

# Historical Overview of QM

- Quantum Mechanics is now over 100 years old, and is one of the most successful scientific theories ever created. We believe it to be the underpinning of all physical laws. But at ordinary human scales, its effects are almost totally masked. Only by looking at phenomena at very short length and time scales can we see quantum behavior.
- By the 1890s, *classical physics*—Newtonian mechanics plus Maxwell's electromagnetic theory and Boltzmann's statistical mechanics—seemed capable of explaining virtually all physical phenomena. But a number of seemingly minor puzzles proved to be gaps that would completely overthrow the classical structure of physics.

# Planck's law

- The first of these puzzles was the attempt by Max Planck to derive the proper distribution of thermal energy for an electromagnetic (EM) field. The model he used was a closed box at temperature  $T$ , empty except for whatever electromagnetic radiation it contained.
- A well-known result from thermodynamics is the *equipartition theorem*: if a system is in thermal equilibrium at temperature  $T$ , every independent degree of freedom contains an average energy of  $k_B T/2$ . For EM radiation in a box of size  $L$ , the degrees of freedom are the *normal modes*, with wavelengths  $\lambda = 2L/n$  for all values of  $n = 1, 2, \dots$  and frequencies  $f = cn/2L$ . Since there are infinitely many normal modes, equipartition implies that the EM radiation in the box has *infinite* energy.

Needless to say, this is not what is observed.

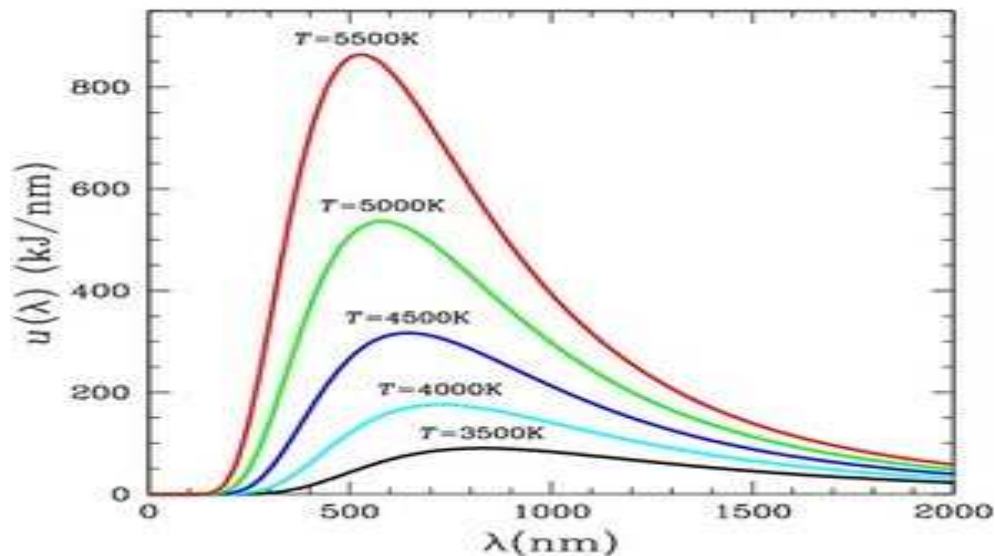
In 1900, Planck came up with a derivation for a finite result. He assumed that the energy in each normal mode came in discrete chunks, proportional to the frequency  $E = hf$ , with a constant of proportionality  $h$ . Instead of each mode containing energy  $k_B T/2$ , it contained  $m$  chunks with a probability proportional to  $\exp(-mhf/k_B T)$ . By choosing the proportionality constant  $h$  appropriately, he derived a distribution law which closely matched experiment. This law is Planck's Law for black-body radiation:

$$E(f) = \frac{8\pi}{c^3} \frac{hf^3}{e^{hf/k_B T} - 1}.$$

The constant of proportionality  $h$  is the incredibly tiny

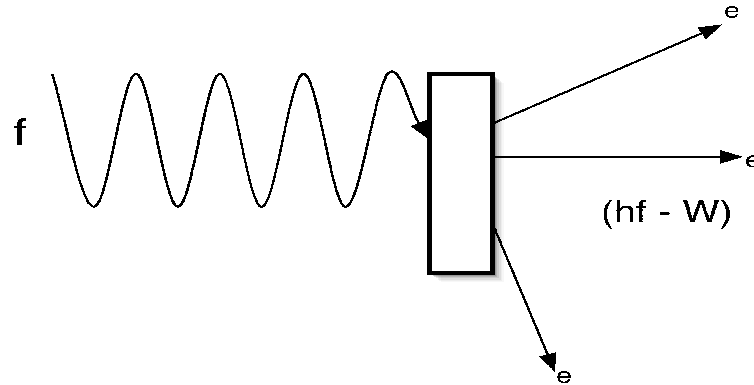
$$h = 6.6261 \times 10^{-34} \text{ kg m}^2/\text{s},$$

