

SI 7: Modular Arithmetic

1. Prove or disprove the following statement: $\forall n \in \mathbb{N}, \quad n^2 - 79n + 1601$ is prime.
2. Recall Euclid's algorithm for the gcd:

$$\begin{aligned}\gcd(0, n) &= n \\ \gcd(m, n) &= \gcd(n \% m, m)\end{aligned}$$

Prove the correctness of Euclid's algorithm (prove that it is guaranteed to find the correct result).

3. Prove that $\forall n, m \in \mathbb{N}$:

$$n \cdot m = \gcd(n, m) \cdot \text{lcm}(m, n)$$