In our example, we write $6 = 2 \cdot 3$ (a power of 2 times an odd number) and compute (in the notation of Section 6.4)

$$\begin{aligned} b_0 &\equiv 11^3 \equiv 8 \pmod{21} \\ b_1 &\equiv 11^6 \equiv 1 \pmod{21} \\ &\gcd(b_0 - 1, 21) = \gcd(7, 21) = 7, \end{aligned}$$

so we obtain $21 = 7 \cdot 3$.

In general, once we have a candidate for r, we check that $a^r \equiv 1 \pmod{n}$. If not, we were unlucky, so we start over with a new a and form a new sequence of quantum states. If $a^r \equiv 1 \pmod{n}$, then we use the exponent factorization method from Section 6.4. If this fails to factor n, start over with a new a. It is very likely that, in a few attempts, a factorization of n will be found.

Continued Fractions

Finally, we show how to find the fraction j/r using the method of continued fractions. We know that $r \le \phi(n) < n$, so we are trying to approximate a number (such as $427/512$) by a rational number j/r with $r < n$.

First, consider the problem of finding a rational number with small denominator close to a real number x. For example, suppose we want to approximate π. Of course, we could use $314/100 = 157/50$, but we can be more accurate and use a smaller denominator by using $22/7$. So a larger denominator does not guarantee a better approximation.

A general procedure for approximating a real number x is the following. Let $[x]$ denote the greatest integer less than or equal to x. Let $a_0 = [x]$ and $x_0 = x$. Then define

$$x_{i+1} = \frac{1}{x_i - a_i}, \qquad a_{i+1} = [x_{i+1}].$$

For example, here's how to proceed for π. We have $[\pi] = 3$. Then $x_1 = 1/(\pi - 3) \approx 7.06251$ and $a_1 = [x_1] = 7$. Next $x_2 = 1/(x_1 - a_1) \approx 15.9966$, and $a_2 = 15$. Continuing, we have $x_3 = 1/(x_2 - a_2) \approx 1.00342$, $a_3 = 1$, and $x_4 = 1/(x_3 - a_3) \approx 292.6$, so $a_4 = 292$. This yields the expansion

$$\pi = 3 + \cfrac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \cdots}}}}.$$

If we stop after a few levels of this continued fraction, we obtain the approximations

$$3, \quad 3 + \frac{1}{7} = \frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}, \quad \cdots.$$

The last approximation is very accurate:

$$\pi = 3.14159265\ldots, \text{ and } \qquad 355/113 = 3.14159292\ldots.$$

This procedure can be carried out for any real number x and produces a sequence of rational numbers $r_1/s_1, r_2/s_2, \ldots$. Each rational number r_k/s_k gives a better approximation to x than any of the preceding rational numbers r_j/s_j with $1 \leq j < k$. It can be shown that if $|x-(r/s)| < 1/2s^2$ for integers r, s, then $r/s = r_i/s_i$ for some i. For example, $|\pi - 22/7| \approx .001 < 1/98$ and $22/7 = r_2/s_2$.

Now let's apply the procedure to 427/512. We have

$$\frac{427}{512} = 0 + \frac{1}{1+\frac{1}{5+\frac{1}{4+\frac{1}{2}}}}.$$

This yields the numbers

$$0, \quad 1, \quad \frac{5}{6}, \quad \frac{211}{253}, \quad \frac{427}{512}.$$

Since we know the period is less than $n = 21$, the best guess is the last denominator less than n, namely $r = 6$.

In general, we compute the continued fraction expansion of $c/2^m$, where c is the result of the measurement. Then we compute the approximations, as before. The last denominator less than n is the candidate for r.

Final Words

The capabilities of quantum computers and quantum algorithms are of significant importance to economic and government institutions. Many secrets are protected by cryptographic protocols. Quantum cryptography's potential for breaking these secrets as well as its potential for protecting future secrets has caused this new research field to grow rapidly over the past few years.

Although the first full-scale quantum computer is probably many years off, and there are still many who are skeptical of its possibility, quantum cryptography has already succeeded in transmitting secure messages over a distance of greater than 24 km, and quantum computers have been built that can handle a (very) small number of qubits. Quantum computation and cryptography have already changed the manner in which computer scientists and engineers perceive the capabilities and limits of the computer. Quantum computing has rapidly become a popular interdisciplinary research area, and promises to offer many exciting new results in the future.