which has units of action. It is now known as *Planck's constant*. Planck called the discrete chunks of energy *quanta*, and they gave the name to *quantum mechanics*.



# The Photoelectric Effect

- Confirmation of the discrete nature of light came in 1905, when Albert Einstein solved another puzzle: the photoelectric effect.
- When light shines on a metal, electrons can be emitted. This is how photovoltaic cells work. The energy of the emitted electrons (the voltage produced) is proportional to the *frequency* of the light, but not to the *intensity*. Below a certain frequency (known as the *work function*  $W$ ), no electrons are emitted at all. Above it, they are. The number of electrons emitted (the current) is proportional to the intensity of the light, but not the frequency.
- Einstein's solution to this puzzle was to take Planck's quanta seriously.

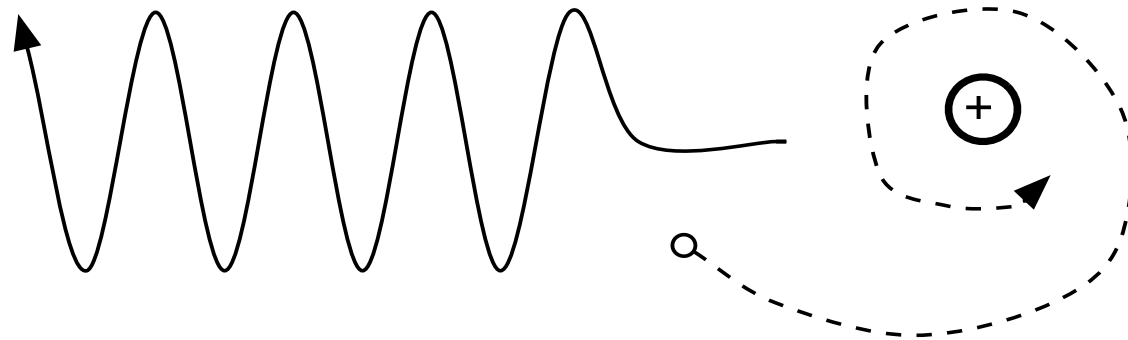


If light does come in discrete chunks with energy  $hf$ , then the photoelectric effect makes sense. Each electron is emitted by being “struck” by a single quantum. The work function  $W$  gives the minimum energy needed to pull an electron free from the metal. The energy  $(hf - W)$  of the emitted electron is the excess over this minimum, and is hence proportional to the frequency. The intensity of the light gives the total *number* of quanta, and hence the number of electrons emitted.

Einstein won the Nobel Prize for his explanation of the photoelectric effect, not for Special or General Relativity or any of his other work. Ironically, in later years he never accepted quantum mechanics, which he had had such an important role in founding.

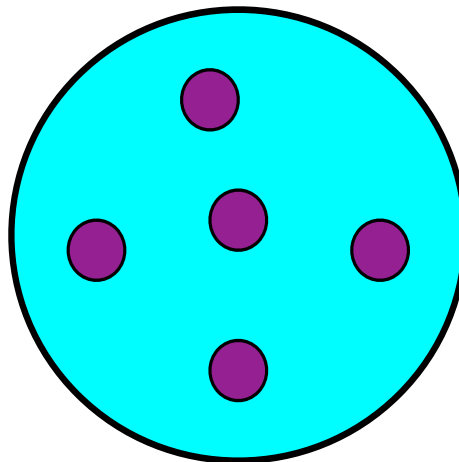
# The Stability of Atoms

- Another puzzle for classical physics was the stability of atoms. If atoms consisted of electrons which orbited a nucleus (the *Solar System Model*), then why are they stable?



- As the electrons whirl around, they should emit electromagnetic radiation and lose energy, causing them to spiral in towards the nucleus.

