QI Lecture 15

The Shor Algorithm

This lecture will make heavy use of number theory and some new notation and ideas:

"$gcd(a, b)$" is the greatest common divisor of a and b. When a and b are coprime, $gcd(a, b) = 1$.

"$x \, mod \, M$" means is the remainder of x divided by M. For example, $13 \, mod \, 8 = 5$. Because it saves room and is easier to read, we'll use "box and subscript"[1] notation for the mod, $[13]_8 = 5$.

"$\phi(M)$", the "Euler phi of M",[2] is the number of positive integers less than M that are coprime to M (share no factors in common). For example, checking off all of the numbers less than ten with factors in common with ten (2 and 5) we get $1, \not{2}, 3, \not{4}, \not{5}, \not{6}, 7, \not{8}, 9, \not{10}$ and therefore $\phi(10) = 4$. For primes, $\phi(P) = P - 1$ and for products of primes $\phi(PQ) = (P - 1)(Q - 1)$.

The Motivation: RSA Encryption

RSA is an example of "trapdoor encryption"; encryption whose security is based on a mathematical operation that's easy to do if you know a secret and effectively impossible if you don't. In this case,

1) Generate very large primes P and Q.
2) Create $M = PQ$.
3) Now randomly generate k, such that $gcd(k, \phi(M)) = 1$.
4) Find k^{-1} such that $kk^{-1} = j\phi(M) + 1$.
5) Make k and M public and keep everything else private.

To turn a message T, where $T < M$, into cyphertext C:

$$C = \left[T^k\right]_M$$

[1] This is non-standard notation, so don't use it in anything you expect other people to understand.
[2] Same Euler as always.

To decrypt:

$$\left[C^{k^{-1}}\right]_M = \left[T^{kk^{-1}}\right]_M = \left[T^{j\phi(M)+1}\right]_M = \left[T^{j\phi(M)}T\right]_M = T$$

This works because $\left[a^{\phi(M)}\right]_M = 1$.[3] For example, $\left[3^{\phi(10)}\right]_{10} = \left[3^4\right]_{10} = [81]_{10} = 1$.

Example If $M = 15$, then $\phi(15) = (5-1)(3-1) = 10$. If the public key is $k = 3$, then solving $3k^{-1} = 10j + 1$ we find that $k^{-1} = 7$.

Given these keys, encrypt and decrypt the message $T = 7$.

$$C = \left[T^k\right]_{15} = \left[7^3\right]_{15} = [343]_{15} = 13$$

$$T = \left[C^{k^{-1}}\right]_{15} = \left[13^7\right]_{15} = [62748517]_{15} = 7$$

■

"Breaking the key" means finding the private key, k^{-1}, given the public key, k and M. Finding k^{-1} amounts to solving for x in $xk + y\phi(M) = 1$, which can be done in logarithmic time.[4] $\phi(M) = (P-1)(Q-1)$ where $M = PQ$, so without P and Q we can't find k^{-1}. But finding P and Q is difficult.

For example, $M = 65639551091939800586975299246999409966764914132193557 71$. What are P and Q?[5]

Shor's algorithm breaks encryption keys by finding the factors of M.

The Trick

Define

$$f(x) = [a^x]_M$$

In a modulus, exponential functions generate infinitely repeating patterns.

[3] This isn't *quite* true when $gcd(a, b) \neq 1$, but it may as well be. We only need $\left[a^{j\phi(M)+1}\right]_M = a$ which *is* always true. For example, $\left[2^4\right]_{10} = 6 \neq 1$ but $\left[2^5\right]_{10} = 2$.

[4] This amounts to doing Euclid's algorithm for finding the gcd.

[5] Obviously, $P = 876432598540936751319034 3$ and $Q = 7489400919273757839048102475 97$.

Example For $M = 15$ and $a = 2$:

$$
\begin{aligned}
[2^0]_{15} &= 1 \\
[2^1]_{15} &= 2 \\
[2^2]_{15} &= 4 \\
[2^3]_{15} &= 8 \\
[2^4]_{15} &= [16]_{15} = 1 \\
[2^5]_{15} &= [32]_{15} = 2 \\
[2^6]_{15} &= [64]_{15} = 4 \\
[2^7]_{15} &= [128]_{15} = 8 \\
[2^8]_{15} &= [256]_{15} = 1 \\
&\ldots
\end{aligned}
$$

This pattern, $1, 2, 4, 8, 1, 2, 4, 8, \ldots$, repeats forever.

■

The "**order of** $[a]_M$" is the smallest number r such that $[a^r]_M = 1$ and for the purposes of these notes this is written "$o([a]_M) = r$". If r is even,

$$
\begin{aligned}
[a^r]_M &= 1 \\
[a^r - 1]_M &= 0 \\
\left[(a^{\frac{r}{2}})^2 - 1\right]_M &= 0 \\
\left[(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)\right]_M &= 0
\end{aligned}
$$

So $(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$ is equal to some multiple of M, and when neither factor alone is a multiple of M, then one must be a multiple of P and the other must be a multiple of Q. Therefore the gcd of either factor with M will yield one of M's two prime factors.

The Shor algorithm factors M by finding r.

Example Since we already know from the last example that $o([2]_{15}) = 4$ and 4 happens to be an even number,

$$
\begin{aligned}
1 &= [2^4]_{15} \\
0 &= [2^4 - 1]_{15} \\
0 &= [(2^2 - 1)(2^2 + 1)]_{15} \\
0 &= [(3)(5)]_{15}
\end{aligned}
$$

Although we (clearly) don't need it, we can find the factors that each of these terms have in common with 15 using the gcd.

$$gcd(15, 3) = 3 \qquad\qquad gcd(15, 5) = 5$$

Evidently, the prime factors of 15 are 3 and 5. Tell your friends.

