1 Shor's Factoring Algorithm

Recall from the previous lecture that to find a nontrivial factor of N, it suffices to find a nontrivial square root of 1 mod N. With probability at least 1/2, $x^{r/2}$ is a nontrivial square root, where x is chosen randomly from Z_N^* and r is its order. Hence, we have reduced the problem of factoring to the problem of computing the order of a randomly chosen x.

1.1 Simplified Case

We begin with the case in which we do our Fourier transforms over Z_q and we happen to have $r \mid q$. This is a totally unreasonable assumption, but the analysis here helps in understanding the general case.

Given x, N, and q (which we suppress in the following), the algorithm is as follows:

Begin with

$$|0\rangle .$$

Apply a Fourier transform over Z_q to get

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle .$$

Perform a classical computation to compute

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \, |x^a \bmod N\rangle .$$

"Measure" the latter quantity (or actually, invoke the principle of safe storage). We will observe some $y = x^k \bmod N$, and the state will collapse into a superposition over all a such that $x^a = y$. That is, we will be left with

$$\frac{1}{\sqrt{q/r}} \sum_{j=0}^{q/r-1} |jr + k\rangle .$$

At this point, we have a uniform superposition over a coset of $\langle r\rangle$. Hence, when we apply another Fourier transform over Z_q, we get a uniform superposition over $\langle q/r\rangle$, regardless of which coset we started in. Now when we make a measurement, we get a random multiple of q/r, and with high probability, when we take $\gcd(lq/r, q)$, we get q/r.

1.2 General Case

In the general case, after applying the first measurement, we get

$$\frac{1}{\sqrt{\lfloor q/r \rfloor}} \sum_{j=0}^{\lfloor q/r \rfloor - 1} |jr + k\rangle \, .$$

This is no longer a coset of a subgroup in Z_q, so the earlier reasoning does not apply. Nevertheless, we will take a Fourier transform over Z_q anyway, and we will show that we get constructive interference primarily at points close to multiples of q/r. In fact, we will be close enough to essentially "round" to the nearest multiple, and this will allow us to calculate r with some reasonable probability.

In what follows, we drop the floors, since it doesn't make much difference for the calculations we will be making.

Applying a Fourier transform over Z_q to the expression above, we get

$$\sum_{c=0}^{q-1} \alpha_c \, |c\rangle \, ,$$

where

$$\alpha_c = \frac{1}{\sqrt{q}} \sum_{j=0}^{q/r-1} \frac{1}{\sqrt{q/r}} \omega^{(jr+k)c} = \omega^{kc} \frac{\sqrt{r}}{q} \sum_{j=0}^{q/r-1} (\omega^{rc})^j .$$

(ω here is a primitive qth root of unity, $e^{2\pi i/q}$.)

Notice that if rc is small mod q, the terms in the sum cover only a small angle in the complex plane, and hence, the magnitude of the sum is almost the sum of the magnitudes. In particular, consider values of c such that $-r/2 \leq rc \bmod q \leq r/2$, so that the terms of the sum cover less than half of the unit circle. Then at least half of the terms make less than a $45°$ angle with the vector sum and each of these contributes at least $1/\sqrt{2}$ of its magnitude to the sum. Hence, for all such c, we have $|\alpha_c| \geq (q/r)(1/2\sqrt{2})(\sqrt{r}/q) = (1/2\sqrt{2})(1/\sqrt{r})$. Upon measurement, each such c is observed with probability at least $1/8r$; hence, with constant probability, we will observe some such c.

Consider how this compares to the simplified case. In that case, for values of c which are multiples of q/r, that is, for which $rc \bmod q = 0$, each term in the sum is 1, so we get complete constructive interference. On the other hand, for any other value of $c = lq/r + k$, the terms in the sum, ω^{jrk}, are evenly spread around the unit circle and completely cancel out. Thus, in the simplified case, we are left with exactly the multiples of q/r.

As an example of the more general case, consider the situation with $N = 15$ and $x = 2$ (so that $r = 4$), with $q = 17$. We perform a Fourier transform over Z_{17} to get a uniform superposition over values mod 17, and then calculate 2^a mod 15 for all values of a mod 17. This gives us

$$\frac{1}{\sqrt{17}}(|0\rangle\,|1\rangle + |1\rangle\,|2\rangle + |2\rangle\,|4\rangle + |3\rangle\,|8\rangle + |4\rangle\,|1\rangle + \cdots).$$

When we measure x^a, we collapse to a state which contains every fourth value of a. For example, measuring $x^a = 2$ results in the state

$$\frac{1}{2}(|1\rangle + |5\rangle + |9\rangle + |13\rangle).$$

Now we do a Fourier transform again. Consider the value of α_{13} after the transform, where we have $rc = 4(13) = 1 \bmod 17$.

$$|\alpha_{13}| = \frac{1}{2}(\frac{1}{\sqrt{17}})(\omega^{13} + \omega^{14} + \omega^{15} + \omega^{16}).$$

Hence, we get primarily constructive interference, and the probability of measuring $c = 13$ will be high. Note that 13 is very close to $3q/r = 12.75$. The other α's with large magnitudes will be similarly close to multiples of q/r.

1.3 Finishing Up

After making our measurement of c, we have a value that, with non-negligible probability, satisfies $-r/2 \leq rc \bmod q \leq r/2$. The problem now is to find the value of r.

We have for some value l that $|cr - lq| \leq r/2$. Rewriting, we get $|c/q - l/r| \leq 1/2q$. The fraction c/q is known to us. Furthermore, with high probability, l will be relatively prime to r, so it suffices to compute l/r in lowest terms. Since we are free to choose q, we need only choose q to be large enough so that there is a unique fraction l/r which is that close to c/q.

Note that $r \leq N$, since it is the order of an element mod N. Furthermore, notice that two fractions whose denominators are no greater than N differ by at least $1/N^2$. Hence, if we choose $q \geq N^2$, there will be a unique fraction l/r satisfying the inequality above with $r \leq N$.

Finally, to calculate l/r, we simply compute the continued fraction expansion of c/q, stopping at the largest denominator smaller than N. By the properties of continued fraction expansions, this always gives us the closest approximation to c/q with denominator smaller than N, which is precisely the value we are looking for.