zad. 4a

Założenia: $ord(g) = n$, $k \in \mathbb{Z}$

Dowód. Bez straty ogólności, zakładamy $k < n$ ponieważ w przeciwnym przypadku:

$$ord(g^k) = ord(g^{pn+k'}) = ord(g^{pn}g^{k'}) = ord(g^{k'})$$

Dla $p, k \in \mathbb{N}$ oraz $k' < k$.

Zgodnie z definicją rzędu musimy pokazać, że $\frac{n}{NWD(n,k)}$ spelnia dwa warunki:

Warunek 1

$(g^k)^{\frac{n}{NWD(n,k)}} = e$

Dowód.

$$(g^k)^{\frac{n}{NWD(n,k)}} = (g^n)^{\frac{k}{NWD(n,k)}} = e^{\frac{k}{NWD(n,k)}} = e$$

□

Warunek 2

$\frac{n}{NWD(n,k)}$ jest dolnym ograniczeniem dla liczb m takich, że $(g^k)^m = e$.

Dowód. Weźmy dowolne $m \in \mathbb{Z}$ takie, że $(g^k)^m = e$.
Skoro $g^n = g^{km} = e$ oraz $n = ord(g)$ to:

$$n \mid km$$

$$\frac{n}{NWD(n,k)} \mid \frac{k}{NWD(n,k)}m$$

$$\frac{n}{NWD(n,k)} \mid m$$

$$\frac{n}{NWD(n,k)} \leqslant m$$

□

Wobec powyższego: $ord(g^k) = \frac{n}{NWD(n,k)}$ □