One way to factor 15

The group of integers relatively prime to 15, \( G_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\} \), has 3 elements of order 2: \((4, 11, 14)\), and 4 elements of order 4: \((2, 7, 8, 13)\).

Note that \(7^x \mod 15 = 1, 7, 4, 13\), and \(8^x \mod 15 = 1, 8, 4, 2, 1, \ldots\).

To factor \(N = 15\), we need to pick some number \(b\) relatively prime to 15, and find the period of \(f(x) = b^x \mod 15\). We pick \(b = 7\) so that \(f(x) = 7^x \mod 15\), and implement

\[
U_f \mathcal{H}^\otimes n |0\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} |x\rangle_n |f(x)\rangle_{n_0}.
\]

For \(N = 15\), the first \(n_0\) such that \(2^{n_0} > N\) is \(n_0 = 4\), so by the general prescription we use \(n = 2n_0 = 8\) input qubits, and hence input states range from 0 to \(2^8 - 1 = 255\).

Suppose we measure the output qubits in the state \(|f(3)\rangle = |13\rangle\). 64 values of \(x\) in the range 0–255 map to 13, so the overall state is left as

\[
\left( \sum_{0 \leq x < 2^n} \gamma_x |x\rangle \right) |13\rangle = \frac{1}{8} \left( |3\rangle + |7\rangle + |11\rangle + \ldots + |255\rangle \right) |13\rangle.
\]

The amplitudes of the input bits are non-zero only for \(x = 3 \mod 4\), i.e., \(\gamma_x = (1/8)\delta_{x, 4k+3}\). As always, the result of the quantum Fourier transform on the state is a classical Fourier transform of the amplitudes, \(U_{\text{FT}} \sum_{x=0}^{2^n-1} \gamma_x |x\rangle = \sum_{y=0}^{2^n-1} \tilde{\gamma}_y |y\rangle\), where

\[
\tilde{\gamma}_y = \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} e^{2\pi i xy/2^n} \gamma_x = \frac{1}{16} \sum_{k=0}^{63} e^{2\pi i (4k+3)y/256} \frac{1}{8} = \frac{1}{128} e^{2\pi i 3y/256} \sum_{k=0}^{63} e^{2\pi i (4k)y/256}.
\]

This is non-zero only when \(2\pi 4y/256 = 2\pi y/64\) is equal to an integer multiple of \(2\pi\), hence only the values \(y = 0, 64, 128, 192\) will be measured, each with probability \((64/128)^2 = 1/4\).

In general if the original function \(f(x)\), and hence the amplitudes \(\gamma_x\), execute many periods \(r\) within the range from 0 to \(2^n - 1\), then the Fourier transform \(\tilde{\gamma}_y\) will be appreciable only near integral multiples of \(2^n/r\), and the measured \(y\) being close to some \(j \cdot 2^n/r\) can be used to infer the original period \(r\). Suppose we measure \(y = 64\). In this case, \(r\) happens to divide \(2^n\) (because \(p\) and \(q\) are of the form \(2^m + 1\)), so we learn directly from \(64 = j \cdot 256/r\) that \(r\) is a multiple of \(256/64 = 4\), and can check that \(7^4 = 1 \mod 15\), so \(r = 4\).

(Had we measured \(y = 128\), we would have inferred that \(r\) is a multiple of \(256/128 = 2\), and so checked \(7^2\) then \(7^4\) and concluded that \(r = 4\); and had we measured \(y = 192\), we’d learn that \(r\) is a multiple of \(256/192 = 4/3\), and the first integer multiple is again \(r = 4\).

To finish factoring 15, recall that \(0 = 7^4 - 1 = (7^2 - 1)(7^2 + 1) \mod 15\), then note that \(7^2 - 1 = 48 = 3 \mod 15\), and \(7^2 + 1 = 50 = 5 \mod 15\), determine (via Euclidean algorithm) that \(\gcd(15,3)=3\) and \(\gcd(15,5)=5\), and hence that 15 = 3 \cdot 5.