Homework 3

MATH 301

Solutions to graded problem

***Exercise 3.** 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 $m \equiv a \pmod{n}$.

Solution. Let $m \in \mathbb{Z}$. By the division algorithm, there exists unique $q, a \in \mathbb{Z}$ such that $m = qn + a$ and $a \in \{0, 1, \ldots, n-1\}$. Rearranging the above equality, we have that $m - a = qn$, and hence $n \mid m - a$. This implies that $m \equiv a \pmod{n}$ and $a \in \{0, 1, \ldots, n-1\}$, as desired. It is left to show that a is unique: let $a' \in \{0, 1, \ldots, n-1\}$ such that $m \equiv a'$ (mod n). Similar to the above (but in reverse), there exists $q' \in \mathbb{Z}$ such that $m = q'n + a'$. As $0 \leq a' < n$, the uniqueness component of the division algorithm implies that $a' = a$. Therefore, there exists a unique $a \in \{0, \ldots, n-1\}$ such that $m \equiv a \pmod{n}$. $\square$

****Exercise 6.** Let $m, n \in \mathbb{N}$ be relatively prime, and let $a, b \in \mathbb{Z}$. Prove that there exists $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

(Hint: Start by writing 1 as a linear combination of m and n.)

Solution. As m and n are relatively prime, there exists $s, t \in \mathbb{Z}$ such that $1 = ms + nt$. From this, we see that $1 - ms = nt$ and $1 - nt = ms$, and hence, $ms \equiv 1 \pmod{n}$ and $nt \equiv 1 \pmod{m}$. Setting $x = bms + ant$, we have

$$x \equiv 0 + ant \equiv a(1) \equiv a \pmod{m}$$

and

$$x \equiv bms + 0 \equiv b(1) \equiv b \pmod{n}.$$

Therefore, x is as desired. $\square$