**Shor’s Algorithm**

Shor’s algorithm is one of the key algorithms discovered for quantum computing. It allows us to factor integers in a much more efficient manner compared to classical techniques. Prime factorisation can be used to crack cryptographic keys, and with a much more efficient factorisation technique being known we may need to reassess our current cryptographic means.

The ‘quantum part’ of the algorithm finds the period of a function and we can use this period to our advantage when factoring a number.

**Properties:**

Postconditions

* Checks that the c\_amod15 function generates a circuit that contains CSwap, CCX, and CX gates
* Checks that the c\_amod15 function throws an exception if a non-coprime integer is entered
* Checks that the qft\_dagger function generates a circuit that contains H, Swap, and Cphase gates
* Checks that qpe\_amod15 function returns a phase between 0 and 1
* Checks that qpe\_amod15 function throws an exception if a non-coprime integer is entered
* Checks that find\_factor function returns an array containing 3 or 5 (or both) upon entering a coprime integer
* Checks that find\_factor function throws an exception upon entering a non-coprime integer

Metamorphic properties

* Checks that a longer circuit is generated if we use a larger power to generate the modular exponentiation circuit
* Checks that an equal length circuit is generated if we use a, equal power to generate the modular exponentiation circuit
* Checks that a longer circuit is generated if we use a larger power to generate the qft dagger circuit
* Checks that an equal length circuit is generated if we use a, equal power to generate the qft dagger circuit