Homework Set 3
(Problems from Chapter 2)

Problems from §2.1

2.1.1. Prove that $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.

2.1.2. If $a \in \mathbb{Z}$, prove that a^2 is not congruent to 2 modulo 4 or to 3 modulo 4.

2.1.3. If a, b are integers such that $a \equiv b \pmod{p}$ for every positive prime p, prove that $a = b$.

2.1.4. Which of the following congruences have solutions:
(a) $x^2 \equiv 1 \pmod{3}$
(b) $x^2 \equiv 2 \pmod{7}$
(c) $x^2 \equiv 3 \pmod{11}$

2.1.5. If $[a] = [b]$ in $\mathbb{Z}_n$, prove that $GCD(a, n) = GCD(b, n)$.

2.1.6. If $GCD(a, n) = 1$, prove that there is an integer b such that $ab = 1 \pmod{n}$.

2.1.7. Prove that if $p \geq 5$ and p is prime, then either $[p]_6 = [1]_6$ or $[p]_6 = [5]_6$.

Problems from §2.2

2.2.1. Write out the addition and multiplication tables for $\mathbb{Z}_4$.

2.2.2. Prove or disprove: If $ab = 0$ in $\mathbb{Z}_n$, then $a = 0$ or $b = 0$.

2.2.3. Prove that if p is prime then the only solutions of $x^2 + x = 0$ in $\mathbb{Z}_p$ are 0 and $p - 1$.

2.2.4. Find all a in $\mathbb{Z}_5$ for which the equation $ax = 1$ has a solution.

2.2.5. Prove that there is no ordering $\prec$ of $\mathbb{Z}_n$ such that

$$\begin{array}{ll} (i) & \text{if } a \prec b, \text{ and } b \prec c, \text{ then } a \prec c; \\ (ii) & \text{if } a \prec b, \text{ then } a + c \prec b + c \text{ for every } c \in \mathbb{Z}_n \quad . \end{array}$$

Problems from §2.3

2.3.1 If n is composite, prove that there exists $a, b \in \mathbb{Z}_n$ such that $a \neq [0]$ and $b \neq [0]$ but $ab = [0]$.

2.3.2 Let p be prime and assume that $a \neq 0$ in $\mathbb{Z}_p$. Prove that for any $b \in \mathbb{Z}_p$, the equation $ax = b$ has a solution.

2.3.3. Let $a \neq [0]$ in $\mathbb{Z}_n$. Prove that $ax = [0]$ has a nonzero solution in $\mathbb{Z}_n$ if and only if $ax = [1]$ has no solution.

2.3.4. Solve the following equations.
(a) $12x = 2$ in $\mathbb{Z}_{19}$.
(b) $7x = 2$ in $\mathbb{Z}_{24}$.
(c) $31x = 1$ in $\mathbb{Z}_{50}$.
(d) $34x = 1$ in $\mathbb{Z}_{97}$.