	202	…	370	…	62	1	6	36	…

- EXAMPLE: N=371 and a=24:

x	0	1	2	3	4	5	6	7	…	39	…	77	78	79	80	…
$f_{24,371}(x)$	1	24	205	97	102	222	134	248	…	160	…	201	1	24	205	…

Modular Powers Function

- These Functions are Periodic
- We Only Need Period of Function
- Period: Find Smallest $x > 0$ Such That:

$$f_{a,N}(x) = a^x (\text{mod } N) = | a^x |_N = 1$$

- Number Theory Theorem: For any coprime $a \leq N$, the function $f_{a,N}$ will evaluate to 1 for some $x<N$. After, $f_{a,N}$ evaluates to 1, the sequence of function values repeats.
- If $f_{a,N}(x)$=1, then

$$f_{a,N}(x+1) = f_{a,N}(1) \qquad f_{a,N}(x+s) = f_{a,N}(s)$$

Finding the Period

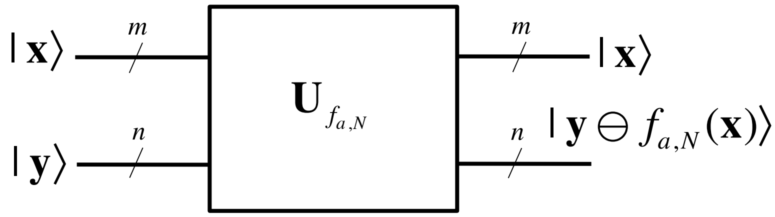
- For Small Numbers (15, 371, 247) Easy to Compute the Period
- Large Numbers with Hundreds of Digits are Beyond Capability of Classical Computers
- Use Quantum Computer with Qubit Superposition to Calculate $f_{a,N}(x)$ for all Needed x
- Must First Synthesize $f_{a,N}(x)$ into a Quantum Cascade

Period Finding Quantum Circuit

- Number of Qubits Required
  - $f_{a,N}$ Always Evaluates to to Value Less Than N
  - Need $n=\log_2(N)$ Qubits to Represent Function Value
  - Need to Evaluate $f_{a,N}$ for at Least First N^2 Values of x, Thus Need $m=\log_2(N^2)=2\log_2(N)=2n$ Qubits for x Values
- Quantum Circuit Represented by Operator:

$$\mathbf{U}_{f_{a,N}}$$

Period Finding Quantum Circuit



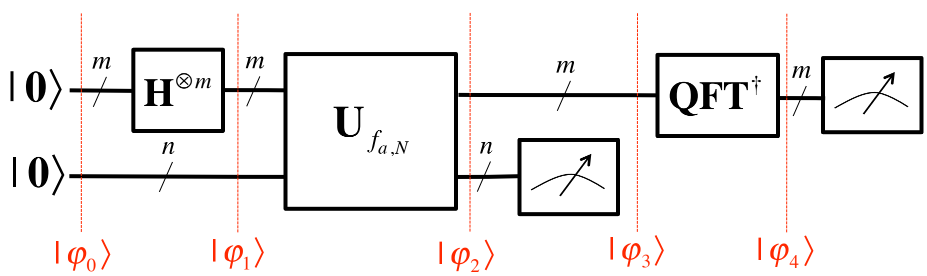
$$|\mathbf{x},\mathbf{y}\rangle \mapsto |\mathbf{x},\mathbf{y}\ominus f_{a,N}(\mathbf{x})\rangle = |\mathbf{x},\left|\mathbf{y}\oplus a^{\mathbf{x}}\right|_N\rangle$$

