Section 1.4, Problem 7:
Prove that the associative and commutative laws hold for addition and multiplication of congruence classes, as defined in Proposition 1.4.2.

Solution:
Addition: we know that associativity and commutativity hold for integer addition. Thus we have the following.
Associativity: \((a_n + b_n) + c_n = [a + b]_n + [c]_n = [(a + b) + c]_n = [a + (b + c)]_n = [a]_n + [b + c]_n = [a]_n + ([b]_n + [c]_n).
Commutativity: \([a]_n + [b]_n = [a + b]_n = [b + a]_n = [b]_n + [a]_n.

Similarly for multiplication.

Section 1.4, Problem 24:
Show that if \(p\) is a prime number, then the congruence \(x^2 \equiv 1 \pmod{p}\) has only the solutions \(x \equiv 1\) and \(x \equiv -1\).

Solution:
The congruence \(x^2 \equiv 1 \pmod{p}\) is equivalent to \(x^2 - 1 \equiv 0 \pmod{p}\).
Factor \(x^2 - 1\): \((x - 1)(x + 1) \equiv 0 \pmod{p}\).
Therefore \(p|(x - 1)(x + 1)\). Since \(p\) is prime, by Euclid’s Lemma \(p|(x - 1)\) or \(p|(x + 1)\).
If \(p|(x - 1)\), then \(x \equiv 1 \pmod{p}\).
If \(p|(x + 1)\), then \(x \equiv -1 \pmod{p}\).
Section 1.4, Problem 27:

Prove Wilson’s theorem, which states that if $p$ is a prime number, then $(p - 1)! \equiv -1 \pmod{p}$.

Hint: $(p - 1)!$ is the product of all elements of $\mathbb{Z}_p^\ast$. Pair each element with its inverse, and use Exercise 24. For three special cases see Exercise 11 in Section 1.3.

Solution:

Since $p$ is prime, every positive integer less than $p$ is relatively prime to $p$. Therefore every element of $\mathbb{Z}_p^\ast$ has an inverse in $\mathbb{Z}_p$. Let $[y]_p$ be the inverse of $[x]_p$. Then $[x]_p[y]_p = [1]_p$ implies that $[xy]_p = [1]_p$, or $xy \equiv 1 \pmod{p}$. By exercise 24, the only solutions of $x^2 \equiv 1 \pmod{p}$ are $x \equiv 1$ and $x \equiv -1$, thus only the elements $[1]$ and $[-1] = [p - 1]$ are inverses of themselves, and if $x \not\equiv 1$ or $-1$, then the inverse of $[x]$ is not equal to $[x]$. Therefore all elements of $\mathbb{Z}_p^\ast$ except for $[1]$ and $[p - 1]$ can be divided into $\frac{p - 3}{2}$ pairs of the form $([x], [x]^{-1})$. The product of the two classes in each pair is $[1]$, thus $(p - 1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p - 1) \equiv 1 \cdot 1 \cdot \ldots \cdot 1 \cdot (p - 1) \equiv -1 \pmod{p}$.

Section 2.1, Problem 9(b):

Show that each of the following formulas yields a well-defined function.

$g : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ defined by $g([x]_8) = [6x]_{12}$.

Solution:

If $[x_1]_8 = [x_2]_8$, then $x_1 \equiv x_2 \pmod{8}$, so $x_1 - x_2 = 8k$ for some $k \in \mathbb{Z}$. Then $6x_1 - 6x_2 = 48k = 12(4k)$. It follows that $6x_1 \equiv 6x_2 \pmod{12}$, i.e. $[6x_1]_{12} = [6x_2]_{12}$. Thus $g$ is well-defined.

Section 2.1, Problem 10(b):

In each of the following cases, give an example to show that the formula does not define a function.

$g : \mathbb{Z}_2 \to \mathbb{Z}_5$ defined by $g([x]_2) = [x]_5$.

Solution:

Since $[0]_2 = [2]_2$, we must have $g([0]_2) = g([2]_2)$. However, $g([0]_2) = [0]_5 \neq [2]_5 = g([2]_2)$. Thus $g$ is not well-defined.