Lecture 17

Correctness.

Proposition 7. *If $d > 1$, then d is either p or q.*

Proof. Since $d \mid N$, by definition, there exists a positive integer e such that $de = N = pq$. Express d and e as a product of primes $d = d_1 \cdots d_i$ and $e = e_1 \cdots e_j$, where i, j are non-negative integers, which is possible by the first part of Theorem 1. So that

$$d_1 \cdots d_i \cdot e_1 \cdots e_j = pq \tag{87}$$

Since $1 < d$, we must have $i \geq 1$. There are two cases

1. $i = 1$. In this case, $d = d_1 \in \{p, q\}$ by the second part of Theorem 1.
2. $i \geq 2$. In this case, $\{d_1, d_2\}$ must be $\{p, q\}$ by the second part of Theorem 1. So $d \geq d_1 d_2 \geq pq$. But this is a contradiction since $d \mid a$ and $0 < a < N$.

So we must be in the first case, which concludes the proof. □

Proposition 8. *If $d' > 1$, then d' is either p or q.*

Proof. Observe that $a^{r/2} - 1 \mod N$ cannot be 0 by the definition of r. So $0 < a^{r/2} - 1 \mod N < N$. Then the proof is the same as before since the only fact about a the previous proof used is $0 < a < N$. □

Fact 7 (Section 13.3 of [Kitaev, Shen, Vyalyi], with $k = 2$)**.** Suppose a is chosen uniformly from the set $\{a' \in \{1, \ldots, N-1\} \mid a' \text{ is coprime to } N\}$, then

$$\Pr[r \coloneqq \mathrm{ord}_N(a) \text{ is even and } a^{r/2} \neq -1 \mod N] \geq 1/2. \tag{88}$$

Comment: proof uses the cyclicity of $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$ and the Chinese Remainder Theorem. For a self-contained set of notes on the cyclicity part, see my notes.

Theorem 2. *The probability that the algorithm outputs "don't know" is at most $1/2$. When it doesn't output "don't know", it outputs p or q.*

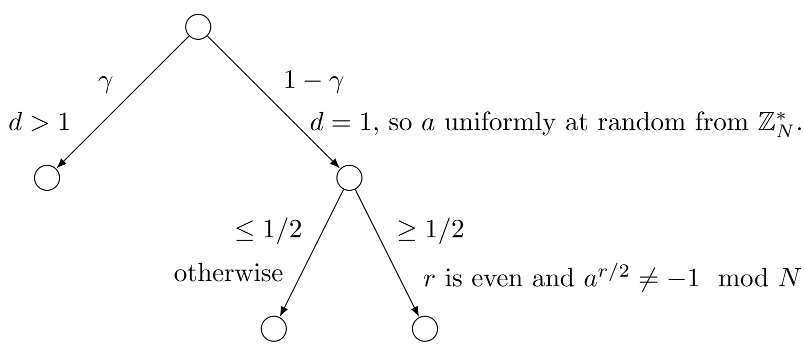
Proof. The second part follows from the previous two propositions, so it suffices to prove the first part.

Let

$$\mathbb{Z}_N^* \coloneqq \{a' \in \{1, \ldots, N-1\} \mid a' \text{ is coprime to } N\} \tag{89}$$

Let $\gamma \in [0, 1]$ denote the probability that $d > 1$. The analysis does not need to know its value. Comment: though could sanity check the γ is small, else don't need quantum algorithm, just randomness is enough!

Draw the following probability diagram.



Then it suffices to show that in the case the event in Eq. (88) occurs, that is $r \coloneqq \mathrm{ord}_N(a)$ is even and $a^{r/2} \neq -1 \mod N$, we go to the third step and have $d' > 1$. Clearly go to the third step, so suffices to show $d' > 1$.

Now,

$$(a^{r/2} - 1)(a^{r/2} + 1) = a^r - 1 \tag{90}$$

Mod N both sides gives

$$(a^{r/2} - 1)(a^{r/2} + 1) = 0 \mod N \tag{91}$$

Therefore, $(a^{r/2} - 1)(a^{r/2} + 1) = NM'$ for some integer M'. So

$$(a^{r/2} - 1 \mod N)(a^{r/2} + 1 \mod N) = NM = pqM \tag{92}$$

for some integer M.

So by Theorem 1, p, q must appear in the prime factorization of $(a^{r/2} - 1 \mod N)(a^{r/2} + 1 \mod N)$. Yet

1. p, q cannot both be in that of $(a^{r/2} - 1 \mod N)$ else $a^{r/2} = 1 \mod N$ contradicting the periodicity of r.
2. p, q cannot both be in that of $(a^{r/2} + 1 \mod N)$ else $a^{r/2} = -1 \mod N$ contradicting the case we are in.

Therefore, exactly one of p or q must be in the prime factorization of $(a^{r/2} - 1 \mod N)$, so $d' := \gcd(a^{r/2} - 1 \mod N, N) > 1$, as required. $\square$