■

What You Need a Quantum Computer For

Typically, $r = O(M)$ (it's smaller, but on the order of M), so it's very big for a reasonable encryption key. For the same M from earlier,

$$M = 6563955109193980058697529924699940996676491413219355771$$

to find the order of 2 classically, you'd need to raise it to every power until

$$\left[2^{6563955109193980058697529175751084743315298140895917832}\right]_M = 1$$

Unfortunately, there isn't enough time before the heat death to raise 2 to every power up to r. A quantum computer raises a to a superposition of every power up to N and then uses the QFT to find the period, r, of the repeating patterns that are created.

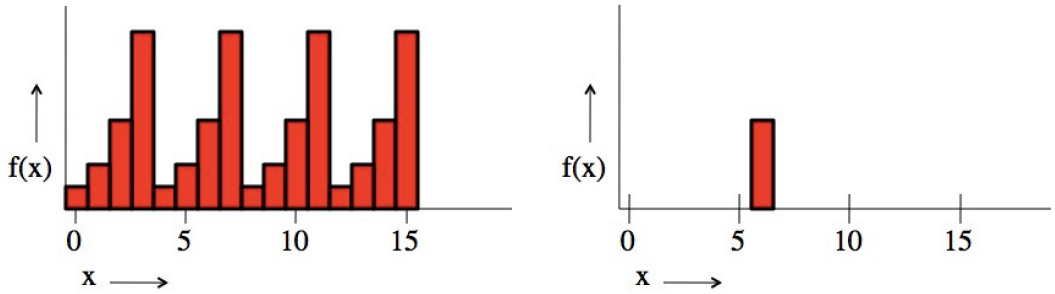

Figure 1: Left: Shor's algorithm uses a QFT to find the period, r, of repeating patterns in $f(x) = [a^x]_M$. Right: In a classical computer we don't have superpositions, so the QFT doesn't make sense. Even worse, Earth isn't large enough to store all of the values of $f(x)$ needed to perform a classical DFT.

We begin with two registers of n qubits each, where $N = 2^n > M^2$ (for reasons that will become clear later).

$$|0\rangle^{\otimes n}|0\rangle^{\otimes n}$$

To save room on notation, we'll stop writing "$\otimes n$" and just keep in mind that both of these registers have n qubits. The first register is then run through a bank of Hadamard operators, $H^{\otimes n}$, to produce an even superposition over all input states.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle$$

We then apply a unitary function, $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ where $\oplus$ is addition mod N, to put $f(x) = [a^x]_M$ into the second register.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

We immediately measure the second register. The value of $f(x)$ is completely irrelevant; the only thing that's important is that the same value recurs every r. In other words, $f(x_0) = f(x_0 + r) = f(x_0 + 2r) = \ldots$ Therefore, a measurement of the second register resulting in $|f(x_0)\rangle$ leaves the system in the state

$$\sqrt{\frac{r}{N}} \sum_{j=0}^{\frac{N}{r}-1} |x_0 + jr\rangle|f(x_0)\rangle$$

Here "$\frac{N}{r}$" is approximate; in reality this value is either $\left\lfloor \frac{N}{r} \right\rfloor$ or $\left\lfloor \frac{N}{r} \right\rfloor + 1$, but considering that N and r are typically both huge numbers, $\frac{N}{r}$ is good enough. The first register is now in a superposition of states spaced r apart, starting at x_0. Having measured the second register, we no longer need to keep track of it.[6]

$$\sqrt{\frac{r}{N}} \sum_{j=0}^{\frac{N}{r}-1} |x_0 + jr\rangle$$

We now apply the QFT

$$|\Psi\rangle = \frac{\sqrt{r}}{N} \sum_{k=0}^{N-1} \left[\sum_{j=0}^{\frac{N}{r}-1} e^{\frac{2\pi i k}{N}(x_0+jr)} \right] |k\rangle = \frac{\sqrt{r}}{N} \sum_{k=0}^{N-1} e^{\frac{2\pi i k}{N}x_0} \left[\sum_{j=0}^{\frac{N}{r}-1} e^{\frac{2\pi i}{N}jrk} \right] |k\rangle$$

The probability distribution on k will tend to spike strongly where $\frac{kr}{N} \approx \mathbb{Z}$ and $e^{2\pi i j \frac{kr}{N}} \approx 1$. Specifically,

$$\boxed{p\left(-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}\right) \geq \frac{4}{\pi^2} \approx 40.5\%}$$

Remember that $r < M$ and $M^2 < N$, so this is a very narrow window for large values of M.

Finally, the first register is measured. The condition that $-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}$, basically means that $[kr]_N \approx 0$ and therefore $\frac{k}{N} \approx \frac{\ell}{r}$, where ℓ means nothing and r is what we're looking for. We know $N = 2^n$ because we built the machine and know how many qubits

[6] We could wait until the end of the algorithm to measure the second register. The time that a measurement is made makes no difference, so if a state is ready to be measured, it doesn't matter if you wait for a while. We measuring here to make the math easier for ourselves and to really underscore the importance of the repeating pattern by using the simplest possible repeating pattern.

it's using, n, and we got k from measuring the first register. All that's left is to do some math and find r.