$$n=\left\lceil \log_2(N)\right\rceil$$

$$m=\left\lceil \log_2(N^2)\right\rceil=\left\lceil 2\log_2(N)\right\rceil=2n$$

- Discussion of Circuit Structure Postponed for Now

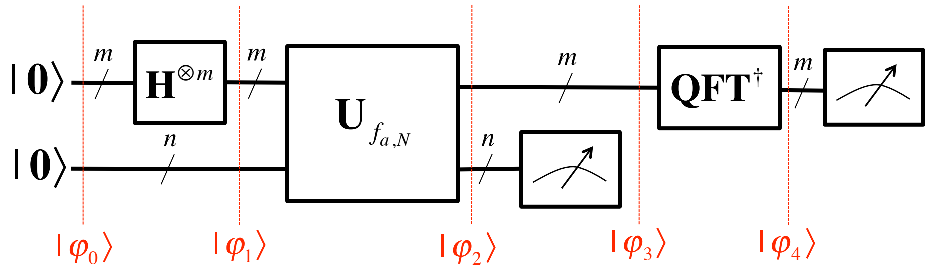
Quantum Circuit



- Evaluate All Input Simultaneously Through Superposition
- Quantum Circuit Transfer Matrix:

$$\left(Measure_m\otimes\mathbf{I}_n\right)\left(\mathbf{QFT}_m^{\dagger}\otimes\mathbf{I}_n\right)\left(\mathbf{I}_m\otimes Measure_n\right)\mathbf{U}_{f_{a,N}}\left(\mathbf{H}^{\otimes m}\otimes\mathbf{I}_n\right)|\mathbf{0}_m,\mathbf{0}_n\rangle$$

Quantum Circuit



$$|\varphi_0\rangle = |\mathbf{0}_m, \mathbf{0}_n\rangle = |\mathbf{0}_m\rangle \otimes |\mathbf{0}_n\rangle$$

$$|\varphi_1\rangle = \left(\mathbf{H}^{\otimes m} \otimes \mathbf{I}_n\right)|\mathbf{0}_m, \mathbf{0}_n\rangle = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, \mathbf{0}_n\rangle}{\sqrt{2^m}}$$

$$|\varphi_2\rangle = \left(\mathbf{H}^{\otimes m} \otimes \mathbf{I}_n\right)\mathbf{U}_{f_{a,N}}\,|\mathbf{0}_m, \mathbf{0}_n\rangle = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, f_{a,N}(\mathbf{x})\rangle}{\sqrt{2^m}} = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, \left|a^{\mathbf{x}}\right|_N\rangle}{\sqrt{2^m}}$$

Example Calculation 1

$$|\varphi_2\rangle = \left(\mathbf{H}^{\otimes m} \otimes \mathbf{I}_n\right)\mathbf{U}_{f_{a,N}}\,|\mathbf{0}_m, \mathbf{0}_n\rangle = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, f_{a,N}(\mathbf{x})\rangle}{\sqrt{2^m}} = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, \left|a^{\mathbf{x}}\right|_N\rangle}{\sqrt{2^m}}$$

- Assume N=15 and a=13:

$$n = \lceil \log_2(N) \rceil = \lceil \log_2(15) \rceil = 4$$

$$m = \lceil \log_2(15^2) \rceil = 2\lceil \log_2(15) \rceil = 2 \times 4 = 8$$

$$|\varphi_2\rangle = \frac{|0,1\rangle + |1,13\rangle + |2,4\rangle + |3,7\rangle + |4,1\rangle + \ldots + |254,4\rangle + |255,7\rangle}{\sqrt{256}}$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{13,15}(x)$	1	13	4	7	1	13	4	7	1	13	4	7	1	…

Example Calculation 2

$$|\varphi_2\rangle = \left(\mathbf{H}^{\otimes m} \otimes \mathbf{I}_n\right)\mathbf{U}_{f_{a,N}}\,|\mathbf{0}_m,\mathbf{0}_n\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, f_{a,N}(\mathbf{x})\rangle}{\sqrt{2^m}} = \frac{\sum_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}, \left|a^{\mathbf{x}}\right|_N\rangle}{\sqrt{2^m}}$$

- Assume N=371 and a=24:

