### Professor Hector Smith

A quantum computer is a digital computer capable of exploiting quantum coherence among the physical two-state systems that store the binary arithmetic information. To factor an integer is to find its expression as a product of prime numbers. The most impressive, most important, and best-known thing about a quantum computer that it can do is to factor with spectacular efficiency a product of two enormous prime numbers. But what on earth can quantum mechanics have to do with factoring?

This question had bothered me for four years, from the time I heard about the discovery that a quantum computer was spectacularly good at factoring until I finally took the trouble to find out how it was done. The answer—you will be relieved, but if you’re like me, also a little disappointed to learn—is that quantum mechanics has nothing at all directly to do with factoring. But it does have a lot to do with waves. Many important waves are periodic, so it is not very surprising that quantum mechanics might be useful in efficiently revealing features associated with periodicity.

Quantum mechanics is connected to factoring through periodicity. It turns out, for purely arithmetic reasons having nothing to do with quantum mechanics, that if we have an efficient way to find the period of a periodic function, then—as we shall discuss—we can easily factor the product of two enormous prime numbers. A quantum computer provides an extremely efficient way to find periods.

This is of considerable practical importance because the great difficulty in factoring such a product—where the two enormous prime numbers are typically each several hundred digits long—is the basis for the security of the most widely used encryption scheme for protecting private information sent over the internet.

In 1994-1995, Peter Shor discovered that a quantum computer would be superefficient at period finding and thereby poses a potential threat to innumerable secrets, whence the explosion of interest in developing quantum computation. The threat is only potential because no quantum computer capable of anything like serious period finding currently exists.

I suspect the emphasis has been put on factoring rather than period finding because factoring is more famously associated with RSA code breaking, although as it happens, period finding can be used directly to crack the RSA code without any need for a detour into factoring. Factoring is also a mathematical concept more familiar to the general public than period finding.

For instance, the focus on factoring has led to some spectacular misrepresentations of Shor’s algorithm in what Einstein called “the secular press.” For example, the New York Times science writer, George Johnson says in his book on quantum computation, *A Shortcut Through Time*, that when the algorithm has done its job, “the solutions—the factors of the number being analyzed—will all be in superposition.” Elsewhere, he says that a quantum computer can “try out all the possible factors simultaneously in superposition then collapse to reveal the answer.”

Neither of these statements bears the slightest resemblance to what the algorithm actually does.