Handout #6: Basic number theory stuff, used in Shor's algorithm for quantum-computing the factors of an integer

Suppose N is some large number that we wish to factor. We proceed by the following steps:

Step 1: Check to see whether N is even, or is the power of some prime. (There are efficient algorithms for performing both checks.) If N is even, divide it by 2 and factor N/2. If N is the power of some prime, there are efficient algorithms for calculating this prime. If N is neither even, nor a prime power, proceed to Step 2.

Step 2: Pick a number $a < N$ at random. Use **Euclid's algorithm** (described below) to find the greatest common divisor of a and N. If $\gcd(a,N) = 1$, proceed to Step 3. If $\gcd(a,N) > 1$, then divide N by it and factor the two resulting numbers.

Step 3: At this point, we have a number $a < N$ that is co-prime to N (i.e., it has no common factors with N that are > 1). Then it is possible to show that the function $f(x) = a^x \bmod N$ is periodic, so that its period r satisfies the equation $a^r \bmod N = 1$. (Proof below.) **We use our quantum computer to find r, by means of the algorithm described in class.**

Step 4: We have now found numbers a and r such that $a^r = kN + 1$, for some integer k. **If we are lucky**, r is even. (Luck is not guaranteed: consider $a = 4$, $N = 63$, $r = 3$.) In that case, we can rewrite this equation as $(a^{r/2} + 1)(a^{r/2} - 1) = kN$, where the two factors on the lhs are integers.

Step 5: We know that at least one of the numbers $(a^{r/2} + 1)$ and $(a^{r/2} - 1)$ shares a factor > 1 with N. We can now use Euclid's algorithm to find the greatest common divisors that N shares with $(a^{r/2} + 1)$ and $(a^{r/2} - 1)$, respectively. **If we are lucky**, one of these will be a number strictly between 1 and N. (Luck is not guaranteed: consider a = 14, N = 15, r = 2.) This completes the procedure.

How lucky do we need to be, in Steps 4 and 5? Well, if N is neither even nor a prime power, and if a is co-prime to N, then the probability is greater than 50% that the r we find will meet the conditions described in Steps 4 and 5. (That's not supposed to be obvious: consider it a bit of number-theory magic.) Given that this procedure can be performed efficiently, that's plenty high enough.

Euclid's algorithm: Suppose we have two integers x and y, with y > x. Then Euclid's algorithm for finding gcd(x,y) (the greatest common divisor of x and y) is based on the following result:

gcd(x,y) = x if y mod x = 0;

gcd(x,y) = gcd(x,y mod x) if y mod x > 0.

It's obvious how to turn this result into an efficient algorithm for computing gcd(x,y). The proof of the result is straightforward. If y mod x = 0, then y = nx, for some integer n, so obviously gcd(x,y) = x. If y mod x > 0, then y = nx + m, for some (positive) integers n and m. Let f = gcd(x,y). Then, since f evenly divides both x and y, it must also evenly divide m. So f is a factor in common to x and m = y mod x. Suppose that there is some f' > f which is also a factor in common to x and m. Then, since f' would have to evenly divide both x and m, it would also evenly divide y. So it would be a factor in common to x and y, which is impossible, since f is the greatest such factor. Therefore f = gcd(x,m).

Proof of stuff used in Step 3: First, it's obvious (by the "pigeonhole principle") that there are integers x and y, with y > x, such that a^x mod N = a^y mod N. Let y be the smallest integer > x that meets this condition. Let r = y – x. Observe that r must be less than N. (Why?)

Suppose that a^r mod N = 1. Then it follows that f(x) = a^x mod N is periodic, with period r: for f(x + r) = ($a^x a^r$) mod N = (a^x mod N)(a^r mod N) mod N = a^x mod N = f(x). [Exercise: Show that mod N "distributes" in the way just used here: that is, show that for any x, y, N, xy mod N = (x mod N)(y mod N) mod N.]

So we need to show, given that a^x mod N = $a^x a^r$ mod N, that a^r mod N = 1. We *cannot* appeal to the result that for any x, y, N, with x ≠ 0, if x mod N = xy mod N, then y mod N = 1; for there is no such result. Counterexample: x = 12, y = 8, N = 21. We *can* appeal to a weaker result:

Suppose x ≠ 0, and x and N are co-prime. Then if x mod N = xy mod N, y mod N = 1.

Proof: Since x mod N = xy mod N, (xy – x) = x(y – 1) must be evenly divisible by N. but x and N share no factors in common. So in fact (y – 1) must be evenly divisible by N. But that is just to say that y mod N = 1.

Now recall that a^x mod N = $a^x a^r$ mod N. Since a shares no factors with N, a^x likewise shares no factors with N. So a^r mod N = 1, as needed.