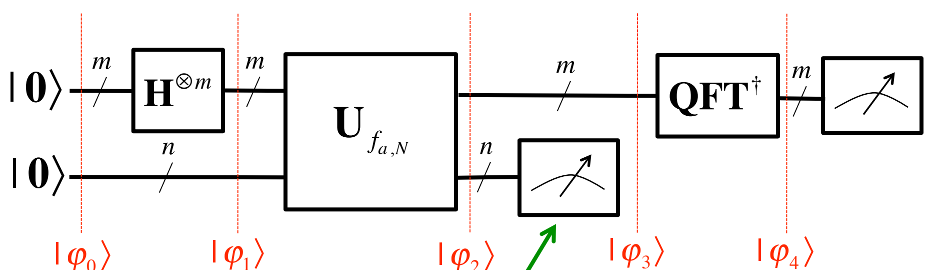
$$n = \lceil \log_2(N) \rceil = \lceil \log_2(371) \rceil = 9$$

$$m = \lceil \log_2(371^2) \rceil = 2\lceil \log_2(371) \rceil = 2 \times 9 = 18$$

$$|\varphi_2\rangle = \frac{|0,1\rangle + |1,24\rangle + |2,205\rangle + |3,97\rangle + |4,102\rangle + \ldots + |2^{18}-1, \left|24^{2^{18}-1}\right|_{371}\rangle}{\sqrt{2^{18}}}$$

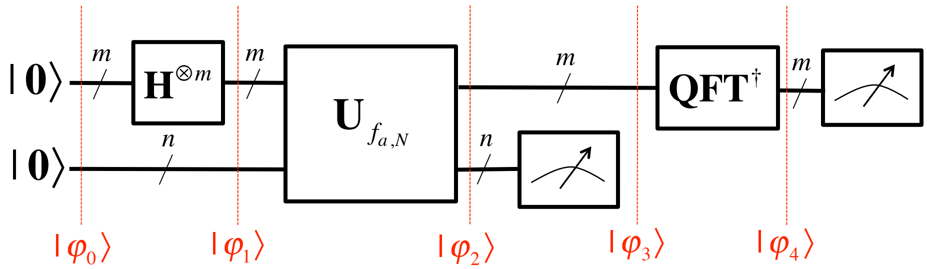
x	0	1	2	3	4	5	6	7	…	39	…	77	78	79	80	…
$f_{24,371}(x)$	1	24	205	97	102	222	134	248	…	160	…	201	1	24	205	…

Quantum Circuit



- Measure Bottom n Qubits of
- Bottom n Qubits are in State of Superposition Before Measurement
- Assume We Measure: $\left|a^{\bar{\mathbf{x}}}\right|_N$
- For Some Particular Bitstring: $\bar{\mathbf{x}}$

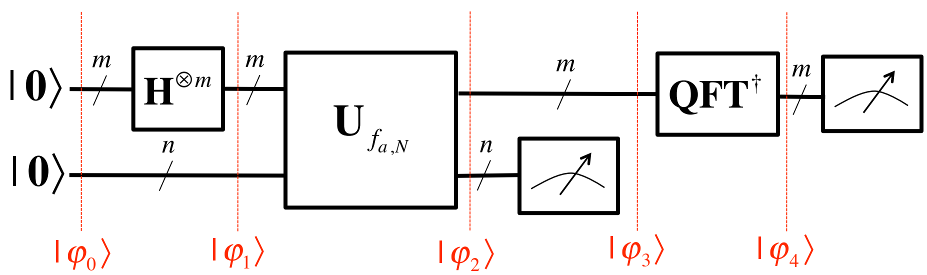
Quantum Circuit



- Assume We Measure: $\left|a^{\bar{\mathbf{x}}}\right|_N$
- For Some Particular Bitstring: $\bar{\mathbf{x}}$
- Since $f_{a,N}$ is Periodic: $a^{\bar{\mathbf{x}}} \equiv \left|a^{\bar{\mathbf{x}}+r}\right|_N$ And $a^{\bar{\mathbf{x}}} \equiv \left|a^{\bar{\mathbf{x}}+2r}\right|_N$
- For any $s \in \mathbb{Z}$