- One attempt to get around this problem is the *Plum Pudding Model*, in which negatively-charged electrons nestle inside a spongy, positively charged nucleus like plums in a pudding.
- Unfortunately, this model could not explain the scattering experiments of Ernest Rutherford; and scientists outside of Britain found it hard to believe nature was built out of plum pudding.



If electrons can orbit the nucleus at any distance, they should absorb and emit radiation at any frequency. However, this is not the case. Atoms absorb and emit EM radiation at only a discrete set of frequencies. For Hydrogen, the simplest atom, these frequencies obey an exact mathematical law:

$$f = cR_H \left( \frac{1}{n^2} - \frac{1}{m^2} \right),$$

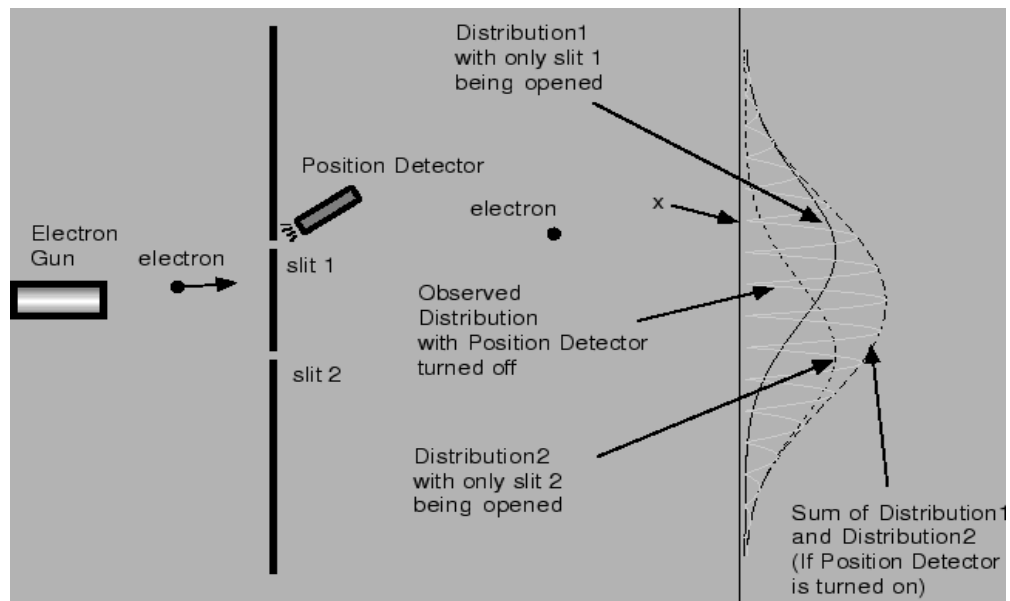
where  $n = 1, 2, \dots$  and  $m = n + 1, n + 2, \dots$

- Niels Bohr suggested that this could be explained if only certain discrete orbits were allowed: orbits whose actions are an exact multiple of Planck's constant of action (plus, for technical reasons,  $1/2$ ). The frequencies corresponding to these orbits turned out to exactly match the above law; and moreover, they explained why atoms were stable, since every atom has a definite lowest possible orbit, the *ground state*.
- The frequencies emitted correspond to energy *differences* between the allowed orbits—each orbit is labeled by an integer  $m$  (or  $n$ ), called a *quantum number*.

# Matter waves and interference

- Another piece of the puzzle was provided by Louis de Broglie in his Ph.D. thesis. Since light, which usually manifests itself as waves, had been shown to sometimes behave like particles, De Broglie speculated that particles might sometimes behave like waves. In particular, he proposed that every particle had an associated wavelength  $\lambda = h/p$  proportional to Planck's constant and inversely proportional to the momentum  $p$ .
- This guess was based on a well known analogy between the paths of particles in a potential and rays in a refracting medium. De Broglie's proposed theory was called *wave mechanics*.

The hypothesis was verified by firing beams of electrons at pairs of slits in a screen. The beam produced an interference pattern on the other side, characteristic behavior for waves. Even more peculiar, the pattern persisted even if the beam intensity was so low that the electrons arrived one at a time. It seemed that electrons could interfere with themselves.



# New Quantum Theory for Old

- The solutions to all of these problems—black body radiation, photoelectricity, the Lyman alpha spectrum and two-slit experiment—were found in an ad hoc way, making changes to classical mechanics one at a time.
- These changes, however, did not provide a complete theory to replace classical physics. That waited for the work of Schrödinger, Heisenberg, Dirac, von Neumann, Pauli, and others in the 1920s and 30s. The early days are now called *the old quantum theory*, and the revolution they led to is known as *quantum mechanics*.

