## Shor's factoring algorithm

Input: $N$, a number to be factored

1. pick a number $1 < a < N$
2. if $a$ and $N$ are not co-prime, compute $g = \text{GCD}(a, N)$ and $N/g$ as the factors, and stop.
3. otherwise, determine the period $r$ of the function $f_{a,N}(x) = a^x \bmod N$
4. if the period is odd, go back to step 1
5. compute $s = a^{\frac{r}{2}} \bmod N$
6. if $s = N - 1$ (equivalent to $-1 \bmod N$), go back to step 1
7. compute $g_1 = \text{GCD}(s+1, N)$ and $g_2 = \text{GCD}(s-1, N)$, and return them

## Example

Let $N = 395861$

Pick $a =$ `random.randrange(2, N)` $= 246793$, so function $f_{a,N}(x) = 246793^x \bmod 395861$

GCD(246793, 395861) $= 1$, so $a$ and $N$ are co-prime

Period $r$ of $f_{a,N}(x) =$ `findPeriod(246793, 395861)` $= 32881$

32881 is odd, so we need to pick another $a$

Pick $a =$ `random.randrange(2, N)` $= 188364$, so function $f_{a,N}(x) = 188364^x \bmod 395861$

GCD(188364, 395861) $= 1$, so $a$ and $N$ are co-prime

Period $r$ of $f_{a,N}(x) =$ `findPeriod(188364, 395861)` $= 197286$

197286 is even, so we can proceed

Compute $s = 188364^{197286/2} \bmod 395861 = 164482$

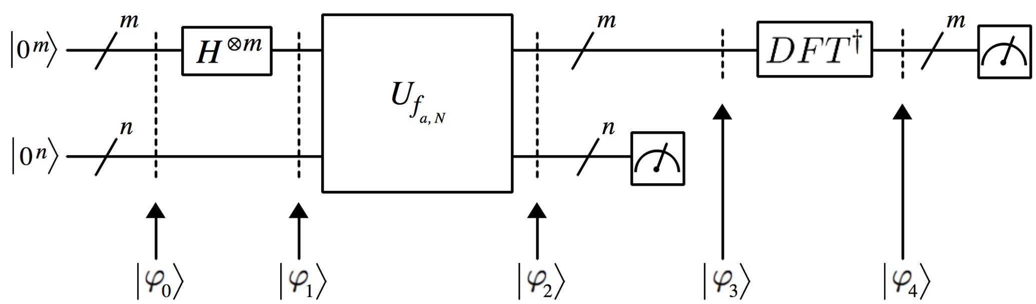
$164482 \neq 395860$, so we can proceed

Compute factor $g_1 = \text{GCD}(s + 1,\, N) = \text{GCD}(164483,\, 395861) = 787$

Compute factor $g_2 = \text{GCD}(s - 1,\, N) = \text{GCD}(164481,\, 395861) = 503$

Sure enough, $787 \times 503 = 395861 = N$

## A quantum circuit for finding the period $r$




Number to be factored $N = 8$, random co-prime $a = 3$, so the function is $f_{3,8}(x) = 3^x \bmod 8$

This function has period $r = 2$:

| $x$ | $f(x)$ |
|---|---|
| 0 | 1 |
| 1 | 3 |
| 2 | 1 |
| 3 | 3 |
| 4 | 1 |
| 5 | 3 |
| 6 | 1 |
| 7 | 3 |
| 8 | 1 |
| ... | |

In this example, the top register will hold $m = 3$ qubits, and the bottom register will hold $n = 2$ qubits. We start by creating an equal superposition of all values of $x$ in the top register, each one paired with 00 in the bottom register:

$$|\varphi_0\rangle = |000\rangle \otimes |00\rangle = |000, 00\rangle$$

$$|\varphi_1\rangle = \tfrac{1}{\sqrt{8}}\Big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\Big) \otimes |00\rangle$$

$$= \tfrac{1}{\sqrt{8}}\Big(|000, 00\rangle + |001, 00\rangle + |010, 00\rangle + |011, 00\rangle + |100, 00\rangle + |101, 00\rangle + |110, 00\rangle + |111, 00\rangle\Big)$$

$$= \tfrac{1}{\sqrt{8}}\Big(|0, 0\rangle + |1, 0\rangle + |2, 0\rangle + |3, 0\rangle + |4, 0\rangle + |5, 0\rangle + |6, 0\rangle + |7, 0\rangle\Big)$$

