

Name:

Problem 1: *Is 2 a primitive root modulo 11?*

For full credit, justify your answer.

Solution: A primitive root modulo m is an integer a with $(a, m) = 1$ such that the order of a is $\phi(m)$.

Here we have that $(2, 11) = 1$ and $\phi(11) = 10$, so the question is simply whether or not the order of 2 modulo 11 is 10 or something smaller.

We note that to compute the order of a number a modulo m , it suffices to check if $a^d \equiv 1 \pmod{m}$ for each divisor d of $\phi(m)$, starting with the smallest divisor. The first time we do get $a^d \equiv 1 \pmod{m}$ is the order of a modulo m . (This is because the order of a number will always divide $\phi(m)$, so we can cut down on our computations a little bit.)

The divisors of $\phi(11) = 10$ are 1, 2, 5 and 10. We know that $2^1 \not\equiv 1 \pmod{11}$, so 2 does not have order 1.

We have that $2^2 \equiv 4 \not\equiv 1 \pmod{11}$, so 2 does not have order 2 modulo 11.

We also have

$$\begin{aligned} 2^5 &\equiv 2^2 \cdot 2^2 \cdot 2 \pmod{11} \\ &\equiv 4 \cdot 4 \cdot 2 \pmod{11} \\ &\equiv 16 \cdot 2 \pmod{11} \\ &\equiv 5 \cdot 2 \pmod{11} \\ &\equiv 10 \not\equiv 1 \pmod{11}. \end{aligned}$$

Therefore 2 does not have order 5 modulo 11.

It follows that 2 must have order 10 modulo 11 (and we can check this: $2^{10} \equiv (2^5)^2 \equiv 10^2 \equiv (-1)^2 \equiv 1 \pmod{11}$), and therefore, **yes**, 2 is a primitive root modulo 11.