Sometimes, for entirely mathematical reasons, the choice of a doesn't produce a useful result and a new a needs to be selected. Selected at random, the probability of picking a useful $a \in [0, N-1]$ is

$$\boxed{p(\textit{good number}) \geq \frac{1}{2}}$$

Here's What You Do With The Results

The condition $-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}$ can be re-written:

$$\begin{array}{rcccl}
-\frac{r}{2} & \leq & [kr]_N & \leq & \frac{r}{2} \\
\ell N - \frac{r}{2} & \leq & kr & \leq & \ell N + \frac{r}{2} \quad (\ell \in \mathbb{Z}) \\
\frac{\ell N}{r} - \frac{1}{2} & \leq & k & \leq & \frac{\ell N}{r} + \frac{1}{2} \\
\frac{\ell}{r} - \frac{1}{2N} & \leq & \frac{k}{N} & \leq & \frac{\ell}{r} + \frac{1}{2N} \\
\frac{\ell}{r} - \frac{1}{2N} & \leq & \frac{k}{N} & \leq & \frac{\ell}{r} + \frac{1}{2N} \\
 & & \left|\frac{k}{N} - \frac{\ell}{r}\right| & \leq & \frac{1}{2N}
\end{array}$$

The statement $\left|\frac{k}{N} - \frac{\ell}{r}\right| \leq \frac{1}{2N}$ is enough to establish uniqueness of ℓ and r given k and N.

For two distinct rational numbers $\frac{a}{b}$ and $\frac{c}{d}$, with $b, d < M$, we have $\left|\frac{a}{b} - \frac{c}{d}\right| = \left|\frac{ad-bc}{bd}\right| \geq \frac{|ad-bc|}{M^2} \geq \frac{1}{M^2}$. Assuming there are two solutions, $\frac{\ell'}{r'}, \frac{\ell}{r}$ we have:

$$\left|\frac{\ell'}{r'} - \frac{\ell}{r}\right| \leq \left|\frac{k}{N} - \frac{\ell}{r}\right| + \left|\frac{k}{N} - \frac{\ell'}{r'}\right| \leq \frac{1}{2N} + \frac{1}{2N} \leq \frac{1}{M^2}$$

Which is impossible for $\frac{\ell'}{r'}, \frac{\ell}{r}$ distinct and $r, r' < M$.

Now, find the continued fraction expansion of $\frac{k}{N}$, and take successfully longer and longer approximations until the last step in which the denominator is less than M. That last continued fraction approximation will be $\frac{\ell}{r}$.

If $(\ell, r) = 1$, then r is found. Otherwise, you've got a reduced fraction, and only a divisor of r has been found. However, for large random values of ℓ and r, $P\left((\ell, r) = 1\right) = \frac{6}{\pi^2} \approx 61\%$. Most of the remaining 39% takes the form of ℓ and r sharing 2, 3, or 5, which is easy to sort out.

A continued fraction takes the form $X = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}}$ and is written $X = [a_0; a_1, a_2, \ldots]$. Truncating a continued fraction yields the best approximation of any number with a denominator less than or equal to the given truncation. a_0 is the integer part of X. $X - a_0 = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}}$ and $\frac{1}{X - a_0} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}$, so a_1 is the integer part of $\frac{1}{X - a_0}$. Repeating this procedure yields the continued fraction.

Example Find the first several continued fraction approximations of π.

$$\lfloor \pi \rfloor = 3 \qquad \pi \approx 3$$

$$\left\lfloor \frac{1}{\pi - 3} \right\rfloor = \lfloor 7.0625133 \rfloor = 7 \qquad \pi \approx [3; 7] = 3 + \frac{1}{7} = \frac{22}{7} \approx 3.1428$$

$$\left\lfloor \frac{1}{7.0625133 - 7} \right\rfloor = \lfloor 15.9965959 \rfloor = 15 \qquad \pi \approx [3; 7, 15] = 3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106} \approx 3.1415094$$

$$\left\lfloor \frac{1}{15.9965959 - 15} \right\rfloor = \lfloor 1.0034157 \rfloor = 1 \qquad \pi \approx [3; 7, 15, 1] = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} = \frac{355}{113} \approx 3.1415929$$

There is no rational approximation to π closer than $\frac{355}{113}$ with a denominator less than or equal to 113.

■

Example Find all of the continued fraction approximations of $X = \frac{10}{47}$.

$$\frac{10}{47} = 0 + \frac{10}{47} \quad \Rightarrow \quad X \approx [0] = 0$$

$$\frac{47}{10} = 4 + \frac{7}{10} \quad \Rightarrow \quad X \approx [0; 4] = 0 + \frac{1}{4} = \frac{1}{4}$$

$$\frac{10}{7} = 1 + \frac{3}{7} \quad \Rightarrow \quad X \approx [0; 4, 1] = 0 + \frac{1}{4 + \frac{1}{1}} = \frac{1}{5}$$

$$\frac{7}{3} = 2 + \frac{1}{3} \quad \Rightarrow \quad X \approx [0; 4, 1, 2] = 0 + \frac{1}{4 + \frac{1}{1 + \frac{1}{2}}} = \frac{3}{14}$$

$$\frac{3}{1} = 3 + 0 \quad \Rightarrow \quad X = [0; 4, 1, 2, 3] = 0 + \frac{1}{4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}}} = \frac{10}{47}$$

■

This is completely irrelevant to the class, but Continued Fractions are, in several significant ways, a better way to represent real numbers than our usual decimal form. They terminate if and only if a number is rational, there is a unique representation for every real number, those that repeat forever are quadratic irrationals[7], $[0;1,2,3,\ldots$ and $[1;2,3,\ldots]$ are reciprocals, and a truncated expansion produces the "best rational approximation" in the sense used by the Shor algorithm.

The worst continued fraction expansion belongs to

$$\varphi = [1;1,1,1,1,1,\ldots] = 1 + \frac{1}{1 + \frac{1}{1+\frac{1}{1+\cdots}}} = 1 + \frac{1}{\varphi}$$

which is the Golden Ratio, $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.6180\ldots$, and the slowest converging CF expansion. Incidentally, the reason that φ can be represented as a quadratic irrational is that it is the solution to the quadratic equation

$$\varphi = 1 + \frac{1}{\varphi} \quad \Rightarrow \quad \varphi^2 - \varphi - 1 = 0$$

[7] solutions to quadratic equations

The Probability The Quantum Part Works

$$-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}$$

is specifically what is meant by "$\frac{kr}{N}$ is close to an integer".