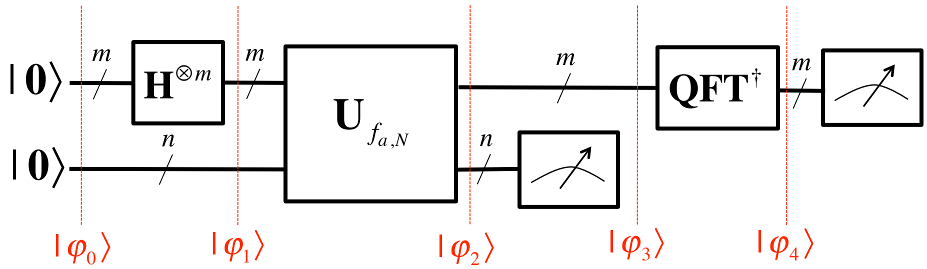
$$a^{\bar{\mathbf{x}}} \equiv \left|a^{\bar{\mathbf{x}}+sr}\right|_N$$

Quantum Circuit



- There are 2^m Superpositions in $|\varphi_2\rangle$
- The Number of Superpositions that have $\left|a^{\bar{\mathbf{x}}}\right|_N$ as the Result are $\left\lfloor \frac{2^m}{r} \right\rfloor$
- This Result is used in the Expression for $|\varphi_3\rangle$

Quantum Circuit

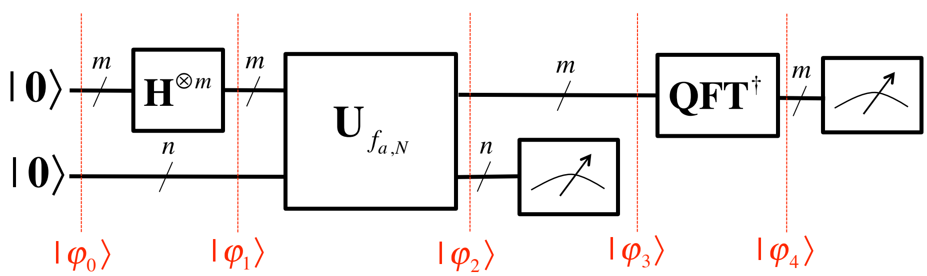


$$|\varphi_3\rangle = \frac{\sum_{a^{\mathbf{x}} \equiv |a^{\bar{\mathbf{x}}}|_N} |\mathbf{x}, |a^{\bar{\mathbf{x}}}|_N\rangle}{\left\lfloor \frac{2^m}{r} \right\rfloor} = \frac{\sum_{j=0}^{2^m/(r-1)} |t_0 + jr, |a^{\bar{\mathbf{x}}}|_N\rangle}{\left\lfloor \frac{2^m}{r} \right\rfloor}$$

- t_0 is the Offset, the First Occurrence of:

$$a^{t_0} \equiv |a^{\bar{\mathbf{x}}}|_N$$

Quantum Circuit



- t_0 is Called the Offset
- $|\varphi_3\rangle$ Stage Employs Entanglement
- Top m and Bottom n Qubits are Entangled Such That When Bottom n are Measured, the Top m Retain Their State

Example Calculation 1

- Recall Earlier Result:

$$|\varphi_2\rangle = \frac{|0,1\rangle + |1,13\rangle + |2,4\rangle + |3,7\rangle + |4,1\rangle + \ldots + |254,4\rangle + |255,7\rangle}{\sqrt{256}}$$

- Assume that After Measurement of Bottom n=4 Qubits, the Value 7 is Obtained:

$$\overline{\mathbf{x}} = 0111 = 7$$

- The Quantum State Becomes:

$$|\varphi_3\rangle = \frac{|3,7\rangle + |7,7\rangle + |11,7\rangle + |15,7\rangle + \ldots + |251,7\rangle + |255,7\rangle}{\left\lceil \frac{256}{4} \right\rceil}$$

