Exercise 1. Is 91 prime? Justify your answer.

Solution 1. No: $91 = 7 \times 13$, so it is not prime.

Exercise 2. This exercise has multiple sub-questions about modular arithmetic.

2.1 Compute $2^{10} \bmod 11$.

2.2 State Fermat's little theorem and explain why your answer to the previous question is consistent with it.

These ideas are the foundation of several primality tests used in modern cryptography.

2.3 Does the converse of Fermat's little theorem hold, i.e. if $a^{p-1} \equiv 1 \pmod{p}$ for some a, must p be prime?

Solution 2. Fermat's little theorem is a cheap first filter for primality: it never wrongly rejects a prime, but it can be fooled by certain composite numbers (Carmichael numbers), which is why the converse fails and why real primality tests use several independent bases.

2.1 By Fermat's little theorem, $2^{10} \equiv 1 \pmod{11}$ since 11 is prime and $\gcd(2, 11) = 1$.

2.2 Fermat's little theorem states that if p is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. Since 11 is prime, this predicts exactly the result computed above.

2.3 No. A composite number p for which $a^{p-1} \equiv 1 \pmod{p}$ holds for some (or even every) a coprime to p is called a pseudoprime (or, if it holds for every valid a, a Carmichael number) – for example $341 = 11 \times 31$ satisfies $2^{340} \equiv 1 \pmod{341}$ despite being composite.