

$p \cdot q \pmod{X^n + 1} = p \cdot q + w \cdot (X^n + 1)$ for some w . We question whether $p(r) \cdot q(r) = (p \cdot q)(r)$

But we actually have:

$$\begin{aligned}(p \cdot q)(r) \pmod{X^n + 1} &= (p \cdot q + w \cdot (X^n + 1))(r) = \\ &= p(r) \cdot q(r) + w(r) \cdot (r^n + 1)\end{aligned}$$

So if we apply modulus on both sides of the equation ($\pmod{r^n + 1}$) we should be able to eliminate the difference: