Hints to 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.

- $\Longrightarrow$ By Division Algorithm $a = nq_1 + r_1$ with $0 \leq r_1 < n$, and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. By hypothesis
$$kn = a - b = (q_1 - q_2)\, n - r_1 - r_2 \quad \Longrightarrow \quad r_1 - r_2 = n\,(k - q_1 + q_2)$$
$$\Longrightarrow \quad n \text{ divides } (r_1 - r_2) \quad \Longrightarrow r_1 - r_2 = 0 \quad \text{because } 0 \leq \ |r_1 - r_2| < n$$
- $\Longleftarrow$ easy (just apply Div. Alg. as above using the hypothesis $r_1 = r_2$)

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

- Try case by case analysis

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

- Choose a prime $p > |a - b|$ Then
$$a \equiv b \pmod{p} \quad \Longrightarrow \quad p|\,(a - b) \quad \Longrightarrow \quad a - b = 0 \quad \text{since } 0 \leq |a - b| < p$$

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

- case by case analysis
  (b) $x^2 \equiv 2 \pmod{7}$
  (c) $x^2 \equiv 3 \pmod{11}$

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

- If $[a]_n = [b_n]$ then
$$a \equiv b \pmod{n} \quad \Longrightarrow \quad a - b = kn \quad \Longrightarrow \quad a = kn + b$$
So any integer that divides both b and n divides a. Similary, $b = a - kn$ implies any integer dividing a and b divides b
$$\begin{aligned} GCD\,(a, n) &= \max\{\text{common divisors of } a \text{ and } n\ \} \\ &= \max\{\text{comnom divisors of } b \text{ and } n\} = CGD\,(b, n) \end{aligned}$$

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

- Proved in class

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 $b = 0$.

- Find a counter-example

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

$$[0]_p = x(x+1)$$

Now apply Theorem 2.8(3), to conclude either $x = [0]_p$ or $x + [1]_p = [0]_p$

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

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

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 $ab = [0]$.

- If n is composite, $n = ab$ with $1 < a, b < n$. But then $[a]_n \neq [0]_n$, $[b]_n \neq [0]_n$ but $[a]_n [b]_n = [ab]_n = [n]_n = [0]_n$.

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.

- By Theorem 2.8 (2), there is a solution $[c]_p$ of $[a]_p x = [1]_p$. Multiply both sides of $[a]_p [c]_p = [1]_p$ by $[b]_p$ to see that $[c]_p [b]_p$ is a solution of $[a]_p x = [b]_p$.

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

- $\Longrightarrow$ Let $[c]_n$ be a non-zero solution of $[a]_n x = [0]_n$. and let $[b]_n$ be a solution of $[1]_n = [a]_n x$. Multiply the last equation by $[c]_n$
$$[c]_n = [c]_n [1]_n = [c]_n ([a]_n [b]_n) = ([c]_n [a]_n) [b]_n = [0]_n [b]_n = [0]_n$$
which is a contradiction with the hypothesis.
$\Longleftarrow$ Similiar.

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 $\mathbb{Z}_{97}$.