Factoring as Period Finding

Suppose we wish to find a factor of an n-bit number N.

Select integer $a \in [2, N-1]$ at random and compute GCD(a, N), which can be done in $O(n^3)$ steps using the Euclidean algorithm.

If GCD$(a, N) \neq 1$, we are done.

So, suppose GCD$(a, N) = 1$.

Order of an element

Integers $a \in [1, N-1]$ coprime to N form a group under multiplication modulo N.

Each element of this group has a finite order r, the smallest positive integer such that

$$a^r \equiv 1 \pmod{N}$$

Determining the order of a is equivalent to finding the period of the function

$$f_{N,a}(x) = a^x \pmod{N}.$$

The order of a can be found in poly(n) time using the quantum period-finding algorithm.

The oracle is implemented by a subroutine that computes the function $f_{N,a}$, which can be done in complexity $O(n^3)$ using classical circuits.

Factoring algorithm

Suppose we have found the order r of a.

If r is odd the factoring algorithm fails and we repeat the procedure with a new randomly chosen element a.

So, suppose we have found an element a co-prime to N whose order r is even. Then,

$$N \text{ divides } (a^{r/2}+1)(a^{r/2}-1).$$

Since r is the order of a, N does not divide $a^{r/2}-1$.

If N also does not divide $a^{r/2}+1$, then N will have a nontrivial common factor with each of $a^{r/2} \pm 1$.

In this case, GCD$(a^{r/2}\pm 1, N)$ are nontrivial factors of N which can be found in $O(n^3)$ steps using the Euclidean algorithm with classical computation.

Factoring algorithm (cont'd)

To summarize, we succeed unless (1) the order r is odd, or (2) r is even but

$$a^{r/2} \equiv 1 \pmod{N}.$$

How likely is success? It turns out the probability of success is at least $1/2$ conditional on a being chosen uniformly from the set of numbers $[2, N-1]$ that are coprime to N.