Example Calculation 2

- Recall Earlier Result:

$$|\varphi_2\rangle = \frac{|0,1\rangle + |1,24\rangle + |2,205\rangle + |3,97\rangle + |4,102\rangle + \ldots + |2^{18}-1, \left|24^{2^{18}-1}\right|_{371}\rangle}{\sqrt{2^{18}}}$$

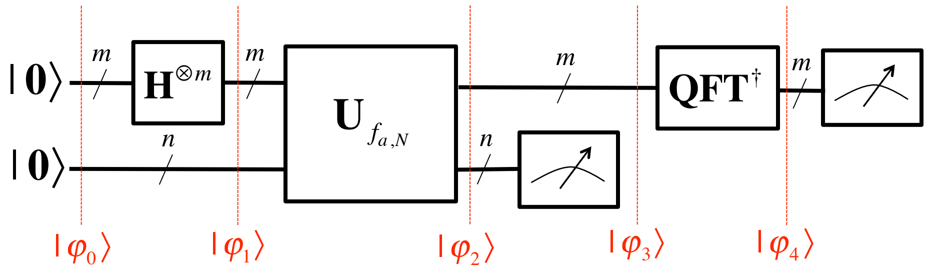
- Assume that After Measurement of Bottom n=9 Qubits, the Value 222 is Obtained:

$$\overline{\mathbf{x}} = 011011110 = 222 = \left|24^5\right|_{371}$$

- The Quantum State Becomes:

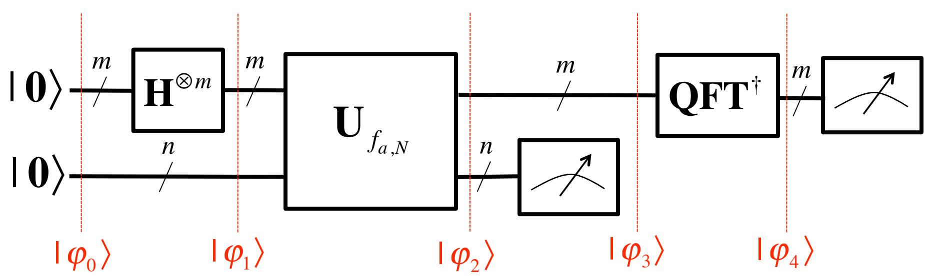
$$|\varphi_3\rangle = \frac{|5,222\rangle + |83,222\rangle + |161,222\rangle + |239,222\rangle + \ldots}{\left\lceil \frac{2^{18}}{78} \right\rceil}$$

Quantum Circuit



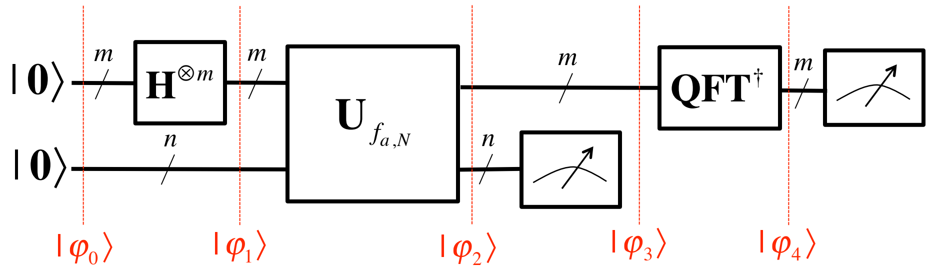
- $|\varphi_4\rangle$ Step of the Quantum Part of Algorithm is Application of the Inverse Quantum Fourier Transform
- Final Step of Algorithm Measures the Top m Qubits

Quantum Circuit



- Make Simplifying Assumption that r Evenly Divides into 2^m
- Shor's Actual Algorithm Does Not Make this Assumption

