

MAT 1362 – Fall 2019

Quiz 7 – DGD 1 (Tuesday) – Solutions

Professor: Alistair Savage

Date: November 5, 2019

QUESTION (3 points). For each of the following questions, write your answer in the standard form: $[0], [1], [2], \dots, [n-1]$, where n is the modulus. Remember to justify your answers.

- (a) Does $[5]$ have an additive inverse in \mathbb{Z}_{18} ? If so, what is it?

Solution: Yes, it does. Since

$$[5] \oplus [13] = [18] = [0],$$

the element $[13]$ is an additive inverse of $[5]$.

- (b) Does $[4]$ have a multiplicative inverse in \mathbb{Z}_9 ? If so, what is it?

Solution: Yes, it does. Since

$$[4] \odot [7] = [28] = [1],$$

the element $[7]$ is a multiplicative inverse of $[4]$.

- (c) Does $[4]$ have a multiplicative inverse in \mathbb{Z}_6 ? If so, what is it?

Solution: No, it does not. There are two ways to show this.

Brute force method: We can check all the possibilities:

$$\begin{aligned} [4] \odot [0] &= [0] \neq [1], & [4] \odot [1] &= [4] \neq [1], \\ [4] \odot [2] &= [8] = [2] \neq [1], & [4] \odot [3] &= [12] = [0] \neq [1], \\ [4] \odot [4] &= [16] = [4] \neq [1], & [4] \odot [5] &= [20] = [2] \neq [1]. \end{aligned}$$

Thus $[4]$ has no multiplicative inverse.

Contradiction: Note that $[4] \odot [3] = [0]$. If $[4]$ had a multiplicative inverse $[a]$, then we would have

$$[3] = [1] \odot [3] = [a] \odot [4] \odot [3] = [a] \odot [0] = [0].$$

But this is a contradiction, since $[3] \neq [0]$.