Computational Number Theory
Quiz 4

Date: 01/11/2025

1. Let p be an odd prime. Consider a binary operation $*$ defined on $S = \mathbb{Z}_p - \{1\}$ defined as: $a * b = a + b - ab$. Show that $(S, *)$ is a group.
2. Decide whether each of the following rings is a field or not.
   (a) $\mathbb{Z}_{11}[x]/(x^2 + 4)$
   (b) $\mathbb{R}[x]/(x^5 - 2)$
3. Let $M = \begin{bmatrix} 10 & 11 \\ 7 & 3 \end{bmatrix}$. Find M^{2025}, with arithmetic in $\mathbb{Z}_{47}$.
4. Let $n \equiv 1 \pmod 5$. Suppose that $x^{n-1} \not\equiv 1$ in $\mathbb{Z}_n[x]$. Show that n is composite.