USS: Introduction to mathematical cryptography
Monday July 25 problems

Factoring using Shor's algorithm

1. Suppose that you are using Shor's algorithm to compute the multiplicative order of 2 modulo 15. Throughout this problem we will use the notation set up in the slides.
   (a) What value of q would you take?
   (b) Suppose that your measurement in Shor's algorithm is $j = 192$. What value would you obtain for r, the multiplicative order of 2 modulo 15? Does it agree with the real multiplicative order of 2 modulo 15?
   (c) Use your value of r to factor 15.
2. Suppose that you wish to factor $N = 35$ using Shor's algorithm, and you use the value $a = 2$.
   (a) What is the multiplicative order r of 2 modulo 35? You can compute this by hand; as a hint to go faster, you may use the fact that the multiplicative order of 2 modulo 35 divides $\varphi(35) = 24$.
   (b) What is $a^{r/2} \pmod{35}$, where r is the multiplicative order of 2 modulo 35?
   (c) If you can, use the value you computed in part (b) to compute a nontrivial factor of 35.
3. Suppose that you wish to factor $N = 33$ using Shor's algorithm, and you use the value $a = 2$.
   (a) What is the multiplicative order r of 2 modulo 33? You can compute this by hand; as a hint to go faster, you may use the fact that the multiplicative order of 2 modulo 33 divides $\varphi(33) = 20$.
   (b) What is $a^{r/2} \pmod{35}$, where r is the multiplicative order of 2 modulo 35?
   (c) If you can, use the value you computed in part (b) to compute a nontrivial factor of 35.

Continued fractions and Shor's algorithm

1. In this problem we will prove that if there is a fraction $\frac{M}{r}$ with $r < N$ such that $\left|\frac{j}{2^q} - \frac{M}{r}\right| < \frac{1}{2N^2}$, then this fraction is unique with this property.
   (a) Suppose that $\frac{M}{r}$ and $\frac{M_1}{r_1}$ are two distinct rational numbers, with $0 < r < N$ and $0 < r_1 < N$. Show that
   $$\left|\frac{M_1}{r_1} - \frac{M}{r}\right| > \frac{1}{N^2}.$$

(b) Suppose, as in Shor's algorithm, that we have

$$\left|\frac{j}{2^q} - \frac{M}{r}\right| < \frac{1}{2N^2} \quad \text{and} \quad \left|\frac{j}{2^q} - \frac{M_1}{r_1}\right| < \frac{1}{2N^2}.$$

Show that $\frac{M}{r} = \frac{M_1}{r_1}$.

Roots of unity

1. In this problem we will prove that if $\zeta \neq 1$ is any other nth of unity (not necessarily primitive), then
$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-2} + \zeta^{n-1} = 0.$$

(a) Use induction to show that for all $n \geq 2$,

$$x^n - 1 = (x-1)\sum_{k=0}^{n-1} x^k = (x-1)(1 + x + x^2 + \cdots + x^{n-2} + x^{n-1}).$$

(b) Use the fact that $\zeta^n - 1 = 0$ and the formula you proved in part (a) to prove that

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-2} + \zeta^{n-1} = 0$$

if $\zeta \neq 1$ is an nth root of unity.

What are the odds of Shor's algorithm succeeding?

Recall that Shor's algorithm begins with choosing a number a with $1 < a < N$ at random. It is possible to show that if if $N = pq$ for p, q two distinct odd primes, the probability that $\gcd(a, N) > 1$ is **negligible** (in the sense of the Tuesday July 19 problem set) as N gets large. So it is very likely that a will be relatively prime to N.

Assuming that $\gcd(a, N) = 1$, Shor's algorithm will work if the multiplicative order r of a modulo N is even and $a^{r/2} \not\equiv -1 \pmod{N}$. In this series of problems we work out what the probability is of this happening. This probability affects how often we expect to have to start the algorithm over with a new a.[1] We will see that it is pretty high, so we don't expect to have to run Shor's algorithm too many times.

This assignment requires the use of the Chinese Remainder Theorem, which you may or may not have seen before. If you have not seen it, then the facts you will need are the following:

1. If $N = pq$ for p, q distinct primes, then $x \equiv 1 \pmod{N}$ if and only if $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$.

