Modern Algebra 1 Section 1 · Assignment 4

JOHN PERRY

Exercise 1. *(pg. 39 Warm Up b) Does* $\{47, 100, -3, 29, -9\}$ *contain a representative from every residue class of* $\mathbb{Z}_5$*? Does* $\{-14, -21, -10, -3, -2\}$*? Does* $\{10, 21, 32, 43, 54\}$*?*

Solution:
The first one does not; both 47 and -3 are in $[2]$. The second and third do. ◊

Exercise 2. *(pg. 39 Warm Up c) What is the additive inverse of* $[13]$ *in* $\mathbb{Z}_{28}$*?*

Solution:
$[15] + [13] = [0]$. ◊

Exercise 3. *(pg. 39 Warm Up d) What is the relationship between 'clock arithmetic' and modular arithmetic?*

Solution:
'Clock arithmetic' is a special case of modular arithmetic. It takes place in $\mathbb{Z}_{12}$. ◊

Exercise 4. *(pg. 39 Warm Up e) (a) What time is it 100 hours after 3 o'clock?*
(b) What day of the week is it 100 days after Monday?

Solution:
(a) There are twenty-four hours in a day, and $100 = 4 \cdot 24 + 4$. By adding four hours to 3 o'clock, we see that 100 hours after 3 o'clock is 7 o'clock.
(b) There are seven days in a week, and $100 = 14 \cdot 7 + 2$. Two days after Monday is Wednesday, so 100 days after Monday is Wednesday. ◊

Exercise 5. *(pg. 39 Warm Up f) Solve the following equations, or else argue that they have no solutions:*
(a) $[4] + X = [3]$, *in* $\mathbb{Z}_6$.
(b) $[4]X = [3]$, *in* $\mathbb{Z}_6$.
(c) $[4] + X = [3]$, *in* $\mathbb{Z}_9$.
(d) $[4]X = [3]$, *in* $\mathbb{Z}_9$.

Solution:
(a) Since $3 - 4 = -1$ and $[-1] = [5]$, $X = [5]$.
(b) No solution. The multiples of $[4]$ in $\mathbb{Z}_6$ are $[4]$, $[8] = [2]$, and $[12] = [0]$. All other multiples appear in those residue classes. *Better explanation:* $[4]X = [3]$ iff $[4X] = [3]$ iff (by Theorem 3.2) $4X - 3 = 6k$ for some $k \in \mathbb{Z}$ iff $4X - 6k = 3$ for some $k \in \mathbb{Z}$. By a previous exercise, 3 must be a multiple of the gcd of 4 and 6. Unfortunately, $\gcd(4,6) = 2$, and 3 is not a multiple of 2. Hence there is no solution to this equation.
(c) Since $3 - 4 = -1$ and $[-1] = [8]$, $X = 8$.
(d) Since $4 \times 3 = 12$ and $[12] = [3]$, $X = 3$. ◊

Exercise 6. *(pg. 39 Exercise 3) In Exercise c you determined the additive inverse of* $[13]$ *in* $\mathbb{Z}_{28}$*. Now determine its multiplicative inverse.*

Solution:

We need x such that $[13]\,x = [1]$. The multiples of $[13]$ are

$$[13],[26],[39]=[11],[24],[37]=[9],[22],[35]=[7],$$
$$[20],[33]=[5],[18],[31]=[3],[16],[29]=[1].$$

The thirteenth multiple is $[1]$. Thus $[13]$ is its own multiplicative inverse. ◊

Exercise 7. *(pg. 39 Exercise 4) Find an example in $\mathbb{Z}_6$ where $[a][b]=[a][c]$, but $[b]\neq[c]$. How is this example related to the existence of multiplicative inverses in $\mathbb{Z}_6$?*

Solution:

If $a=2$, $b=3$, and $c=6$, then $[a][b]=[a][c]=[0]$. This is related to multiplicative inverses because if $[a]$ had a multiplicative inverse, then we could multiply it to both sides of the equation and show that $[b]=[c]$. ◊

Exercise 8. *(pg. 40 Exercise 5) If $\gcd(a,m)=1$, then the GCD identity 2.4 guarantees that there exist integers u and v such that $1=au+mv$. Show that in this case, $[u]$ is the multiplicative inverse of $[a]$ in $\mathbb{Z}_m$.*

Solution:

Let $a,m\in\mathbb{Z}$ be arbitrary, but fixed. Assume that $\gcd(ab)=1$. Then there exist $u,v\in\mathbb{Z}$ such that

$$1 = au+mv$$
$$1-au = mv.$$

By Theorem 3.2 and the definition of modular multiplication, $[a][u]=[au]=[1]$, showing that $[u]$ is the multiplicative inverse of $[a]$ in $\mathbb{Z}_m$. ◊

Exercise 9. *(pg. 40 Exercise 6) Now use essentially the reverse of the argument from Exercise 5 to show that if $[a]$ has a multiplicative inverse in $\mathbb{Z}_m$, then $\gcd(a,m)=1$.*

Solution:

Let $a,m\in\mathbb{Z}$ be arbitrary, but fixed. Assume that $[a]$ has a multiplicative inverse in $\mathbb{Z}_m$. This means that there exists $[u]\in\mathbb{Z}_m$ such that $[au]=[a][u]=[1]$. By Theorem 3.2, $1-au=km$ for some $k\in\mathbb{Z}$. Thus

$$1 = au+km$$

for some $u,k\in\mathbb{Z}$. Thus 1 is a linear combination of a and m. Since no smaller positive integer exists, 1 is the smallest positive linear combination of a and m. By Corollary 2.5, $\gcd(a,m)=1$. ◊

Exercise 10. *(pg. 40 Exercise 7) According to what you have shown in Exercises 5 and 6, which elements of $\mathbb{Z}_{24}$ have multiplicative inverses? What are the inverses of each of those elements? (The answer is somewhat surprising.)*

Solution:

The elements that have multiplicative inverses are [1], [5], [7], [11], [13], [17], [19], and [23]. The "surprise" is that each invertible element is its own inverse. ◊

Exercise 11. *(pg. 40 Exercise 9) Prove that the multiplication on $\mathbb{Z}_m$ as defined in the text is well-defined, as claimed in Section 3.2.*

Solution:

Let $[a],[b] \in \mathbb{Z}_m$ be arbitrary, but fixed. By definition, $[a][b] = [ab]$. We must show that if $[x] = [a]$, then $[x][b] = [a][b]$. That is, the fact that a residue class has two different representations does not affect the product

Since $[x] = [a]$, Theorem 3.2 tells us that

$$x - a = km \tag{1}$$

for some $k \in \mathbb{Z}$. We want to show that $[x][b] = [a][b]$. It would suffice to show that $[xb] = [ab]$, since the definition of modular arithmetic would then imply $[x][b] = [a][b]$. We could apply Theorem 3.2 to get $[xb] = [ab]$ if we could find some integer j such that $xb - ab = jm$. Recalling equation (1),

$$\begin{aligned} x - a &= km \\ (x-a)b &= (km)b \\ xb - ab &= (kb)m. \end{aligned}$$

By closure, $kb \in \mathbb{Z}$. As hoped, Theorem 3.2 applies: $[x][b] = [xb] = [ab] = [a][b]$. ______$\Diamond$