Next, we apply the unitary gate $U_{f_{3,8}}$ to all five qubits, which entangles each value of $x$ in the top register with its corresponding value $f_{3,8}(x)$ in the bottom register via quantum parallelism:

$$|\varphi_2\rangle = \tfrac{1}{\sqrt{8}}\Big(|0, 1\rangle + |1, 3\rangle + |2, 1\rangle + |3, 3\rangle + |4, 1\rangle + |5, 3\rangle + |6, 1\rangle + |7, 3\rangle\Big)$$

$$= \tfrac{1}{\sqrt{8}}\Big(|000, 01\rangle + |001, 11\rangle + |010, 01\rangle + |011, 11\rangle + |100, 01\rangle + |101, 11\rangle + |110, 01\rangle + |111, 11\rangle\Big)$$

The state vectors for $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are shown below:

$|\varphi_1\rangle =$

```
000,00 [  1/√8  ]
000,01 [     0  ]
000,10 [     0  ]
000,11 [     0  ]
001,00 [  1/√8  ]
001,01 [     0  ]
001,10 [     0  ]
001,11 [     0  ]
010,00 [  1/√8  ]
010,01 [     0  ]
010,10 [     0  ]
010,11 [     0  ]
011,00 [  1/√8  ]
011,01 [     0  ]
011,10 [     0  ]
011,11 [     0  ]
100,00 [  1/√8  ]
100,01 [     0  ]
100,10 [     0  ]
100,11 [     0  ]
101,00 [  1/√8  ]
101,01 [     0  ]
101,10 [     0  ]
101,11 [     0  ]
110,00 [  1/√8  ]
110,01 [     0  ]
110,10 [     0  ]
110,11 [     0  ]
111,00 [  1/√8  ]
111,01 [     0  ]
111,10 [     0  ]
111,11 [     0  ]
```

$|\varphi_2\rangle =$

```
000,00 [     0  ]
000,01 [  1/√8  ]
000,10 [     0  ]
000,11 [     0  ]
001,00 [     0  ]
001,01 [     0  ]
001,10 [     0  ]
001,11 [  1/√8  ]
010,00 [     0  ]
010,01 [  1/√8  ]
010,10 [     0  ]
010,11 [     0  ]
011,00 [     0  ]
011,01 [     0  ]
011,10 [     0  ]
011,11 [  1/√8  ]
100,00 [     0  ]
100,01 [  1/√8  ]
100,10 [     0  ]
100,11 [     0  ]
101,00 [     0  ]
101,01 [     0  ]
101,10 [     0  ]
101,11 [  1/√8  ]
110,00 [     0  ]
110,01 [  1/√8  ]
110,10 [     0  ]
110,11 [     0  ]
111,00 [     0  ]
111,01 [     0  ]
111,10 [     0  ]
111,11 [  1/√8  ]
```

Next, we measure the bottom two qubits. We will either observe **01** or **11**, at random, corresponding to the values $f_{3,8}(x) = 1$ or 3. Suppose we observe **11**, corresponding to 3. Because of entanglement, this will force the top three qubits into a new superposition state $|\varphi_3\rangle$ consisting of the possible values $x = 1$, 3, 5, or 7, but NOT the values 0, 2, 4, or 6.

$$|\varphi_3\rangle = \tfrac{1}{2}\Big(|001\rangle + |011\rangle + |101\rangle + |111\rangle\Big)$$

$$= \tfrac{1}{2}\Big(|1\rangle + |3\rangle + |5\rangle + |7\rangle\Big)$$

The new amplitudes of $|\varphi_3\rangle$ are $\dfrac{1}{\sqrt{\lfloor \frac{2^m}{r} \rfloor}} = \dfrac{1}{\sqrt{\lfloor \frac{2^3}{2} \rfloor}} = \frac{1}{2}$

$|\varphi_3\rangle =$

```
000 [    0  ]
001 [  1/2  ]
010 [    0  ]
011 [  1/2  ]
100 [    0  ]
101 [  1/2  ]
110 [    0  ]
111 [  1/2  ]
```

