Homework 2

MATH 301

Solution to graded problem

Exercise 7. Let $n \in \mathbb{N}$. Prove that given any $m \in \mathbb{Z}$, there exists a unique element $a \in \{0, 1, 2, \ldots, n-1\}$ such that $m = a \pmod{n}$.

Proof. Let $m \in \mathbb{Z}$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < n$. From this, we can write $m - r = qn$, which implies that $q \mid (m - r)$. Hence, by the definition of equivalence modulo n, we have $m = r \pmod{n}$. Setting $a = r$ establishes the existence of $a \in \{0, 1, 2, \ldots, n-1\}$ such that $m = a \pmod{n}$. It is left to show that a is unique. Suppose $b \in \{0, 1, 2, \ldots, n-1\}$ and $a = b \pmod{n}$. Observe that $|a - b| \in \{0, 1, 2, \ldots, n-1\}$ and that $n \mid |a - b|$ by Exercise 4. The only element of $\{0, 1, 2, \ldots, n-1\}$ divisible by n is 0; therefore, $|a - b| = 0$ and $b = a$, which establishes the uniqueness of a. $\square$