

9 Modular Arithmetic (Continued)

Problem 9.1 Let $a, n \in \mathbb{N}$, $n > 1$ be relatively prime. Prove that $[a]_n$ has a *multiplicative inverse* in \mathbb{Z}/n , i.e., there exist $b \in \mathbb{Z}$ such that $[a]_n[b]_n = [1]_n$.

Problem 9.2 Let $n \in \mathbb{N}$, $n > 1$. Let $x \in \mathbb{Z}/n$. Prove that multiplicative inverse of x in \mathbb{Z}/n (if exists) is unique, i.e., if for $y, z \in \mathbb{Z}/n$ we have $xy = [1]_n$ and $xz = [1]_n$ then $y = z$.

Notation 9.1 Denote the multiplicative inverse of x by x^{-1} .

Problem 9.3 Find all invertible elements of $\mathbb{Z}/10$ and their inverses.

Problem 9.4 Let p be a prime. Find all invertible elements of \mathbb{Z}/p .

Problem 9.5 Let $n \in \mathbb{N}$, $n > 1$ and $a, b \in \mathbb{Z}/n$. Suppose a is invertible. Prove that the equation $ax = b$ has a unique solution $x \in \mathbb{Z}/n$.

Problem 9.6 Show that the condition “ a is invertible” in the previous problem is necessary.

Problem 9.7 Let $n \in \mathbb{N}$, $n > 1$ and $a, b, c, d \in \mathbb{Z}/n$. Suppose a is invertible. Prove that if $ab = ac$ then $b = c$, i.e., we can cancel an invertible element on both sides of a formula.

Problem 9.8 Show that the condition “ a is invertible” in the previous problem is necessary.