For every $b \in \left[-\frac{r}{2}, \frac{r}{2}\right]$, there is a $k = \left[br^{-1}\right]_N$ such that $[kr]_N = b \in \left[-\frac{r}{2}, \frac{r}{2}\right]$. So, the fact that $-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}$ for r different values of k is trivial in that there are r numbers in the interval from $-\frac{r}{2}$ to $\frac{r}{2}$.

We assume that $-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}$ and therefore, using $b = kr \leq \frac{r}{2}$,

$$\begin{aligned}
p(k) &= |\langle k|\Psi\rangle|^2 \\
&= \frac{r}{N^2}\left|\sum_{s=0}^{N-1} e^{\frac{2\pi i s}{N}x_0}\left[\sum_{j=0}^{\frac{N}{r}-1} e^{\frac{2\pi i}{N}jrs}\right]\langle k|s\rangle\right|^2 \\
&= \frac{r}{N^2}\left|e^{\frac{2\pi i k}{N}x_0}\sum_{j=0}^{\frac{N}{r}-1} e^{\frac{2\pi i}{N}jrk}\right|^2 \\
&= \frac{r}{N^2}\left|\sum_{j=0}^{\frac{N}{r}-1} e^{\frac{2\pi i}{N}jrk}\right|^2 \\
&= \frac{r}{N^2}\left|\sum_{j=0}^{\frac{N}{r}-1} e^{\frac{2\pi i}{N}jb}\right|^2 \\
&= \frac{r}{N^2}\left|\frac{1-e^{\frac{2\pi i}{N}\frac{N}{r}b}}{1-e^{\frac{2\pi i}{N}b}}\right|^2 \\
&= \frac{r}{N^2}\left|\frac{1-e^{2\pi i\frac{b}{r}}}{1-e^{2\pi i\frac{b}{N}}}\right|^2
\end{aligned}$$

When $\theta \in [-\pi, \pi]$, we have that $\frac{2}{\pi}|\theta| \leq \left|1-e^{i\theta}\right| \leq |\theta|$. Notice that since $|b| \leq \frac{r}{2}$, we know that $2\pi\frac{b}{r} \leq \pi$, and because $r < M \leq \sqrt{N}$, we also trivially know that $2\pi\frac{b}{N} << \pi$. Therefore,

$$\begin{aligned}
&\geq \frac{4}{\pi^2}\frac{r}{N^2}\left|\frac{2\pi\frac{b}{r}}{1-e^{2\pi i\frac{b}{N}}}\right|^2 \\
&\geq \frac{4}{\pi^2}\frac{r}{N^2}\left|\frac{2\pi\frac{b}{r}}{2\pi\frac{b}{N}}\right|^2 \\
&= \frac{4}{\pi^2}\frac{r}{N^2}\left|\frac{N}{r}\right|^2 \\
&= \frac{4}{\pi^2}\frac{1}{r}
\end{aligned}$$

So $p(k) \geq \frac{4}{\pi^2 r}$ for each value of k such that $-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}$. There are r different such values of k and therefore

$$\boxed{p\left(-\frac{r}{2} \leq [kr]_N \leq \frac{r}{2}\right) \approx rp(k) \geq \frac{4}{\pi^2} \approx 40.5\%}$$

Some Number Theory

This section is about trying to understand the math and issues a little better, by considering $M = 35 = 5 \cdot 7$.

Notice the use of the direct product in "$\mathbb{Z}_{35} \cong \mathbb{Z}_5 \otimes \mathbb{Z}_5$". In the same way we describe the basis of product spaces, $A \otimes B$, using pairs of states, we can describe $\mathbb{Z}_{35}$ using pairs of numbers, one each in $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

The order, $r = o(a)$, is the smallest number such that $[a^r]_M = 1$. Notice that

$$r | \phi(PQ)$$

or in this case, $r|\phi(35) = (5-1)(7-1) = 24$. This is a result from group theory

Theorem (Lagrange's theorem)**.** *The number of elements in a subgroup always divides the number of elements in the group.*

The group here is the "multiplicative group mod M", $\mathbb{Z}_M^\times$, which is composed of all numbers coprime to M, of which there are $\phi(M)$, and the subgroups are "cyclic subgroups". For example, since $[8^4]_{35} = 1$, the set of powers of 8,

$$S = \left\{8, 8^2, 8^3, 8^4, 8^5, 8^6, \ldots\right\} = \left\{8, 8^2, 8^3, 1, 8, 8^2, \ldots\right\} = \left\{1, 8, 8^2, 8^3\right\} = \{1, 8, 29, 22\}$$

is a multiplicative subgroup. Notice that any pair of numbers multiplied together is just another power of 8, and thus still in the set. And of course, $r = 4|24 = \phi(35)$!

$a \in \mathbb{Z}_5$	$o(a)$
0	1
1	1
2	4
3	4
4	2

$a \in \mathbb{Z}_7$	$o(a)$
0	1
1	1
2	3
3	6
4	3
5	6
6	2

Using the Chinese Remainder Theorem you can look at any number in $\mathbb{Z}_M$ as a pair of numbers in the product space $\mathbb{Z}_M \cong \mathbb{Z}_P \otimes \mathbb{Z}_Q$. To go $\mathbb{Z}_M \to \mathbb{Z}_P \otimes \mathbb{Z}_Q$ take the corresponding mod and to go $\mathbb{Z}_P \otimes \mathbb{Z}_Q \to \mathbb{Z}_M$ use the Chinese Remainder Theorem.[8]

[8] For reasonably finite M, it's easier to just have a list (like the 35 example in this lecture) of corresponding representations, $z \leftrightarrow (x, y)$, rather than to apply the CRT every time you want to go $\mathbb{Z}_P \otimes \mathbb{Z}_Q \longrightarrow \mathbb{Z}_{PQ}$.

