Multiplicative orders - Solution

May 8, 2025

Let $N \in \mathbb{N}$ and $x \in G = (\mathbb{Z}/N\mathbb{Z})^*$ be an element of the multiplicative group. From group theory we know that the order $\text{ord}(x)$ of x is a divisor of the order of the group $\text{ord}(G)$. We also know that $x^{k\,\text{ord}(x)} = 1$ for all $k \in \mathbb{N}$.

Now to solve the exercise we first factor $N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Then we calculate the order of G with $\text{ord}(G) = (p_1 - 1)p_1^{e_1 - 1}(p_2 - 1)p_2^{e_2 - 1} \dots (p_k - 1)p_k^{e_k - 1}$, which we then also factor into $\text{ord}(G) = q_1^{f_1} q_2^{f_2} \dots q_l^{f_l}$. We can now reduce each of the exponents to find the least divisor d which has $x^d = 1$. This is then the order.