Introduction to mathematical cryptography
Homework problems
Week 9

17. Use the Miller-Rabin test to check that 11 is a prime.

18. Let p be an odd prime. Prove the polynomial congruence (with variable X)

$$X^{p-1} - 1 \equiv (X-1) \cdot \ldots \cdot (X-(p-1)) \qquad \bmod p.$$

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.