Math 412. Adventure sheet on §2.2 and §2.3: Arithmetic in $\mathbb{Z}_N$

DEFINITION: For a positive integer N, $\mathbb{Z}_N$ is the set of congruence classes of integers modulo N.

A. RECAP FROM LAST TIME:

(1) What are the elements of $\mathbb{Z}_3$? What are the elements of the elements of $\mathbb{Z}_3$?[1]
(2) How many elements are in $\mathbb{Z}_N$ in general? Why?
(3) Given two elements $[x]$ and $[y]$ in $\mathbb{Z}_N$, we came up for a rule for adding $[x]$ and $[y]$ to get another element in $\mathbb{Z}_N$. In the book this was denoted $[x] \oplus [y]$ in §2.2 and then denoted $[x] + [y]$ in §2.3.
(4) Compute $[120] + [13]$ and $[-19] + [23]$ in $\mathbb{Z}_6$.
(5) What is the general rule for $[x] + [y]$ in $\mathbb{Z}_N$? Why was this rule "easier said than done"? That is, what was crucial to check when posing this definition?
(6) Given two elements $[x]$ and $[y]$ in $\mathbb{Z}_N$, we came up for a rule for multiplying $[x]$ and $[y]$ to get another element in $\mathbb{Z}_N$. In the book this was denoted $[x] \odot [y]$ in §2.2 and then denoted $[x] \cdot [y]$ or $[x][y]$ in §2.3.
(7) Compute $[120] \cdot [13]$ and $[-19] \cdot [23]$ in $\mathbb{Z}_6$.
(8) What is the general rule for $[x] \cdot [y]$ in $\mathbb{Z}_N$? Why was this rule "easier said than done"? That is, what was crucial to check when posing this definition?
(9) Come up with a general rule for $[x] - [y]$ in $\mathbb{Z}_N$. Why is it well-defined?

B. BASIC PROPERTIES OF ADDITION AND MULTIPLICATION IN $\mathbb{Z}_N$: Addition and multiplication in $\mathbb{Z}_N$ behave a lot like they do in $\mathbb{Z}$.

(1) Show that $[a]_N \cdot [b]_N = [b]_N \cdot [a]_N$ for every $a, b \in \mathbb{Z}$. In other words, prove that multiplication is commutative.
(2) Show that $[a]_N \cdot ([b]_N + [c]_N) = [a]_N \cdot [b]_N + [a]_N \cdot [c]_N$ for every $a, b, c \in \mathbb{Z}$.
(3) Can you guess what some of the other properties might be? We will prove them next time.

C. SOLVING EQUATIONS IN $\mathbb{Z}_N$:

(1) Rewrite the equation $[a]x = [b]$ in $\mathbb{Z}_N$ as a congruence ($\equiv$) equation involving integers.[2] What is the relationship between a solution of the congruence equation and the original equation in $\mathbb{Z}_N$?
(2) Rewrite the equation $[a]x = [b]$ in $\mathbb{Z}_N$ as a statement involving division ($|$) of integers. What is the relationship between a solution of the division statement and the original equation in $\mathbb{Z}_N$?
(3) Show that if $(a, N) = 1$, then $[a]x = [1]$ has a solution in $\mathbb{Z}_N$.
(4) Based on the previous part, what technique would you use to solve $[a]x = [1]$?
(5) For more complicated equations, things are a bit harder. Solve the equation $[2]x^2 - [5] = [0]$ in $\mathbb{Z}_9$ by plugging in values.

D. SOLVING $[a]x = [b]$ IN $\mathbb{Z}_p$ WHEN p IS PRIME:

(1) Prove that if p is prime and $[a] \neq [0]$, then $[a]x = [1]$ always has a solution in $\mathbb{Z}_p$.
(2) Prove that if p is prime and $[a] \neq [0]$, then $[a]x = [0]$ implies $x = [0]$ in $\mathbb{Z}_p$.
(3) Prove that if p is prime and $[a] \neq [0]$, then $[a]x = [1]$ always has a *unique* solution in $\mathbb{Z}_p$.
(4) Prove that if p is prime and $[a] \neq [0]$, then $[a]x = [b]$ always has a *unique* solution in $\mathbb{Z}_p$.

E. SOLVING $[a]x = [b]$ IN $\mathbb{Z}_N$ WHEN N IS NOT PRIME:

(1) Solve $[9]x = [3]$, $[3]x = [1]$, and $[9]x = [4]$ in $\mathbb{Z}_{12}$.
(2) Let a and n be two integers, not both zero. Prove that $\{ra + sn \mid r, s \in \mathbb{Z}\} = \{k(a, n) \mid k \in \mathbb{Z}\}$.
(3) When does $[a]x = [b]$ have a solution in $\mathbb{Z}_N$? When does it have multiple solutions?

---

[1] This is not a riddle!

[2] where x is an unknown element of $\mathbb{Z}_N$!