Example Arbitrarily choosing two numbers to do with math:

$$[8]_{35} \sim ([3]_5, [1]_7) \qquad [2]_{35} \sim ([2]_5, [2]_7)$$

Because $\mathbb{Z}_{35} \cong \mathbb{Z}_5 \otimes \mathbb{Z}_7$ we can add or multiply these numbers in either space and arrive at the same answer. To go back and forth between $\mathbb{Z}_{35} \leftrightarrow \mathbb{Z}_5 \otimes \mathbb{Z}_7$ it will be easiest to refer to the $\mathbb{Z}_{35}$ table on the following page.

Multiplying in $\mathbb{Z}_{35}$:

$$[8 \times 2]_{35} = [16]_{35} \sim ([1]_5, [2]_7)$$

Multiplying in $\mathbb{Z}_5 \otimes \mathbb{Z}_7$:

$$([3]_5, [1]_7) \times ([2]_5, [2]_7) = ([3 \times 2]_5, [1 \times 2]_7) = ([1]_5, [2]_7) \sim [16]_{35}$$

Adding in $\mathbb{Z}_{35}$:

$$[8 + 2]_{35} = [10]_{35} \sim ([0]_5, [3]_7)$$

Adding in $\mathbb{Z}_5 \otimes \mathbb{Z}_7$:

$$([3]_5, [1]_7) + ([2]_5, [2]_7) = ([3 + 2]_5, [1 + 2]_7) = ([0]_5, [3]_7) \sim [10]_{35}$$

■

$a \in \mathbb{Z}_{35}$	$\mathbb{Z}_5 \otimes \mathbb{Z}_7$	$r = o(a)$	$\left[a^{\frac{r}{2}} - 1\right]_{35} \left[a^{\frac{r}{2}} + 1\right]_{35}$
0	$(0,0)$	1	
1	$(1,1)$	1	
2	$(2,2)$	12	$(28,30)$
3	$(3,3)$	12	$(28,30)$
4	$(4,4)$	6	$(28,30)$
5	$(0,5)$	6	$(19,21)$
6	$(1,6)$	2	$(5,7)$
7	$(2,0)$	4	$(13,15)$
8	$(3,1)$	4	$(28,30)$
9	$(4,2)$	6	$(28,30)$
10	$(0,3)$	6	$(19,21)$
11	$(1,4)$	3	
12	$(2,5)$	12	$(28,30)$
13	$(3,6)$	4	$(28,30)$
14	$(4,0)$	2	$(13,15)$
15	$(0,1)$	1	
16	$(1,2)$	3	
17	$(2,3)$	12	$(28,30)$
18	$(3,4)$	12	$(28,30)$
19	$(4,5)$	6	$(33,35)$
20	$(0,6)$	2	$(19,21)$
21	$(1,0)$	1	
22	$(2,1)$	4	$(28,30)$
23	$(3,2)$	12	$(28,30)$
24	$(4,3)$	6	$(33,35)$
25	$(0,4)$	3	
26	$(1,5)$	6	$(5,7)$
27	$(2,6)$	4	$(28,30)$
28	$(3,0)$	4	$(13,15)$
29	$(4,1)$	2	$(28,30)$
30	$(0,2)$	3	
31	$(1,3)$	6	$(5,7)$
32	$(2,4)$	12	$(28,30)$
33	$(3,5)$	12	$(28,30)$
34	$(4,6)$	2	$(33,35)$

Blue numbers are not coprime to 35. There are always $M - \phi(M) = PQ - (P-1)(Q-1) = P + Q - 1$ non-coprimes, and here we see $5 + 7 - 1 = 11$ blue numbers. As $M = PQ$ becomes

very large, the probability of randomly picking an a that isn't coprime to M is effectively zero,[9] so the fraction of blue numbers drops to effectively zero.

Red numbers are good choices for a, since $\left[a^{\frac{r}{2}}-1\right]_M\left[a^{\frac{r}{2}}+1\right]_M$ is a pair of numbers s.t.

$$\gcd\left(\left[a^{\frac{r}{2}}\pm 1\right]_M, M\right) = P, Q$$

For example,

$$\left[2^{\frac{12}{2}}\pm 1\right]_{35} = [64\pm 1]_{35} = [29\pm 1]_{35} = 28, 30$$

$$\gcd(28, 35) = 7 \qquad\qquad \gcd(30, 35) = 5$$

[9] a would have to be a multiple of either P or Q, primes which are each at least dozens of digits long.

The Probability The Math Part Works

There are some difficulties that can crop up before the Shor algorithm is even run that have to do with the assumptions put on a.

1) a is not coprime to M. In which case you're already done.

For $gcd(a, M) \neq 1$, a has no order, because $[a^r]_M \neq 1$, $\forall r$. However, this is unlikely. The number of numbers not coprime to M is $M - \phi(M) = PQ - (P-1)(Q-1) = P+Q-1 \approx 2\sqrt{M}$. So, the chance of randomly picking a non-coprime number is about $\frac{2\sqrt{M}}{M} = \frac{2}{\sqrt{M}}$.

That said, if this happens, you're done because you've already found a factor of M. Also, call someone and tell them about the fact that you've just experienced one of the least likely things to ever happen to anyone.