# Properties of Quantum Mechanics

- What are the revolutionary properties of quantum mechanics? Any quantum theorist can make his or her own list of quantum peculiarities. Here is mine:  
*indeterminism, interference, uncertainty and complementarity, discrete spectra for bound systems, superposition (linearity), and entanglement.*
- We will use many of these properties in this course, and come to understand them in a technical sense. But let us first get a qualitative picture of what they mean.

# Indeterminism

- The most fundamental distinction between classical and quantum mechanics is that classical mechanics is a *deterministic* theory: given perfect knowledge of the current state of a system, its state at all past and future times is, in principle, calculable. In classical mechanics, probabilities are used only to describe situations where one's knowledge is incomplete.
- By contrast, quantum mechanics makes statements only about *probabilities*. If the same measurement is performed on several identically prepared systems, one cannot in general expect the same outcome. This is not because we lack information about the systems described; rather, it is because the outcome of the measurement is inherently unpredictable.

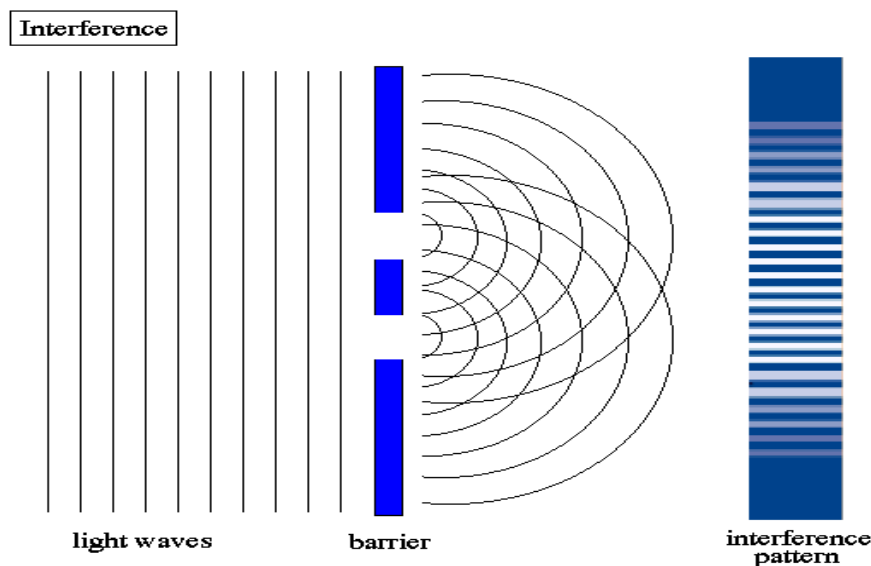
# Interference

- Probabilities in quantum mechanics are not calculated directly, but from *probability amplitudes*<sup>\*</sup>, which are *complex numbers*. The probability is the *square* of the probability amplitude. Their relationship is similar to that between the amplitude of a wave and its intensity.
- For example, in the two-slit experiment, the amplitude for a particle to hit a particular point on the screen is the sum of the amplitude to go through slit A and hit the point, and the amplitude to go through slit B and hit the point. The probability to hit the point is then

$$p = |\alpha_A + \alpha_B|^2.$$

- Because the amplitudes can either add or cancel each other out, this system exhibits *interference fringes*.

Some parts of the screen will not be hit by particles, even though there is a nonzero amplitude to reach that part of the screen from each slit. Other parts will be hit at a higher rate.



\*The probability interpretation of QM was presented first by Max Born. It was in a footnote to this pioneering paper, added in proof, that he realized that probabilities were not equal to the amplitudes but to their squares.

# Uncertainty

For a classical particle, complete information is given by the position of the particle and its velocity (or momentum). For a quantum particle, this is not the case. As famously realized by Heisenberg, a measurement of a particle's position disturbs its momentum, with the size of the disturbance related to the precision of the measurement. Similarly, a measurement of the momentum disturbs the particle's position. This constraint on the precision with which position and momentum can be measured is quantified by the inequality

$$(\Delta x)^2(\Delta p)^2 \geq \frac{\hbar^2}{4}, \quad \hbar = h/2\pi.$$

- This constraint *could* be seen as just a practical limitation on the precision of measurements; we might imagine that particles really do have precise positions and momenta, which we are unable to exactly determine.
- However, in quantum mechanics an even more radical explanation holds: in fact, the two quantities *are not even simultaneously well-defined*. As we will see, quantum states that give both a precise position and momentum (or any other pair of incompatible quantities) do not exist.