Quantum Circuit



- With Simplifying Assumption, We Measure:

$$x = \frac{\lambda 2^m}{r}$$

- Where λ is Some Whole Number

Quantum Circuit

- Known Values After Measurement are 2^m and x
- Dividing Whole Number x by 2^m Yields

$$\frac{x}{2^m} = \frac{\lambda 2^m}{r 2^m} = \frac{\lambda}{r}$$

- $\frac{\lambda}{r}$ is Reduced to an Irreducible Fraction and Denominator Then Becomes the Sought After r Value (the period)
- Without Simplifying Assumption, Process is Repeated and Results are Analyzed to Obtain r

Using Period to Get Factors

- We now Know the Period of $f_{a,N}$ for Some Value of a
- Number Theory Theorem States that for the Majority of a Values, r is an Even Number
- If it Turns Out that r is Odd, We Throw the Result Out and Try Again by Choosing Another a Value
- Once Even r is Found, We Have:

$$a^r \equiv |1|_N$$

Using Period to Get Factors

- Subtracting 1 From Both Sides of the Congruence Yields:

$$a^r - 1 \equiv |0|_N$$

$$N \mid \left(a^r - 1\right)$$

- Using the Facts:

$$1 = 1^2 \qquad x^2 - y^2 = (x+y)(x-y)$$

- Results in:

$$N \mid \left(a^r - 1\right) = N \mid \left(\sqrt{a^r} + 1\right)\left(\sqrt{a^r} - 1\right) = N \mid \left(a^{\frac{r}{2}} + 1\right)\left(a^{\frac{r}{2}} - 1\right)$$

Using Period to Get Factors

- Since r is Even, Exponent Yields a Whole Number

$$N \mid \left(a^r - 1\right) = N \mid \left(\sqrt{a^r} + 1\right)\left(\sqrt{a^r} - 1\right) = N \mid \left(a^{\frac{r}{2}} + 1\right)\left(a^{\frac{r}{2}} - 1\right)$$

- Any Factor of N is Also a Factor of $\left(a^{\frac{r}{2}} + 1\right)$ or $\left(a^{\frac{r}{2}} - 1\right)$
- Can Employ Classical Euclid's Algorithm to Search for Factor of N

$$\mathrm{GCD}\left(\left(a^{\frac{r}{2}} + 1\right), N\right) \text{ or } \mathrm{GCD}\left(\left(a^{\frac{r}{2}} - 1\right), N\right)$$

Using Period to Get Factors

- Problem Can Occur if: $a^{\frac{r}{2}} \equiv \left|-1\right|_N$
- When This Occurs Right Side of Following Equation Becomes Zero and no Information about N Results

$$N \mid \left(a^{\frac{r}{2}} + 1\right)\left(a^{\frac{r}{2}} - 1\right)$$

- If This Occurs Must Try Again With Different Value of a

GCD and Factor Example

- Period of $f_{2,15}$ is 4 or: $2^4 \equiv |1|_{15}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{2,15}(x)$	1	2	4	8	1	2	4	8	1	2	4	8	1	…

- Using Previous Result with GCD:

$$15 \mid \left(2^2+1\right)\left(2^2-1\right)$$

$$\mathrm{GCD}\left(5,15\right)=5 \qquad \mathrm{GCD}\left(3,15\right)=3$$

GCD and Factor Example

- Period of $f_{6,371}$ is 26 or: $6^{26} \equiv |1|_{371}$

x	0	1	2	3	4	5	6	7	…	13	…	25	26	27	28	…
$f_{6,371}(x)$	1	6	36	216	183	356	281	202	…	370	…	62	1	6	36	…

- It Is Also True That:

$$6^{\frac{26}{2}} = 6^{13} \equiv |370|_{371} \equiv |-1|_{371}$$

- This is the Problem Case
- Must Discard $a=6$ and Try Again With New a Value

GCD and Factor Example

- Period of $f_{24,371}$ is 78 or $24^{78} \equiv |1|_{371}$

x	0	1	2	3	4	5	6	7	…	39	…	77	78	79	80	…
$f_{24,371}(x)$	1	24	205	97	102	222	134	248	…	160	…	201	1	24	205	…

