In a conventional computer, information is represented by quantities that obey the laws of classical physics, such as the voltage levels in a logic circuit. But as the size of microelectronics shrinks, quantum physics becomes increasingly important.

In the early 1980s, this observation led Paul Benioff and later Richard Feynman to consider how to compute with information represented by quantum mechanical quantities. For example, an atomic electron has certain quantum states of motion with energies that are discrete or quantized. An electron could be used to represent a binary 0 when it is in one of these states and to represent a binary 1 when it is in a second state. The representation of a single bit of information by such a two-state quantum system has come to be known as a qubit. (Other examples of qubits include the two distinct polarizations of a photon and the orientation of the intrinsic angular momentum or spin of an atomic nucleus, which can be parallel or antiparallel to an applied magnetic field.)

With two or more qubits, we can consider quantum logical “gate” operations in which the state of one qubit changes in a way that is contingent upon the state of another. These gate operations are the building blocks of a quantum computer. However, because of the quantum mechanical superposition principle, qubits are not restricted to the binary 0 or 1 values only. This would let a quantum computer perform much more general quantum gate operations than ordinary computers can using conventional Boolean operations.

In 1994, Peter Shor showed that this new freedom would let a quantum computer find the prime factors of composite integers much more efficiently than any conventional computer. Subsequently, Lov Grover showed that a quantum computer could also search an unstructured database more efficiently than any classical computer. Because integer factorization and related problems that are computationally intractable with conventional computers are the basis for the security of modern public key cryptosystems, Shor’s result has turned quantum computation into a very active research field. Likewise, researchers are devoting considerable effort to determining the classes of problems that are amenable to a “quantum speedup.”

In this special issue, we have three articles highlighting the status of these algorithmic investigations. George Cybenko’s article provides an introduction to quantum algorithms, Richard Josza then casts quantum factoring into a bigger class of problems, and Colin Williams surveys the status of quantum search algorithms.