Exercise 7.1

Task

Show that for any $x \in Z_n$, we have $D_{n,d}(E_{n,e}(x)) = x^{ed} \mod n = x$. In the text we showed this for $x \in Z_n^*$. Be careful not to repeat that argument, you have to include the case where $x \notin Z_n^*$. Hint: by the Chinese Remainder theorem, $x^{ed} \equiv x \mod n$ if and only if $x^{ed} \equiv x \mod p$ and $x^{ed} \equiv x \mod q$.

Solution

In order to prove this we can look at two cases:

Case 1: $x \in Z_n^*$

This case we've already seen proven in the book, but let's sketch it for completeness.

We want to show that $D_{n,d}(E_{n,e}(x)) = x$ for all $x \in Z_n^*$. We'll use the fact that the order of the group Z_n^* is $\phi(n) = (p-1)(q-1)$. Also, $ed \mod (p-1)(q-1) = 1$.

Therefore, we have:

$$D_{n,d}(E_{n,e}(x)) = x^{ed} \mod n = x^{ed \mod (p-1)(q-1)} \mod n = x^1 \mod n = x$$

Case 2: $x \in Z_n \setminus Z_n^*$

In this case, we have that x is either a multiple of p or of q i.e. $gcd(n, x) \neq 1$. From the Chinese Remainder Theorem we know that $x^{ed} = x \mod n \iff x^{ed} = x \mod p$ and $x^{ed} = x \mod q$.

Let's check if this holds when $x = tp$ i.e. a multiple of p. We'll only need to prove it for one of p and q and then we can swap the letters and use the same proof. It will still hold as we have picked p here arbitrarily.

So, we have that $x = tp$, and we need to show that $x^{ed} = x \mod p$ and $x^{ed} = x \mod q$.

The first one is $x^{ed} \mod p = tp^{ed} \mod p = 0 = tp \mod p = x \mod p$. Because both sides are a multiple of p, they're both zero.

The second is $x^{ed} = x \mod q$. k is some integer.

$$x^{ed} \mod q = x^{ed-1}x = x^{1+k\phi(n)-1} \mod q = x^{k(p-1)(q-1)} \mod q = (x^{q-1})^{k(p-1)} \mod q = 1^{k(p-1)}x \mod q = x \mod q$$

And we can apply the same approach if x is a multiple of q instead, but it will be the same outcome. This proves the second case.