- Checking for Problem Case:

$$24^{\frac{78}{2}} = 24^{39} \equiv |160|_{371} \neq |-1|_{371}$$

- Can Use This a Value

$$371 \mid \left(24^{39}+1\right)\left(24^{39}-1\right)$$

$$\mathrm{GCD}(161,371) = 7 \qquad \mathrm{GCD}(159,371) = 53$$

$$371 = 7 \times 53$$

Shor's Factoring Algorithm

Input: Positive Integer N with $n = \lceil \log_2(N) \rceil$

Output: Factor p of N if it Exists

1) Use classical polynomial algorithm to determine of N is prime or a power of a prime. If N is prime or power of prime, declare that it is and halt.
2) Randomly choose an integer a such that $1<a<N$. Invoke Euclid's algorithm to determine GCD(a,N). If GCD is not 1, Then Halt.

Shor's Factoring Algorithm

3) Use Quantum Circuit to find period r.

4) If r is odd or is the "problem case", return to step 2 and choose another a value.

5) Invoke Euclid's algorithm to calculate:

$$\mathrm{GCD}\left(\left(a^{\frac{r}{2}}+1\right),N\right) \text{ or } \mathrm{GCD}\left(\left(a^{\frac{r}{2}}-1\right),N\right)$$

Return at least one of the nontrivial solutions.

Implementing $\mathbf{U}f_{a,N}$

- Operation of $f_{a,N}(\mathbf{x})$ Considered on Bit-by-Bit Basis
- Radix Polynomial Representation of $\mathbf{x}$:

$$\mathbf{x} = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \ldots + x_2 2^2 + x_1 2^1 + x_0 2^0$$

$$f_{a,N}(\mathbf{x}) = \left|a^{\mathbf{x}}\right|_N = \left|a^{x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \ldots + x_2 2^2 + x_1 2^1 + x_0 2^0}\right|_N$$

$$f_{a,N}(\mathbf{x}) = \left|a^{x_{n-1}2^{n-1}}\right|_N \times \left|a^{x_{n-2}2^{n-2}}\right|_N \times \ldots \times \left|a^{x_1 2^1}\right|_N \times \left|a^{x_0 2^0}\right|_N$$

Implementing $\mathbf{U}f_{a,N}$

- Rewrite This as an Inductive Formula:

$$f_{a,N}(\mathbf{x}) = \left|a^{x_{n-1}2^{n-1}}\right|_N \times \left|a^{x_{n-2}2^{n-2}}\right|_N \times \ldots \times \left|a^{x_1 2^1}\right|_N \times \left|a^{x_0 2^0}\right|_N$$

$$y_0$$

$$y_1$$

$$y_{n-2}$$

$$y_{n-1}$$

$$f_{a,N}(\mathbf{x}) = y_{n-1} = y_{n-2} \times \left|a x_{n-1} 2^{n-1}\right|_N \qquad y_j = y_{j-1} \times \left|a^{x_j 2^j}\right|_N$$

Implementing $\mathbf{U}f_{a,N}$

$$y_j = y_{j-1} \times \left|a^{x_j 2^j}\right|_N$$

- When x_j=0 We Have:

$$y_j = y_{j-1}$$

- When x_j=1 We Should Multiply $y_{j\text{-}1}$ by:

$$\left|a^{x_j 2^j}\right|_N$$

- When a and N are Coprime, Operation of Multiplying by This Factor is Reversible and Unitary – Realizable as Quantum Cascade

Implementing $\mathbf{U}f_{a,N}$

- For Each j, There is a Unitary Operator:

$$\mathbf{U}_{\left|a^{2^j}\right|_N} \rightarrow \mathbf{U}_{a^{2^j}}$$

- Each of These Operators are Performed Conditionally Based on Value of x_j
- To Implement we use a Controlled Version of the Operator
- The Quantum Cascade has the Form as Shown on the Following Overhead

Implementing $\mathbf{U}f_{a,N}$