

Exercises

- Let $n = 12$. Determine $\text{ord}_n(a)$ for each a in the complete reduced residue system modulo n .
- Review the proof for the theorem: If $\gcd(a, n) = 1$ with $n > 0$, the positive integer x is a solution the congruence $a^x \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid x$.
- Review the proof for the theorem: If $\gcd(a, n) = 1$ with $n > 0$, then

$$a^i \equiv a^j \pmod{n}$$

if and only if

$$i \equiv j \pmod{\text{ord}_n(a)}.$$