Question 6

(a)

We denote a polynomial with degree $\phi(n)-1$ by $f(x) = f_0 + f_1 x + \ldots + f_{\phi(n)-1}x^{\phi(n)-1}$. It is trivially true that if $f(x) = g(x)$, then $f(\zeta_i) = g(\zeta_i)$ for all $1 \le i \le \phi(n)$.

On the other hand, if for two polynomials f, g with degree $\phi(n)-1$, their NTT representations are exactly identical, then for all $1 \le i \le \phi(n)$:

$$f(\zeta_i) = g(\zeta_i)$$

Define $h(x) = f(x) - g(x)$, then $\zeta_1, \zeta_2, \ldots, \zeta_{\phi(n)}$ are distinct roots of $h(x)$. This means that $h(x)$ must have form:

$$h(x) = h'(x)(x-\zeta_1)(x-\zeta_2)\ldots(x-\zeta_{\phi(n)})$$

Because $f(x), g(x)$ both have degree $\phi(n)-1$, the degree of $f(x)-g(x)$ cannot be more than $\phi(n)-1$. Therefore, $h(x)$ must be 0, because otherwise it must have degree of at least $\phi(n)$. ■

(b)

Recall the NTT transformation described in part (1): $\mathrm{NTT}(f) \mapsto (f(\zeta_1), f(\zeta_2), \ldots, f(\zeta_{\phi(n)}))$. From here we know:

$$\begin{aligned}
\mathrm{NTT}(f\cdot g) &= ((f\cdot g)(\zeta_1), (f\cdot g)(\zeta_2), \ldots, (f\cdot g)(\zeta_{\phi(n)})) \\
&= (f(\zeta_1)\cdot g(\zeta_1), f(\zeta_2)\cdot g(\zeta_2), \ldots, f(\zeta_{\phi(n)})\cdot g(\zeta_{\phi(n)})) \\
&= (f(\zeta_1), f(\zeta_2), \ldots, f(\zeta_{\phi(n)})) \circ (g(\zeta_1), g(\zeta_2), \ldots, g(\zeta_{\phi(n)})) \\
&= \mathrm{f} \circ \mathrm{g}
\end{aligned}$$

■