Notice that the non-zero amplitudes of $|\varphi_3\rangle$ are separated by intervals of length $r = 2$, equal to the period of $f$. But the first non-zero amplitude starts at $|001\rangle$, not $|000\rangle$. We need to transform $|\varphi_3\rangle$ so that the non-zero amplitudes start at $|000\rangle$. That is, we want to make the *amplitude offset* be 0. We can accomplish this by applying the matrix $DFT^\dagger$ to $|\varphi_3\rangle$ to obtain $|\varphi_4\rangle$:

$|\varphi_4\rangle \ =$

```
000 [   1/√2  ]
001 [      0  ]
010 [      0  ]
011 [      0  ]
100 [  -1/√2  ]
101 [      0  ]
110 [      0  ]
111 [      0  ]
```

The $DFT^\dagger$ transformation also transforms the interval between non-zero amplitudes from $r$ to $\frac{2^m}{r}$. Furthermore, the non-zero amplitude values change as well, since the new state vector contains a different number of them, compared to before. In the above case, the interval becomes $2^3/2 = 4$. Measuring $|\varphi_4\rangle$ will give either **000** or **100** with equal probability, corresponding to $x = 0$ or $x = 4$. If we get **100**, we know that the amplitude interval must be 4, since the amplitude offset is now guaranteed to be 0, and we can calculate the period $r$ directly:

$r = \dfrac{2^m}{x} = \dfrac{2^3}{4} = 2$, which is the correct period of $f_{3,8}$.

However, if measuring $|\varphi_4\rangle$ gives **000** instead, this will not tell us the amplitude interval. In general, we need to run the period-finding algorithm several times and accumulate an empirical set of measurements of $|\varphi_4\rangle$. We then look for the smallest non-zero value, which with high probability will correspond to the correct amplitude interval. From there, we can calculate the period $r$ as above.

## Discrete Fourier Transform

When the number of input qubits $m = 3$, the number of amplitudes $M = 2^m = 2^3 = 8$, so the DFT is an $8 \times 8$ matrix consisting of powers of the eighth root of unity $\omega = e^{\frac{\pi}{4}i}$, scaled by $\frac{1}{\sqrt{8}}$.

$$\mathrm{DFT}[row,\ col] = \frac{1}{\sqrt{M}}(\omega^{row})^{col}$$

$$= \frac{1}{\sqrt{8}} \begin{bmatrix} (\omega^0)^0 & (\omega^0)^1 & (\omega^0)^2 & (\omega^0)^3 & (\omega^0)^4 & (\omega^0)^5 & (\omega^0)^6 & (\omega^0)^7 \\ (\omega^1)^0 & (\omega^1)^1 & (\omega^1)^2 & (\omega^1)^3 & (\omega^1)^4 & (\omega^1)^5 & (\omega^1)^6 & (\omega^1)^7 \\ (\omega^2)^0 & (\omega^2)^1 & (\omega^2)^2 & (\omega^2)^3 & (\omega^2)^4 & (\omega^2)^5 & (\omega^2)^6 & (\omega^2)^7 \\ (\omega^3)^0 & (\omega^3)^1 & (\omega^3)^2 & (\omega^3)^3 & (\omega^3)^4 & (\omega^3)^5 & (\omega^3)^6 & (\omega^3)^7 \\ (\omega^4)^0 & (\omega^4)^1 & (\omega^4)^2 & (\omega^4)^3 & (\omega^4)^4 & (\omega^4)^5 & (\omega^4)^6 & (\omega^4)^7 \\ (\omega^5)^0 & (\omega^5)^1 & (\omega^5)^2 & (\omega^5)^3 & (\omega^5)^4 & (\omega^5)^5 & (\omega^5)^6 & (\omega^5)^7 \\ (\omega^6)^0 & (\omega^6)^1 & (\omega^6)^2 & (\omega^6)^3 & (\omega^6)^4 & (\omega^6)^5 & (\omega^6)^6 & (\omega^6)^7 \\ (\omega^7)^0 & (\omega^7)^1 & (\omega^7)^2 & (\omega^7)^3 & (\omega^7)^4 & (\omega^7)^5 & (\omega^7)^6 & (\omega^7)^7 \end{bmatrix} = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\ 1 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\ 1 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49} \end{bmatrix}$$

These numbers all have magnitude 1, and differ only in their phase.