2. If $N = pq$ for p, q distinct primes, then $x \equiv -1 \pmod{N}$ if and only if $x \equiv -1 \pmod{p}$ and $x \equiv -1 \pmod{q}$.

[1] There is another point at which the algorithm can fail when we interpret the outcome of the quantum algorithm using continued fractions, but we ignore that for now.

1. In this problem, p is an odd prime. We first compute the odds that an element chosen uniformly at random from $(\mathbb{Z}/p\mathbb{Z})^\times$ has odd order.

   (a) Suppose that $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$; show that the element $g^s \in (\mathbb{Z}/p\mathbb{Z})^\times$ has multiplicative order
   $$k = \frac{p-1}{\gcd(p-1, s)}.$$
   Here $s = 0, 1, 2, \ldots, p-2$.

   (b) Let $p - 1 = 2^e m$ with m odd. Using your work from part (a), show that the order of $g^s \in (\mathbb{Z}/p\mathbb{Z})^\times$ is odd if and only if 2^e divides s.

   (c) If s is chosen uniformly at random from the values $s = 0, 1, 2, \ldots, p-2$ (in other words, each of these numbers has an equal chance of being chosen), show that the probability that the order of $g^s \in (\mathbb{Z}/p\mathbb{Z})^\times$ is odd is $\frac{1}{2^e}$.

2. Now let $N = pq$ for p, q two distinct odd primes, and let $1 < a < N$ with $\gcd(a, N) = 1$. Suppose further that the multiplicative order of a modulo p is k and the multiplicative order of a modulo q is ℓ. Finally, write $p - 1 = 2^e m$ for m odd and $q - 1 = 2^f m'$ for m' odd.

   (a) Show that if r is the multiplicative order of a modulo N, then r is the least common multiple of k and ℓ.

   (b) Using your result from part (a), show that r is odd if and only if both k and ℓ are odd.

   (c) Since a is chosen randomly, we can show using the result of problem 1 that k is odd with probability $\frac{1}{2^e}$ and ℓ is odd with probability $\frac{1}{2^f}$. In addition, the event that k is odd is independent from the event that ℓ is odd. What is the probability that r is odd?

   (d) Show that the probability that r, the multiplicative order of a modulo N is odd, is always less than or equal to $\frac{1}{4}$, so that r is even with probability at least $\frac{3}{4}$.

3. Finally, assuming that r is even, we must compute the probability that $a^{r/2} \equiv -1 \pmod{N}$. This is trickier, so we will only cover a special case here, but this probability is always less than or equal to $\frac{1}{2}$. Throughout this problem we use the notation we have established in problems 1 and 2 above.

   (a) Prove that $a^{r/2} \equiv -1 \pmod{p}$ if and only if $2\gcd(k, \ell)$ does not divide ℓ. (This means that the largest power of 2 that divides ℓ is smaller than the largest power of 2 that divides k.) Note that by symmetry it is also true that $a^{r/2} \equiv -1 \pmod{q}$ if and only if $2\gcd(k, \ell)$ does not divide k.

   (b) Prove that $a^{r/2} \equiv -1 \pmod{N}$ if and only if the largest power of 2 that divides k is equal to the largest power of 2 that divides ℓ.

(c) Suppose that $e = f = 1$, and remember that we assume that r is even. Show that the probability that $a^{r/2} \equiv -1 \pmod{N}$ is $\frac{1}{4}$.

The conclusion you should draw from this problem is that overall, these two constraints (that r needs to be even, and that $a^{r/2} \not\equiv -1 \pmod{N}$) balance each other out: When e and f are large, then the probability that r is even is really big, but it's only just a little bit better than 50-50 probability that $a^{r/2} \not\equiv -1 \pmod{p}$. So overall in that case the chance of success is approximately $\frac{1}{2}$. When $e = f = 1$ (so e and f are as small as they can be), then the probability that r is even is $\frac{3}{4}$, which is as small as it can be, but the probability that $a^{r/2} \not\equiv -1 \pmod{N}$ is $\frac{3}{4}$, so overall the probability of success is $\frac{9}{16}$, which is also close to $\frac{1}{2}$. All of the other cases make it more likely that we will succeed. So overall the probability that the a we choose will be suitable is always greater than $\frac{1}{2}$.