Ralph's quantum factoring

Ralph knows factoring a large number (say, 300 digits) into its prime numbers is a very computationally-intensive task. However, Shor's quantum factoring algorithm is exponentially faster than the best classical factoring algorithm. The algorithm is composed of two parts: classical and quantum order-finding utilizing the quantum period-finding algorithm (order-finding is a special case of period-finding where the function takes a specific form such as $f(x) = a^x \bmod N$).

The classical part.

Problem: we wish to factor the integer N.

1. Pick a random integer $a < N$.

2. Compute $GCD(a, N)$ (use Euclid's algorithm for greatest common divisor (GCD)).

3. If $GCD(a, N) = b \neq 1$, then the number is a nontrivial factor of N and the other factor is N/b.

The quantum part.

4. Otherwise, use the quantum period-finding algorithm (discussed below) to find r, the period of the function $f(x) = a^x \bmod N$. The period r is the smallest integer such that $f(x) = f(x + r)$.

5. If r is odd, go back to step 1.[1]

6. If $a^{r/2} \equiv -1 \bmod N$, go back to step 1.[2]

7. Otherwise, at least one of $GCD\left(a^{r/2} - 1, N\right)$ and $GCD\left(a^{r/2} + 1, N\right)$ are nontrivial factors of N and we are done.

Example. $N = 15, a = 7, r = 4, GCD\left(7^2 - 1, 15\right) = GCD(48, 15) = 3$, $GCD\left(7^2 + 1, 15\right) = GCD(50, 15) = 5$. For N that is a product of two distinct primes p and q, Euler's totient function $\varphi(N) = N - p - q + 1$ or $(p - 1)(q - 1)$. For $N = 15, \varphi(N) = 8$ and r divides 8. More generally, Euler's totient is the number of integers relatively prime to N. For $N = 15$, we have $1, 2, 4, 7, 8, 11, 13, 14$ or eight integers. Euler's totient function is $\varphi(N) = N \prod_{p(N)} \left(1 - \frac{1}{p(N)}\right)$ where $p(N)$ are the distinct prime factors of N. For $N = 15, \varphi(N) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8$.

Background.

The intuition for using GCD to find the factors stems from Fermat's factoring approach.

$$b^2 - c^2 = N \tag{1}$$

$$(b + c)(b - c) = N \tag{2}$$

$$(b + c)(b - c) \equiv 0 \bmod N \tag{3}$$

Utilize the period-finding function to set $b^2 = a^r$ or the square-root factor $b = \sqrt{a^r} = a^{r/2}$ and let $c = 1$, then substitution gives

$$\left(a^{r/2} + 1\right)\left(a^{r/2} - 1\right) \equiv 0 \bmod N \tag{4}$$

[1] We want to assure $a^{r/2}$ is an integer.

[2] We want to avoid the degenerate case where $GCD\left(a^{r/2} + 1, N\right)$ might be one.

This follows from properties of modular arithmetic. In particular, if $c_1 \equiv b_1 \bmod n$ and $c_2 \equiv b_2 \bmod n$, then $c_1 c_2 \equiv b_1 b_2 \bmod n$. Hence, if either is a factor of N their modular product is congruent to zero.

$$\left(a^{r/2}+1\right) \bmod N \left(a^{r/2}-1\right) \equiv 0 \bmod N \tag{5}$$

Quantum period-finding algorithm. As with many other quantum computational advantages, the key to quantum period-finding lies with the discrete quantum Fourier transform. The quantum Fourier transform is a unitary operator (symmetric but not Hermitian) whose inverse is simply the conjugate of the matrix (since the matrix is symmetric it is equal to its transpose). The discrete inverse quantum Fourier transform is

$$F_Q = \frac{1}{\sqrt{Q}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_n & \omega^2 & \omega^3 & \cdots & \omega^{Q-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(Q-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(Q-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{Q-1} & \omega^{2(Q-1)} & \omega^{3(Q-1)} & \cdots & \omega^{(Q-1)(Q-1)} \end{bmatrix} \tag{6}$$

where $\omega = \exp\left[\frac{2\pi i}{Q}\right]$.

