Lecture 9

In which we show how to solve the integer factoring problem given an algorithm for the period-finding problem.

1 The Algorithm

In the past lecture we described a quantum polynomial time algorithm for finding the period of a periodic function. We summarize below the properties of the algorithm.

Theorem 1 (Lecture 8) *Let $M = 2^m$ and let $f : \{0, \ldots, M-1\} \to \{0, \ldots, M-1\}$ be a function computable by a classical circuit of size S, and suppose that f is such that there is a $1 \leq r \leq \sqrt{M}$ with the properties that*

$$\forall x \in \{0, \ldots, M-r-1\}. f(x) = f(x+r)$$

$$\forall x \in \{0, \ldots, M-r-1\}. f(x), f(x+1), \ldots, f(x+r-1) \text{ are all different}$$

Then, given the circuit for f, there is a quantum algorithm of complexity $O(S+m^3)$ that finds r.

Given the above algorithm, the following is an algorithm that, given a composite integer N, finds a non-trivial factor of N in polynomial time with constant probability.

- Input: N
- Let m be such that $2^m \leq N^2 < 2^{m+1}$ and let $M := 2^m$
- Step 1: if there is a $k \geq 2$ such that $N = a^k$, then output a The existence of such a factorization of N can be found by trying all k between 2 and $\log_2 N$ and then, for a fixed k, use binary search to determine if there is an a such that $a^k = N$.
- Step 2: pick a random $a \in \{1, \ldots, N-1\}$. If $\gcd(a, N) \neq 1$, then output $\gcd(a, N)$

- Step 3: find the smallest r such that $a^r \equiv 1 \bmod N$

  This is where use the period-finding algorithm. We define the function $f(x) := a^x \bmod N$ with domain $\{0, \ldots, M-1\}$. Such a function is computable in time $O(m^3)$ and so it has a (known) polynomial size classical circuit. The value r is such that $f(x) = f(x+r)$ for every x, and we can also see that $f(0), \ldots, f(r-1)$ have to be all different, otherwise we would have $a^j \equiv a^i \bmod N$, and so $a^{j-i} \equiv 1 \bmod N$, and r would not be the smallest power of a that gives us 1. We also have $r \leq N \leq \sqrt{M}$, so we can use the quantum period-finding algorithm applied to f to find r.

- Step 4: if r is even and $a^{r/2} \not\equiv -1 \bmod N$, output $\gcd(a^{r/2} + 1 \bmod N, N)$, otherwise output $\perp$.

To see what happens at Step 4, consider the following fact:

Claim 2 *Suppose that y is such that*

- $y \not\equiv 1 \bmod N$
- $y \not\equiv -1 \bmod N$
- $y^2 \equiv 1 \bmod N$

Then $y + 1 \bmod N$ share a non-trivial common factor with N.

PROOF: We have

$$0 = y^2 - 1 \bmod N = (y-1) \cdot (y+1) \bmod N$$

so we have that

$$(y - 1 \bmod N) \cdot (y + 1 \bmod N)$$

is a multiple of N. But both $(y - 1 \bmod N)$ and $(y + 1 \bmod N)$ are smaller than N, and non-zero, so for their product to be a multiple of N it means that the factors of N are split non-trivially between the two numbers. □

The claim shows that if we give an output different from $\perp$ at Step 4 then it is a correct output, because we can apply the claim with $y = a^{r/2}$ noting that we cannot have $a^{r/2} \equiv 1 \bmod N$ or else r would not be the smallest power of a such that $a^r \equiv 1 \bmod N$.

It is clear that if the algorithm gives an output at Step 1 or at Step 2 then it is a non-trivial factor of N.

If N is composite, then it can be written as $N = p_1^{k_1} \cdot \ldots p_\ell^{k_\ell}$. If $\ell = 1$, then $k_1 \geq 2$ and the algorithm finds a non-trivial factor at Step 2. This means that in the rest of the analysis we may restrict ourselves to the case $\ell \geq 2$. Conditioned on not giving an output at Step 2, the algorithm selects an a uniformly at random in $\mathbb{Z}_N^*$, where $\mathbb{Z}_N^*$ is the set of all integers a such that $\gcd(a, N) = 1$, together with the operation of multiplication.

In order to conclude that the algorithm finds a non-trivial factor of N with constant probability, it remains to prove that

Lemma 3 (Main) *Let $N = p_1^{k_1} \cdot \ldots \cdot p_\ell^{k_\ell}$ be a composite number with $\ell \geq 2$ distinct prime factors. Select uniformly at random an element $a \in \mathbb{Z}_N^*$. Then there is probability at least $1 - 2^{\ell-1} \geq 1/2$ that the order r of a is even and that $a^{r/2} \not\equiv -1 \bmod N$.*

Where the *order* of an element $a \in Z_n^*$ is the smallest $r > 0$ such that $a^r \equiv 1 \bmod N$.

2 Proof of the Main Lemma

Our analysis will proceed by considering the value of $a \bmod p_i^{k_i}$ for each $i = 1, \ldots, \ell$, and the order of $a \bmod p_i^{k_i}$ for each i.

We begin with the following fact, whose proof we skip.

Claim 4 *Let p be prime and let b be selected uniformly at random in $\mathbb{Z}_{p^k}^*$. Let r be the order of b. Then, with probability 1/2, the largest power of 2 that divides r is also the largest power of 2 that divides $(p-1) \cdot p^{k-1}$, and with probability 1/2 it is not.*

In particular, the above claim shows that if we pick b at random in $\mathbb{Z}_{p^k}^*$ and compute the order r of b, and find what is the largest power 2^d of 2 that divides r, then each possible value of d has probability at most 1/2 of occurring.

The next observation is that, by the Chinese remainders theorem, the mapping

$$a \rightarrow a \mod p_1^{k_1}, a \mod p_2^{k_2}, \cdots, a \mod p_\ell^{k_\ell}$$

is a bijection between $\mathbb{Z}_N^*$ and $\mathbb{Z}_{p_1^{k_1}}^* \times \cdots \times \mathbb{Z}_{p_\ell^{k_\ell}}^*$.

This means that if we sample a uniformly at random from $\mathbb{Z}_N^*$ and then compute

$$\begin{aligned} a_1 &:= a \bmod p_1^{k_1} \\ &\cdots \\ a_\ell &:= a \bmod p_\ell^{k_\ell} \end{aligned}$$

then each a_i is uniformly distributed in $\mathbb{Z}_{p_i^{k_i}}^*$ and the a_i are mutually independent.

Let r_i be the order of a_i in $\mathbb{Z}^*_{p_i^{k_i}}$, let 2^{d_i} be the largest power of two that divides r_i. The main lemma follows from the following fact. (Because the d_i are independent random variables, and each of them takes each possible value with probability at least 1/2.)

Lemma 5 *If the order r of a is odd, or if it is even and $a^{r/2} \equiv -1 \bmod N$, then $d_1 = d_2 = \cdots = d_\ell$.*

Proof: Notice that each r_i divides r, so if r is odd it means that each r_i has to be odd and so $d_1 = d_2 = \cdots = d_\ell = 0$.

If r is even and $a^{r/2} \equiv -1 \bmod N$, then we also have $a_i^{r/2} \equiv -1 \bmod p_i^{k_i}$. This means that r_i cannot divide $r/2$, because otherwise $a_i^{r/2} \equiv 1 \bmod p_i^{k_i}$. But if r_i divides r and does not divide $r/2$ it follows that the largest power of two dividing r_i is also the largest power of two dividing r, so if we let 2^d be the largest power of two dividing r we have $d_1 = d_2 = \cdots = d_\ell = d$.

□