2) r isn't even. In which case you pick a new a and repeat.

$$[1]_M \sim ([1]_P, [1]_Q)$$

which means that if $z \sim (x, y)$ and $o([x]_P) = b$ and $o([y]_Q) = c$, then $o([z]_M) = lcm(b, c)$, because

$$[z^{lcm(b,c)}]_M \sim \left([x^{lcm(b,c)}]_P, [y^{lcm(b,c)}]_Q\right) = \left(\left[\left(x^b\right)^{\frac{lcm(b,c)}{b}}\right]_P, \left[\left(y^c\right)^{\frac{lcm(b,c)}{c}}\right]_Q\right) = ([1]_P, [1]_Q)$$

where, by definition, $\frac{lcm(b,c)}{b}$ and $\frac{lcm(b,c)}{c}$ are integers.

Write $\phi(P) = P - 1 = 2^j p$ and $\phi(Q) = Q - 1 = 2^\ell q$, where p, q are the products of all of the odd prime factors of $P-1$ and $Q-1$ respectively. Not that $j, \ell \geq 1$, since $P-1$ and $Q-1$ are both even. The numbers with odd order mod M are those numbers where both numbers in their $\mathbb{Z}_P \otimes \mathbb{Z}_Q$ representation have odd order in mod P and mod Q.

For a prime modulus, P, the number of numbers of order d, where $d|\phi(P)$, is $\phi(d)$. For example, in the $M = 7$ example we see that there are two numbers of order 6 ($\phi(6) = (3-1)(2-1) = 2$), two of order 3 is ($\phi(3) = 3 - 1 = 2$), one of order 2 is ($\phi(2) = 2 - 1 = 1$), and one of order 1 ($\phi(1) = 1$).

So the number of numbers with odd order is

$$\sum_{d|p} \sum_{f|q} \phi(d)\phi(f) = \left[\sum_{d|p} \phi(d)\right]\left[\sum_{f|q} \phi(f)\right] = pq$$

This last step is due to the fact that, in general

$$\sum_{d|N} \phi(d) = N$$

which is just one of those amazing results from number theory.
For example,

$$\phi(1) = 1, \phi(2) = 1, \phi(5) = 4, \phi(10) = 4 \qquad \text{and} \qquad 1 + 1 + 4 + 4 = 10$$

Only numbers coprime to M have definable orders, and there are $\phi(M) = \phi(P)\phi(Q) = 2^{j+\ell}pq$ of those, so the chance of randomly picking a number with an odd order is

$$\frac{1}{\phi(M)} \sum_{d|p} \sum_{f|q} \phi(d)\phi(f) = \frac{pq}{2^{j+\ell}pq} = \frac{1}{2^{j+\ell}} \leq \frac{1}{4}$$

Picking a new a is at least 75% likely to yield a number that has an even order.

Example In the 35 example, we find that of the 24 numbers coprime to 35, only 3 have an odd order, $\{1, 11, 16\}$. Notably, $\frac{3}{24} \leq \frac{1}{4}$.

This lines up exactly with the prediction, that the number of odd-order numbers would be $pq = 1 \cdot 3 = 3$, where p and q are the odd factors of $\phi(5) = 4$ and $\phi(7) = 6$.

■

3) $\left[a^{\frac{r}{2}}\right]_M = -1$**.** In which case $(a^{\frac{r}{2}} + 1)$ is a multiple of M, and neither term has non-trivial factors.[10] Picking a new a will work at least two thirds of the time.

Returning to the product representation, $\mathbb{Z}_M \cong \mathbb{Z}_P \otimes \mathbb{Z}_Q$, we can write $a \sim (x, y)$. Again, $o([x]_P) = B$ and $o([y]_Q) = C$ means that $o([a]_M) = lcm(B, C) = r$. In a prime modulus, $x^2 = 1$ if and only if $x = 1, -1$. So, if $a^r \sim (x^r, y^r) = (1, 1) \sim 1$, then $\left(x^{\frac{r}{2}}, y^{\frac{r}{2}}\right) = (\pm 1, \pm 1)$

There are now three cases:

i)	$\left(x^{\frac{r}{2}}, y^{\frac{r}{2}}\right) = (1, 1) \sim 1$	Impossible, since this would imply that the order is actually $\frac{r}{2}$.
ii)	$\left(x^{\frac{r}{2}}, y^{\frac{r}{2}}\right) = (1, -1)\ or\ (-1, 1)$	This is the ideal case, where $a^{\frac{r}{2}} \neq -1$.
iii)	$\left(x^{\frac{r}{2}}, y^{\frac{r}{2}}\right) = (-1, -1) \sim -1$	This is the problem case.

Rewrite $o([x]_P) = B = 2^i b$, $o([y]_Q) = C = 2^k c$, where b, c are the products of all of the odd factors of B and C. Now, notice what happens when (x, y) is raised to the $\frac{r}{2}$:

[10] "Non-trivial factors" means P or Q, but not $M = PQ$.

$$
\begin{aligned}
& \left(x^{\frac{r}{2}}, y^{\frac{r}{2}}\right) \\
= & \left(x^{\frac{1}{2}lcm(B,C)}, y^{\frac{1}{2}lcm(B,C)}\right) \\
= & \left(x^{\frac{1}{2}2^{max(i,k)}lcm(b,c)}, y^{\frac{1}{2}2^{max(i,k)}lcm(b,c)}\right) \\
= & \left(x^{2^{max(i,k)-1}b\frac{c}{gcd(b,c)}}, y^{2^{max(i,k)-1}c\frac{b}{gcd(b,c)}}\right) \\
= & \begin{cases} (1,-1) & ,i<k \\ (-1,1) & ,i>k \\ (-1,-1) & ,i=k \end{cases}
\end{aligned}
$$

Because if $i < k$, then $B = 2^i b | 2^{max(i,k)-1} b$, similarly for $i > k$. The $\frac{b}{gcd(b,c)}$ and $\frac{c}{gcd(b,c)}$ terms are odd, so they leave the sign the same. We find that the problem only occurs when $i = j$.

