

Math 255 - Spring 2022
The order of a modulo n
10 points

This homework invites you to provide two proofs having to do with the order of a modulo n .

1. Let p be an odd prime. Show that if a has order 3 modulo p , then $a + 1$ has order 6 modulo p .

Hint: You may use the following result without proof: If $a \not\equiv 1 \pmod{p}$ and a has order t modulo p , then

$$a^{t-1} + a^{t-2} + \dots + a + 1 \equiv 0 \pmod{p}.$$

2. Prove that if a has order $n - 1$ modulo n , then n is a prime.