# Complementarity

This idea—that different ways of describing a system may be mutually exclusive—is called *complementarity*. For position and momentum, this means that we can write down amplitudes for every possible position of a particle, OR for every possible momentum, but not both, because those quantities cannot be simultaneously measured. If  $\psi(x)$  is the *wavefunction* giving the amplitude to be at every point  $x$ , we can also write down  $\tilde{\psi}(p)$  (the Fourier transform) which gives the amplitude for every point  $p$ . But there is no similar function  $\psi(x, p)$ . For variables other than position and momentum, similar restrictions hold. In particular, for the kind of *discrete* variables used in quantum information theory, uncertainty and complementarity still apply (though they take a somewhat different form).

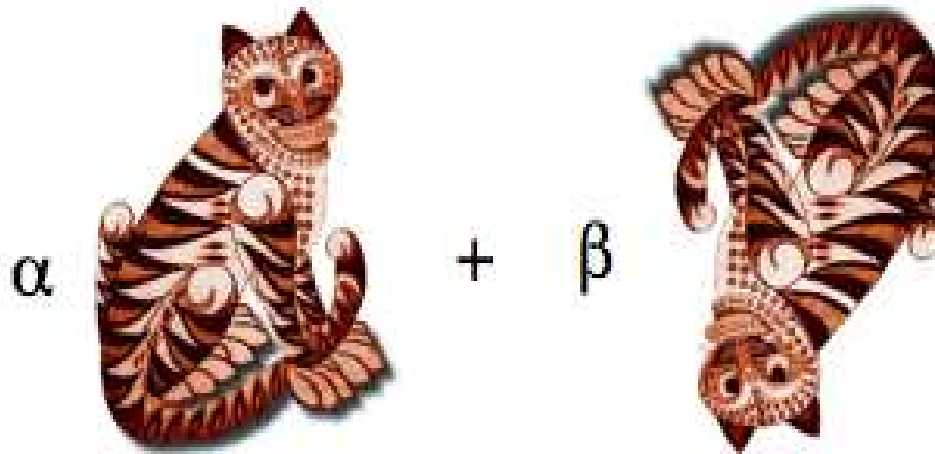
# Discrete spectrum

- For the Bohr atom, only certain discrete orbits were allowed, with discrete values of the energy. These values are called *energy levels*. Discrete spectra are common for bound systems in quantum mechanics.
- This discreteness is useful in quantum information theory, because it matches the discreteness assumed in quantifying classical information. For instance, the simplest quantum system would be one with only two distinct levels. This is analogous to a classical bit, which can take one of two possible values. In quantum information theory, most of the systems we will deal with have only a finite number of discrete levels.
- However, while the number of energy levels may be finite, the possible states are *continuous*. This is because of another property of quantum mechanics: *linearity*.

# Superposition

- Suppose that  $\psi$  and  $\phi$  are two valid states of a quantum system. (That is, two possible *wavefunctions*.) Then  $a\psi + b\phi$ , where  $a$  and  $b$  are complex numbers, is *also* a valid state of the system. This is an example of a superposition.
- The reason such superpositions are possible is because quantum mechanics is a *linear* theory. The set of all states forms a complex vector space (or Hilbert space). The evolution equation for states, the *Schrödinger equation*, is a linear differential equation. The various physical quantities in the theory are represented by linear operators (matrices) on the Hilbert space.

- It is linearity which makes possible the famous Schrödinger's Cat paradox, in which a cat is simultaneously alive and dead.
- (More strictly speaking, it is in a superposition of being alive and dead.)



# Entanglement

This last property of quantum mechanics is one of the most difficult to explain; but it plays a crucial role in quantum computation and quantum information. If a quantum system consists of multiple subsystems—for instance, of several distinct particles—it is possible for the *joint* system to have a definite state  $\psi$ , while none of the subsystems has a well-defined state. In this situation, the subsystems are said to be *entangled*.

$$\psi(x, y) \neq \psi(x)\psi(y).$$

While this may sound like a strange and exotic situation, in fact it is not. Almost all states of multiple subsystems are entangled. But the effects of entanglement are masked at larger scales.

