

ANSWERS FOR PROBLEM SET III

Section 6C, page 105.

8. (i) We seek to solve $[6]X = [4]$ in \mathbb{Z}_{10} . In other words, what multiples of 6 have the units digit of 4? Answer: $x = 4$ and $x = 9$ (or -1).

(v) We seek to solve $[13]X = [16]$ in \mathbb{Z}_{19} . 19 is prime, so we have a field. $3(13) - 2(19) = 1$, so the inverse of $[13]$ is $[3]$. $X = [13]^{-1}[16] = [3][16] = [48] = [10]$.

Section 6D, page 109.

33. We know that the p classes

$$[0], [b], [b^2], \dots, [b^{p-1}]$$

form a complete list of the p elements in \mathbb{Z}_p . Therefore there can be no duplication in this list. In particular, the class $[b]$ occurs only *once*.

The class $[1]$ must be somewhere in the list. The claim is that $[1]$ is the *last* item in the list. At least it is not the *first*.

We argue by contradiction. Suppose, to the contrary, $[1]$ occurred earlier. Then the *next* item in the list is $[b]$. But $[b]$ is also the second item, which contradicts the lack of duplication.

We conclude that $[1]$ must be last in the list.

Cf. Fermat's theorem, on page 175.

Section 6E, page 112.

44. In \mathbb{Z}_{12} , the units are $[1]$, $[5]$, $[7]$, and $[11]$. Each one is its own inverse.

As a consequence, we see that in \mathbb{Z}_{12} , the quadratic equation $x^2 = 1$ has *four* roots.

Section 6F, page 116.

60. 11 is prime, so we have a field. $2(6) - 11 = 1$, so $[6]^{-1}$ is $[2]$. $X = [6]^{-1}[3] = [2][3] = [6]$.

Section 7A, page 130.

6. We define (as at the top of page 130) $-x$ to be the unique y for which $x + y = 0_R$. Therefore to show that $t = -x$, it suffices to show that $x + t = 0_R$.

In particular, to show that $t = -(ab)$, it suffices to show that $ab + t = 0_R$. We want to do this when $t = (-a)b$ and when $t = a(-b)$.

Both of those are easy. (The hard part was seeing what is needed.)

15. \mathbb{Z}_6 has two units: $[1]$ and $[5]$. \mathbb{Z}_7 has six units: $[1]$, $[2]$, $[3]$, $[4]$, $[5]$, and $[6]$. \mathbb{Z}_8 has four units: $[1]$, $[3]$, $[7]$, and $[5]$.

Section 7C, page 138.

23. The trivial solution to $ax = 0$ is $x = 0$. When a is a zero divisor, there must also be (by definition of zero divisor) a non-trivial solution.

31. In \mathbb{Z}_{26} , we see that $[22]$ is not a unit, so it has no inverse.

$$[9]^{-1} = [3], \quad [11]^{-1} = [19], \quad [17]^{-1} = [23]$$