Solution set 7: Shor's factoring algorithm

1) "Classical" factoring via period finding.

- For $a = 13$, we have

$$\begin{aligned} 13^0 \text{mod} 15 &= 1 \text{mod} 15 = 1 \\ 13^1 \text{mod} 15 &= 13 \text{mod} 15 = 13 \\ 13^2 \text{mod} 15 &= 169 \text{mod} 15 = 4 \\ 13^3 \text{mod} 15 &= 2197 \text{mod} 15 = 7 \end{aligned}$$

  or, more easily: $13^3 \text{mod} 15 = ((13^2 \text{mod} 15) \times 13) \text{mod} 15 = 4 \times 13 \text{mod} 15 = 52 \text{mod} 15 = 7$.

$$\begin{aligned} 13^4 \text{mod} 15 &= 7 \times 13 \text{mod} 15 = 91 \text{mod} 15 = 1 \\ 13^5 \text{mod} 15 &= 1 \times 13 \text{mod} 15 = 13 \text{mod} 15 = 13 \\ &\cdots \end{aligned}$$

  The consecutive outputs of $13^x \text{mod} 15$ are thus $1, 13, 4, 7, 1, 13, 4, 7, \ldots$, so the period of $13^x \text{mod} 15$ is $r = 4$.

- We compute $\gcd(13^{4/2}+1, 15) = \gcd(170, 15) = 5$ and $\gcd(13^{4/2}-1, 15) = \gcd(168, 15) = 3$. Those are indeed the prime factors of fifteen.

As a second example, for $a = 11$, modular exponentiation gives $1, 11, 1, 11, \ldots$ so now the period is $r = 2$. And indeed, $\gcd(11^{2/2} + 1, 15) = \gcd(12, 15) = 3$ and $\gcd(11^{2/2} - 1, 15) = \gcd(10, 15) = 5$.

2) Quantum factoring of 15

- Initialization $\mapsto |0\rangle|0\rangle$
- Hadamard $\mapsto (|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)|0\rangle$
- Controlled modular exponentiation
  $\mapsto |0\rangle|1\rangle + |1\rangle|13\rangle + |2\rangle|4\rangle + |3\rangle|7\rangle + |4\rangle|1\rangle + |5\rangle|13\rangle + |6\rangle|4\rangle + |7\rangle|7\rangle$
- Rewrite $\mapsto (|0\rangle + |4\rangle)|1\rangle + (|1\rangle + |5\rangle)|13\rangle + (|2\rangle + |6\rangle)|4\rangle + (|3\rangle + |7\rangle)|7\rangle$
  The period in the amplitudes of the first register is $r = 4$, but we could never determine r from measuring the first register, as all eight terms $|0\rangle$ through $|7\rangle$ carry equal weight and we randomly get one of them if we measure. Measurement of the first register returns one of the possible outcomes of $13^x \text{mod} 15$, for some random value of x. This isn't useful either — we might as well classically evaluate $13^x \text{mod} 15$ for some random x.

- Quantum Fourier Transform
  $\mapsto (|0\rangle + |2\rangle + |4\rangle + |6\rangle)|1\rangle + (|0\rangle - i|2\rangle - |4\rangle + i|6\rangle)|13\rangle +$
  $(|0\rangle - |2\rangle + |4\rangle - |6\rangle)|4\rangle + (|0\rangle + i|2\rangle - |4\rangle - i|6\rangle)|7\rangle$
- Measurement of the first register gives $0, 2, 4$ or 6. From the way the algorithm is constructed, these are integer multiples of the period, inverted with respect to the register size of three qubits, i.e. an integer times $2^3/r$. It is possible to extract r from the measurement outcome (you may have to repeat the algorithm a few times), but the first register is a bit small to really appreciate how this works.

If the first register had 8 qubits, measurement of the final state would give $0, 64, 128$ or 192 (the integer multiples of $2^8/r = 64$. Now it's possible to find r, for instance via the continued fractions algorithm, which gives

$$\begin{aligned} 64/256 = 1/4 &\mapsto r = 4(\text{correct}) \\ 128/256 = 1/2 &\mapsto r = 2(\text{mistake}) \\ 192/256 = 3/4 &\mapsto r = 4(\text{correct}) \end{aligned}$$

Alternative, one can repeat the measurement a few times, and take the greatest common denominator between the measurement outcomes, which gives 64. We know this number is the inverted period, $2^8/r$, so we deduce that $r = 4$. From $r = 4$, we proceed as under 1).