Once again writing $\phi(P) = 2^j p$ and $\phi(Q) = 2^\ell q$, we can find the number of numbers with the property that $a \sim (x, y)$, where $o([x]_P) = 2^i b$, $o([y]_Q) = 2^k c$ and $i = k$. Keeping in mind that the order of x must divide $\phi(P) = 2^j p$ and similarly for y,

$$
\begin{aligned}
& \textstyle\sum_{b|p} \sum_{c|q} \sum_{k=1}^{min(j,\ell)} \phi(2^k b)\phi(2^k c) \\
= & \textstyle\sum_{b|p} \sum_{c|q} \sum_{k=1}^{min(j,\ell)} \phi(2^k)^2 \phi(b)\phi(c) \\
= & \left[\textstyle\sum_{b|p} \phi(b)\right]\left[\sum_{c|q} \phi(c)\right]\left[\sum_{k=1}^{min(j,\ell)} \phi(2^k)^2\right] \\
= & [p]\,[q]\left[\textstyle\sum_{k=1}^{min(j,\ell)} (2^{k-1})^2\right] \\
= & \frac{pq}{4} \textstyle\sum_{k=1}^{min(j,\ell)} 4^k \\
= & \frac{pq}{4} \frac{4^{min(j,\ell)+1}-4}{4-1} \\
= & \frac{pq}{12}\left(4^{min(j,\ell)+1} - 4\right) \\
= & \frac{pq}{3}\left(4^{min(j,\ell)} - 1\right)
\end{aligned}
$$

Here we used the properties $\phi(st) = \phi(s)\phi(t)$ when $gcd(s,t) = 1$ and $\phi\left(p^k\right) = (p-1)p^{k-1}$ when p is prime. Also, the sum begins at $k = 1$, because we require that the order must be even (and include at least one power of two).

So, the probability of picking an a such that $a^{\frac{r}{2}} = -1$ is:

$$\begin{aligned} p &= \frac{1}{\phi(M)}\frac{pq}{3}\left(4^{min(j,\ell)}-1\right) \\ &= \frac{1}{2^{j+\ell}pq}\frac{pq}{3}\left(4^{min(j,\ell)}-1\right) \\ &= \frac{1}{3}\frac{1}{2^{j+\ell}}\left(4^{min(j,\ell)}-1\right) \\ &\leq \frac{1}{3}\frac{1}{2^{j+\ell}}4^{min(j,\ell)} \\ &\leq \frac{1}{3}\frac{1}{2^{2min(j,\ell)}}4^{min(j,\ell)} \\ &= \frac{1}{3} \end{aligned}$$

Example In the $M = 35$ example, we have that $19^3 \sim (4,6)$, $24^3 \sim (4,6)$, $34 \sim (4,6)$. These are the only values of a such that $\left[a^{\frac{r}{2}}\right]_{35} = -1$ and the only values that produce pairs $(33,35)$. These pairs are useless since

$$\gcd(33,35) = 1 \qquad\qquad \gcd(35,35) = 35$$

But fortunately, there are only 3 of these problem-numbers out of 24 and

$$\frac{3}{24} \leq \frac{1}{3}$$

Finally, for $\phi(5) = 4 = 2^2 \cdot 1$ and $\phi(7) = 6 = 2^1 \cdot 3$ we have that $min(1,2) = 1$ and therefore the number of these issue-numbers is

$$\frac{pq}{3}\left(4^{min(j,\ell)}-1\right) = \frac{3}{3}\left(4^1-1\right) = 3$$

■

For large $M = PQ$, we don't have to worry about accidentally picking a multiple of P or Q. So, overall there's a chance $q \leq \frac{1}{4}$ of picking an a with odd order r and of the remaining even-ordered a, there's a chance of $p \leq \frac{1}{3}$ of an ineffective value, and therefore

$$\boxed{p(\textit{good number}) \geq \frac{3}{4}\cdot\frac{2}{3} = \frac{1}{2}}$$

Speed

Using binary exponentiation $f(x)$ can be evaluated in logarithmic time.

For values of N of the form $N = 2^n$ the Discrete Quantum Fourier Transform works in $O(\log(N \log(N)))$ time.

On average, each step in the continued fraction approximation halves the distance to the true value. As a result, continued fraction expansions work in logarithmic time.

There is a net chance of 50% that a will be chosen correctly, a 40.5% chance that given a proper a the correct value of r will be found, and a 61% chance that $(\ell, r) = 1$ (which typically doesn't require a new run of the algorithm).

So, in any given run the chance of a complete success is approximately 12%, but a correct answer is easy to verify.

Repeating the algorithm a fixed number of times multiplies the processing time by a constant, but does make the time greater than logarithmic.

Exercises

If you're doing this entirely by hand, then remember that you never have to worry about numbers larger than N when you're doing math mod N.

Example:

$$\left[6^7\right]_{13} = ?$$

By writing $\left[6^7\right]_{13} = \left[6^4 6^2 6^1\right]_{13}$, we can use "exponentiation by squaring":

$$\left[6^2\right]_{13} = [36]_{13} = 10$$

$$\left[6^4\right]_{13} = \left[\left(6^2\right)^2\right]_{13} = \left[10^2\right]_{13} = [100]_{13} = 9$$

In this last step, you could be clever/lazy by using the fact that $[10]_{13} = [-3]_{13}$ and so

$$\left[10^2\right]_{13} = \left[(-3)^2\right]_{13} = 9$$

Finally,

$$\left[6^7\right]_{13} = \left[6^4 6^2 6^1\right]_{13} = [9 \cdot 10 \cdot 6]_{13} = [9 \cdot 60]_{13} = [9 \cdot 8]_{13} = [72]_{13} = 7$$

or just to make the numbers as small as possible at each step:

$$\left[6^7\right]_{13} = [9 \cdot 10 \cdot 6]_{13} = [(-4) \cdot (-3) \cdot 6]_{13} = [12 \cdot 6]_{13} = [(-1) \cdot 6]_{13} = [-6]_{13} = 7$$

■

#1) The Ballad of 2 mod 15.

