

The Four Postulates (for a single quantum bit)

1. The state of a quantum bit (a qbit) is described by a two-element vector with complex components, and may be written as: $\alpha|0\rangle + \beta|1\rangle$.
2. As long as we don't measure a qbit, the evolution of its state (i.e., sending the qbit through a "quantum gate") can be modeled by multiplying the current state by a unitary matrix.
3. The measurement of a qbit is represented using a Hermitian matrix. The result of the measurement is one of the eigenvalues of the matrix, and the resulting state is one of the eigenvectors of the matrix.
4. If a qbit is in the state $\alpha|0\rangle + \beta|1\rangle$, the probability of a measurement resulting in a "0" is $|\alpha|^2$ and the probability of a measurement resulting in a "1" is $|\beta|^2$. If a qbit is in the state $|\psi\rangle$, the probability of a measurement resulting in the state $|\phi\rangle$ is $|\langle\phi|\psi\rangle|^2$.

Right now, these four statements should make absolutely no sense whatsoever. You'll know that you've gotten to "square one" in quantum computing, when you understand all four of them, and can apply them to a simple problem.

As we cover the "required math concepts" you might want to occasionally look at the four postulates, to see if things are beginning to shape up.