The algorithm follows.

1. Given N, choose $Q = 2^q$ such that $N^2 \leq Q \leq 2N^2$ and create q $|0\rangle$ qubits in the first register. Then apply the Hadamard operator H to each qubit. This creates the state

$$\frac{1}{\sqrt{Q}} \left[|0\rangle + |1\rangle + |2\rangle + \cdots + |2^q - 1\rangle\right] \tag{7}$$

where say for $q = 3$, $|0\rangle$ is $|000\rangle$, $|1\rangle$ is $|001\rangle$, $|2\rangle$ is $|010\rangle$, $|3\rangle$ is $|011\rangle$, $|4\rangle$ is $|100\rangle$, $|5\rangle$ is $|101\rangle$, $|6\rangle$ is $|110\rangle$, and $|7\rangle$ is $|111\rangle$.

2. Compute $f(k) = a^k \bmod N$ where the first register is $|k\rangle$ and put the result in the second register. For $N = 15$ and $a = 7$, for example, this produces state

$$\frac{1}{\sqrt{Q}} \left[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + \cdots\right] \tag{8}$$

3. Apply the inverse Fourier transform to the first register and measure the first register. This step is most easily accomplished by two measurements and invoking the principle of implicit measurement for the first measurement. Since the second register is hereafter untouched, measuring the first register effectively determines the result for the second register. Based on the state above (for $N = 15$), the result for the second register is either $|1\rangle, |7\rangle, |4\rangle$, or $|13\rangle$. Suppose $|7\rangle$ is the result, then the inverse Fourier transform is applied to the resultant first register

$$\frac{2}{\sqrt{Q}} \left[|1\rangle + |5\rangle + |9\rangle + \cdots\right] \tag{9}$$

For $N = 15, q = 8$, this generates a probability distribution with masses equal to $\frac{1}{4}$ each associated with $|0\rangle, |64\rangle, |128\rangle$, and $|192\rangle$. The second measurement is one of these values.

4. The continued fraction for this realized value divided by 2^q determines the order r. Suppose we draw $|192\rangle$, then the convergent for the continued fraction $\frac{192}{256} = 0 + \frac{1}{1+\frac{1}{3}}$ is $3/4$ and the denominator is the number we're after. Now, we check $a^4 \equiv 1 \bmod N$, if true $r = 4$.[3] If not then try multiples of 4, for instance, $a^8 \equiv 1 \bmod N$.[4] If multiples fail then start over by drawing a new random integer a.

5. Return to step 7 above, calculate $GCD\left(a^{r/2} - 1, N\right)$ and $GCD\left(a^{r/2} + 1, N\right)$ at least one is a factor of N. Task complete.

Suggested:

1. For $N = 15$, $a = 7$, and $Q = 2^8 = 256$, verify the classical factoring algorithm. (Hint: find the period r by brute-force using $f(x) = f(x + r)$ in step 4.)

2. For $N = 15$, $a = 7$, and $Q = 2^8 = 256$, verify the quantum factoring algorithm.

[3] Euler's generalization of Fermat's theorem states $a^{\varphi(N)} \equiv 1 \bmod N$ for a and N relatively prime where $\varphi(N)$ is Euler's phi or totient. $\varphi(15) = 8$ rather than 4 but all multiples of 4 satisfy the congruence with modulus 15. Recall from discussions of public key encryption, if Euler's phi can be discovered then finding the decoder (and breaking the encryption) is straightforward by Euclid's algorithm.

[4] If we draw $|128\rangle$, $N = 15$, and $a = 7$, then the convergent is $1/2$ and $a^2 \equiv 4 \bmod 15$ so we try $r = 4$ which satisfies the period-finding criterion $a^4 \equiv 1 \bmod 15$.