Here you'll run through the quantum part of Shor's algorithm in order to factor 15. Rather than use an $N > 15^2$, we'll use $N = 16$, because the math will be *much* easier. The initial state is

$$|\psi\rangle = \frac{1}{4} \sum_{x=0}^{15} |x\rangle|0\rangle$$

where the first register is presently $|x\rangle$ and the second is presently $|0\rangle$. Incidentally, both registers are made from 4 qubits, since $N = 16 = 2^4$. Define $f(x) = \left[2^x\right]_{15}$.

a) Apply $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$.

b) "Measure" the second register by randomly[11] picking one of the possible states (they should all be equally likely). What is the state that remains after this measurement?

c) Now that the second register is in a definite state, ignore it (literally stop bothering to write it down). Explicitly perform/calculate the QFT of the first register.

d) "Measure" the first register by randomly selecting one of the available states (they should all be equally likely). The result of this measurement is "k". What is $\frac{k}{N}$?
Since $\frac{kr}{N} \approx \ell \in \mathbb{Z}$, $\frac{k}{N} \approx \frac{\ell}{r}$ where $r < 15$. What is r?

e) Calculate $[2^r]_{15}$, $\left[2^{\frac{r}{2}}+1\right]_{15}$, and $\left[2^{\frac{r}{2}}-1\right]_{15}$.

f) Find the greatest common divisor between 15 and each of $\left[2^{\frac{r}{2}}+1\right]_{15}$ and $\left[2^{\frac{r}{2}}-1\right]_{5}$.

#2) The Curious Case of 20 mod 35.

Define $f(x) = [20^x]_{35}$ and an initial state

$$|\eta\rangle = \frac{1}{8}\sum_{x=0}^{63}|x\rangle|0\rangle$$

a) Suppose the final measurement at the end of Shor's algorithm is $k = 32$. What is r?

b) Calculate $[20^r]_{35}$, $\left[20^{\frac{r}{2}}+1\right]_{35}$, and $\left[20^{\frac{r}{2}}-1\right]_{35}$.

c) Find the greatest common divisor between 35 and each of $\left[20^{\frac{r}{2}}+1\right]_{35}$ and $\left[20^{\frac{r}{2}}-1\right]_{35}$.

d) Your answers to c should feel a little incomplete. What's going on here?

#3) Quantum Interpretation

Typically, the results from a quantum computer are not perfect, but close. Pretend we want to factor

$$M = 21$$

We need an N such that $M^2 < N$, so we choose

$$N = 2^9 = 512$$

[11] Seriously, convince yourself that you're making a random choice. Use dice or coins or something.

because it's the smallest power of 2 greater than $21^2 = 441$. So, although it doesn't matter, this particular calculation could be done with two 9-qubit registers. Finally, because small numbers are better, we choose

$$a = 2$$

We'll use Shor's algorithm to find r, the order of 2 and the smallest number such that

$$[2^r]_{21} = 1$$

The output of the algorithm (the only important part[12]) is

$$k = 425$$

a) Use continued fractions to approximate $\frac{k}{N}$ with a converging series of simpler fractions. Stop when you get to $\frac{\ell}{r}$, where r is the largest and last denominator smaller than $M = 21$.

To get you started with $\frac{k}{N} = \frac{425}{512}$:

$$\frac{425}{512} = 0 + \frac{425}{512} \quad \Rightarrow \quad X \approx [0] = 0$$

$$\frac{512}{425} = 1 + \frac{87}{425} \quad \Rightarrow \quad X \approx [0;1] = 0 + \frac{1}{1} = 1$$

What is r?

b) Find $q = \left[a^{\frac{r}{2}} - 1\right]_{21}$ and $p = \left[a^{\frac{r}{2}} + 1\right]_{21}$.

c) Find $gcd(q, 21)$ and $gcd(p, 21)$.

#4(optional) The Chimera of 4 mod 35.

The big idea behind this question is to get you to think of the one big "gear" $\mathbb{Z}_M$ as a pair of "gears" $\mathbb{Z}_P \otimes \mathbb{Z}_Q$.

a) Find the order, s, of $[4]_5$, by calculating $[4]_5, \left[4^2\right]_5, \left[4^3\right]_5, \ldots$

b) Find the order, t, of $[4]_7$, by calculating $[4]_7, \left[4^2\right]_7, \left[4^3\right]_7, \ldots$

c) The product representation of 4, in $\mathbb{Z}_5 \otimes \mathbb{Z}_7$, is $4 \sim (4,4)$. Find the order, r, of $[4]_{35}$, by calculating $([4]_5, [4]_7), \left(\left[4^2\right]_5, \left[4^2\right]_7\right), \left(\left[4^3\right]_5, \left[4^3\right]_7\right), \ldots$, remembering that $1 \sim (1,1)$.

[12] It doesn't matter what result you see when measuring the second register (just that you measure it).

d) Write an equation that relates r, s, and t, and justify it.

e) Test the equation you came up with in part d, on $34 \sim (4, 6)$ (just look up the orders in the tables). Explain what you had to correct for.

If you already corrected for it: good. This idea, of looking at $\mathbb{Z}_P \otimes \mathbb{Z}_Q$ to understand the behavior (including the orders) of $\mathbb{Z}_M$, is a lot of what's happening in the "The Possible Difficulties Are" section.