

Q2a: By Lemma 5.1, we have that there will be $\phi(n)$ elements a of $\mathbb{Z}/n\mathbb{Z}$ such that $\text{ord}_G(a) = n$, since the ϕ function counts how many numbers less than n are coprime with n .

Q2b: By the Chinese remainder theorem, there exists an isomorphism ψ from $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/mn\mathbb{Z}$. By similar reasoning as above, there will be $\phi(mn)$ elements of $\mathbb{Z}/mn\mathbb{Z}$ with order mn . Since ψ is an isomorphism, there will also be $\phi(mn)$ elements in $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with order mn given by mapping $a \mapsto \psi^{-1}(a)$.

Q2c: We know from basic results about group theory that $\text{ord}_G(a) \leq |G|$. Since $|G| = \phi(n)$, it suffices to show that $\text{ord}_G(a)$ is never equal to $\phi(n)$. Suppose that for some element, a , $\text{ord}_G(a) = \phi(n) = (q-1)(p-1)$. This implies that

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq} \iff a^{p-1} \equiv 1 \pmod{q} \text{ and } a^{q-1} \equiv 1 \pmod{p}$$

By CRT + FLT this implies that $a \equiv 1 \pmod{pq}$. However the order of 1 is 1. A contradiction. Thus no element has an order of $\phi(n)$.