Math 412. §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.

Part 1: Getting acquainted.

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) *Recall:* 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.
Question: Compute $[120] + [13]$ and $[-19] + [23]$ in $\mathbb{Z}_6$.

(4) What is the general rule for $[x] + [y]$ in $\mathbb{Z}_N$? Why is this rule well defined?

(5) *Recall:* 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.
Question: Compute $[120] \cdot [13]$ and $[-19] \cdot [23]$ in $\mathbb{Z}_6$. (There's a way to do this without a calculator and without much work)

(6) What is the general rule for $[x] \cdot [y]$ in $\mathbb{Z}_N$? Why is this rule well defined?

(7) Come up with a general rule for $[x] - [y]$ in $\mathbb{Z}_N$. Why is it well-defined?

Solution.

(1) The elements of $\mathbb{Z}_3$ are $[0]_3$, $[1]_3$ and $[2]_3$. The element $[0]_3$ is the class of all integers that are divisible by 3. The other two elements $[1]_3$ are the classes of all integers of the form $3q + 1$ and $3q + 2$, where q is any integer.

(2) $\mathbb{Z}_n$ has n elements: $[0]_n, [1]_n, \ldots, [n-1]_n$.

(3) $[120] + [13] = [133]$ and $[-19] + [23] = [4]$.

(4) $[x] + [y] = [x + y]$, but we had to check that this was *well-defined*! We have seen[2] examples of "rules" that don't actually work. Remember that some possible rules turn out to not depend only on the input but also depend on how we write it, which is bad. A good rule is one that does not change when we change the way we write the input. In this particular case, we had to see that if we chose different representatives for the class of $[x]$ and $[y]$, the answer would still be the same. For example, $[5]_2 + [3]_2 = [8]_2 = [1]_2 + [1]_2$.

[1] This is not a riddle!

(5) $[120] \cdot [13] = [0]$ and $[-19] \cdot [23] = [-23]$.

(6) See (4).

(7) $[x] - [y] = [x - y]$. We can directly prove that this is well-defined as follows: if $[x] = [x']$ and $[y] = [y']$, then $n|(x - x')$ and $n|(y - y')$, so

$$n|(x - x') - (y - y') = (x - y) - (x' - y').$$

This means $[x - y] = [x' - y']$.

Another approach would be to define the expression $[x] - [y]$ to mean $[x] + [-1][y]$. Then we would know this is operation is well-defined, as addition and multiplication of equivalence classes are well-defined, and we would have a to do a little work to show that $[x] - [y] = [x - y]$.

B. COMMON SENSE PROPERTIES 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.

Solution.

(1) $[a]_N \cdot [b]_N = [a \cdot b]_N = [b \cdot a]_N = [b]_N \cdot [a]_N$, where we used that the multiplication of integers is commutative.

(2) $[a]_N \cdot ([b]_N + [c]_N) = [a]_N[b + c]_N = [a(b + c]_N = [ab + ac]_N = [a]_N[b]_N + [a]_N[c]_N$, where we used the same property holds for any integers a, b, c.

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.[3] 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.

(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.

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

Solution.

(1) $ay \equiv b \mod N$ where $[y]_N = x$. If $y \in \mathbb{Z}$ is a solution to the congruence equation, then $x = [y]$ is a solution to the original equation in $\mathbb{Z}_N$.

(2) $N|(ay - b)$ where $[y]_N = x$. If $y \in \mathbb{Z}$ is a solution to the congruence equation, then $x = [y]$ is a solution to the original equation in $\mathbb{Z}_N$.

(3) If $(a, N) = 1$, there exist $u, v \in \mathbb{Z}$ such that $au + Nv = 1$, so $N|(1 - au)$. Then $[a]_N \cdot [u]_N = [1]_N$.

(4) We would use the Euclidean algorithm to find the integers u and v such that $au + Nv = 1$.

(5) $x = [4], [5]$.

Part 2: Going deeper (helpful for Webwork).

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 $\mathbb{Z}_p$.

Solution.

(1) If p is prime and $[a]_p \neq [0]_p$, then $p \nmid a$. The only positive divisors of p and 1 and p, so $(a, p) = 1$. We then apply C. (2).

(2) If $[a]x = [0]$, and $y \in x$, then $p|ay$. Since p is prime and $p \nmid a$, $p|y$. That is, $x = [y] = [0]$.

(3) We already proved that there exists a solution. To see uniqueness, assume $[a] \neq [0]$, and suppose $[a]x_1 = [a]x_2 = [1]$. Then $[a](x_1 - x_2) = [0]$. By the previous part, $x_1 - x_2 = [0]$, so $x_1 = x_2$.

(4) For existence, take some x such that $[a]x = [1]$. Then $[a]([b]x) = [b]$. For uniqueness, assume $[a] \neq [0]$, and suppose $[a]x_1 = [a]x_2 = [b]$. Then, $[a](x_1 - x_2) = [0]$, so $x_1 - x_2 = [0]$ as above.

E. Solving $[a]x = [b]$ in $\mathbb{Z}_N$ when N is not prime:

(1) Solve, if possible: $[9]x = [3]$, $[3]x = [1]$, and $[9]x = [4]$ in $\mathbb{Z}_{12}$.

(2) Let a and n be two integers, not both zero. Prove that $\{ra + sn \mid r, s \in \mathbb{Z}\} = \{k \cdot (a, n) \mid k \in \mathbb{Z}\}$.

(3) When does $[a]x = [b]$ have a solution in $\mathbb{Z}_N$? When does it have multiple solutions?

Solution.

(1) For $[9]x = [3]$, the solution set is $\{[3], [7], [11]\}$. For the others, there are no solutions!

(2) Write $P = \{ra + sn \mid r, s \in \mathbb{Z}\}$ and $Q = \{k \cdot (a, n) \mid k \in \mathbb{Z}\}$. We will show that $P \subseteq Q$ and $Q \subseteq P$, which proves that $P = Q$.
$Q \subseteq P$: By Theorem 1.2, we know that $(a, n) = au + nv$ for some $u, v \in \mathbb{Z}$, which shows that $(a, n) \in P$. Taking $r = ku$ and $s = kv$, we get $ra + sb = k(a, n)$, so $k(a, n) \in P$.
$P \subseteq Q$: Fix some $r, s \in \mathbb{Z}$. Since $(a, n)|a$ and $(a, n)|n$, $(a, n)|ra + sn$. Then there exists some $k \in \mathbb{Z}$ such that $k(a, n) = ra + sb$.

(3) By the previous part, there exist some integers $r, s \in \mathbb{Z}$ such that $b = ra+sN$ if and only if $(a, N)|b$. In other words, N divides $b - ra$ for some r if and only if $(a, N)|b$, which characterizes when we can solve $[a]x = [b]$. If $(a, N) \neq 1$, we can find some $d \in \mathbb{Z}$ such that $d \cdot (a, N) = N$. Then $[d] \neq [0]$, and $[a][d] = [0]$. Thus, if $[a]x = [b]$, then also $[a](x + [d]) = [0]$, so there are distict solutions.