- At the quantum level, entanglement behaves very much like classical correlation: measurement outcomes on different subsystems are correlated. But these correlations can be stronger than any possible classical correlation. This result was proven theoretically by John Bell in the 1960s, and experimentally demonstrated by both Clauser and Aspect in the 1970s and 1980s.
- Much has been made of entanglement, including various wild assertions that quantum mechanics is *nonlocal*: that once in contact, quantum systems continue to influence each other even when far apart. These assertions are very overstated. But it is true that entanglement is rather different from any phenomenon which occurs in classical physics.

# QIP: A Prehistory

- As microelectronic components get smaller and smaller, computer chips are steadily approaching the point where quantum effects must be taken into account. However, by the 1980s, some people were already starting to ask if quantum mechanics could actually be exploited to make new information processing techniques possible.
- The first to propose an intrinsically quantum mechanical computer was P. Benioff in 1980. Y. Manin and R. Feynman both proposed that a quantum computer might be able to efficiently simulate quantum systems—something that ordinary classical computers find very difficult. (This idea of quantum simulation remains one of the most important potential applications of a quantum computer.)

# Reversible Computation

- But is a quantum computer even possible? As we will see, such a computer must operate *reversibly*; that is, it cannot dissipate energy. Ordinary computers are highly dissipative, as anyone who has ever felt the heat they give off has noticed.
- In the 1970s, Charles Bennett of IBM showed that any computation can, in principle, be done reversibly, based on work from the 60s by Rolf Landauer. That is, in principle, there is no requirement that a computer consume power to operate (though it may take energy to start a computation). This paved the way for the possibility of reversible quantum computers.

# Deutsch's Algorithm

- In 1985, David Deutsch presented a new idea. Because of linearity, a quantum computer can be in a superposition of *different computations*. For instance, a computer could simultaneously calculate the value of a function  $f(x)$  for every possible input  $x$  in a single run. Deutsch called this possibility *quantum parallelism*, and speculated that, just like ordinary parallelism, it would increase computing power.
- Naive applications of quantum parallelism add nothing to the power of the computer. But in 1988, Deutsch found a clever algorithm that exploited quantum parallelism indirectly to solve a problem more efficiently than any possible classical computer. The problem was artificial, but it was the first example where a quantum computer could be shown to be more powerful.

# Quantum Cryptography

- Meanwhile, in 1984, Charles Bennett and Gilles Brassard found another way in which quantum properties could be exploited for information processing. They exploited the uncertainty principle as a way to distribute a cryptographic key with perfect security. Single quanta are used to send the bits of the key, in one of two possible complementary variables. If an eavesdropper tries to intercept the bits and measure them, this automatically disturbs them in such a way that it can always be detected.
- This and similar schemes are called *quantum cryptography* or *quantum key distribution* (QKD). This is the quantum information protocol which is closest to being real technology.

# Further Progress

- Artur Ekert, in 1991, proposed another scheme for quantum cryptography, this one based on entanglement rather than uncertainty.
- Bennett and collaborators found yet other uses for entanglement: *quantum teleportation*, in which separated experimenters, sharing two halves of an entangled system, can make use of the entanglement to transfer a quantum state from one to another using only classical communication; and *superdense coding*, in which sending a single *quantum* bit allows the transmission of two bits of *classical* information.

- Richard Josza and David Deutsch extended Deutsch's original algorithm to a more general, but still artificial version of Deutsch's problem.
- D.R. Simon found another problem, albeit still rather specialized, in which quantum computers outperformed classical computers. The stage was being set for the real breakthrough.
- A mathematician named Peter Shor at AT&T Research Labs became interested in the potential of algorithms on quantum computers to solve computationally difficult problems.

# Shor's Factoring Algorithm

- In 1994, Peter Shor published a paper showing that a quantum computer could decompose a large number into its prime factors in a time of polynomial order in the length of the number.
- The difficulty of factoring is the basis for the RSA public-key encryption algorithms, which is the basis for secure transactions on the world wide web.
- Suddenly, it was known that quantum computers could in principle solve a problem of importance in the real world.

# From Prehistory to Today

- Rather than being an obscure interest for a handful of physicists and computer scientists, quantum information processing was suddenly of interest to researchers in many fields.
- In the almost 15 years since the factoring algorithm was discovered, the fields of quantum information and quantum computation have exploded.
- In this course, we'll see why.

*Next time: the simplest quantum system.*