

Math 342 Tutorial

June 25, 2025

Question 1. Show that if \bar{a} is an inverse of a modulo n , then $\text{ord}_n \bar{a} = \text{ord}_n a$.

Question 2. Assume that $(a, n) = 1 = (b, n)$. Do the following. **(a)** If $(\text{ord}_n a = \text{ord}_n b) = 1$, then $\text{ord}_n ab = \text{ord}_n a \cdot \text{ord}_n b$. **(b)** If we do not assume $(\text{ord}_n a = \text{ord}_n b) = 1$, then what can be said about $\text{ord}_n ab$.

Question 3. **(a)** Suppose $d \mid \phi(n)$. Is it true that there is an integer a for which $\text{ord}_n a = d$. **(b)** Show that if $(a, n) = 1$ and $\text{ord}_n a = st$, then $\text{ord}_n a^t = s$. **(c)** Show that if $(a, n) = 1$ and $\text{ord}_n a = n - 1$, then n is prime.

Question 4. Show that r is a primitive root modulo the prime p if and only if r is an integer with $(r, p) = 1$ such that

$$r^{(p-1)/q} \not\equiv 1 \pmod{p}$$

for every prime divisor q of $p - 1$.

Question 5. Let $m = a^n - 1$. Show the following. **(a)** $\text{ord}_{ma} = n$, and **(b)** $n \mid \phi(m)$.

Question 6. Let p be a prime, and let $\phi(p - 1) = q_1^{e_1} \cdots q_k^{e_k}$ where each q_i is prime. **(a)** Show there are integers a_1, \dots, a_k such that $\text{ord}_p a_i = q_i^{e_i}$ for each $i = 1, \dots, k$. **(b)** Show that $a = a_1 \cdots a_k$ is a primitive root modulo p . **(c)** Follow the procedure outlined above to show find a primitive root modulo 29.

Question 7. Show that if p is an odd prime then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod{8}, \\ -1 & \text{if } p \equiv -1, -3 \pmod{8}. \end{cases}$$

Question 8. Determine those primes p for which $(-3 \mid p) = -1$ and those primes q for which $(-3 \mid q) = 1$.

Question 9. Prove that 5 is a quadratic residue of an odd prime p if $p \equiv \pm 1 \pmod{10}$, and that 5 is a non residue if $p \equiv \pm 3 \pmod{10}$.