# Solutions 05

**P5.1.** Solve the system of linear equations $\mathbf{A}\mathbf{X} = \mathbf{B}$ where

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

and the entries are

**i.** in $\mathbb{Q}$,
**ii.** in $\mathbb{Z}/\langle 2 \rangle$,
**iii.** in $\mathbb{Z}/\langle 3 \rangle$, or
**iv.** in $\mathbb{Z}/\langle 7 \rangle$.

*Solution.*

**i.** Finding the reduced row echelon form of the augmented matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -2 \\ 0 & -2 & -1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & -3 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 1/3 \\ 0 & 1 & 0 & 2/3 \\ 0 & 0 & 1 & -4/3 \end{bmatrix},$$

we see that the unique rational solution is $\mathbf{X} = \frac{1}{3}\begin{bmatrix} 1 & 2 & -4 \end{bmatrix}^{\mathsf{T}}$.

**ii.** Finding the reduced row echelon form of the augmented matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

we see that the unique solution with entries in $\mathbb{Z}/\langle 2 \rangle$ is $\mathbf{X} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^{\mathsf{T}}$.

**iii.** Finding the reduced row echelon form of the augmented matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 2 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

we see that there is no solution with entries in $\mathbb{Z}/\langle 3 \rangle$.

**iv.** Finding the reduced row echelon form of the augmented matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 6 \\ 1 & 6 & 6 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 6 & 1 & 5 \\ 0 & 5 & 6 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 6 \\ 0 & 1 & 6 & 2 \\ 0 & 0 & 4 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

we see that the unique solution with entries in $\mathbb{Z}/\langle 7 \rangle$ is $\mathbf{X} = \begin{bmatrix} 5 & 3 & 1 \end{bmatrix}^{\mathsf{T}}$. □

**Remark.** Since $3 \equiv 1 \bmod 2$, it follows that $3^{-1}\begin{bmatrix} 1 & 2 & -4 \end{bmatrix}^{\mathsf{T}} \equiv \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^{\mathsf{T}} \bmod 2$. Similarly, we have $(3)(5) \equiv 15 \equiv 1 \bmod 7$, so $3^{-1}\begin{bmatrix} 1 & 2 & -4 \end{bmatrix}^{\mathsf{T}} \equiv \begin{bmatrix} 5 & 10 & -20 \end{bmatrix}^{\mathsf{T}} \equiv \begin{bmatrix} 5 & 3 & 1 \end{bmatrix}^{\mathsf{T}} \bmod 7$.

**P5.2.** Demonstrate that the equation $x^6 + y^{12} = 703$ has no integer solutions.

*Solution.* If the given equation had integer solutions, then it would also have solutions modulo 7. Reducing modulo 7 gives $x^6 + y^{12} \equiv 3 \mod 7$. Fermat's Little Theorem implies that

$$x^6 \equiv \begin{cases} 0 \mod 7 & \text{if } x \equiv 0 \mod 7, \\ 1 \mod 7 & \text{if } x \not\equiv 0 \mod 7, \end{cases}$$

and

$$y^{12} = (y^6)^2 \equiv \begin{cases} 0 \mod 7 & \text{if } y \equiv 0 \mod 7, \\ 1 \mod 7 & \text{if } y \not\equiv 0 \mod 7. \end{cases}$$

It follows that

$$x^6 + y^{12} \equiv \begin{cases} 0 \mod 7 & \text{if } x \equiv 0 \mod 7 \text{ and } y \equiv 0 \mod 7, \\ 1 \mod 7 & \text{if } x \not\equiv 0 \mod 7 \text{ and } y \equiv 0 \mod 7, \\ 1 \mod 7 & \text{if } x \equiv 0 \mod 7 \text{ and } y \not\equiv 0 \mod 7, \\ 2 \mod 7 & \text{if } x \not\equiv 0 \mod 7 \text{ and } y \not\equiv 0 \mod 7. \end{cases}$$

We deduce that $x^6 + y^{12} \not\equiv 3 \mod 7$. Since the congruence has no solutions, the original equation has no integer solutions. □

**P5.3.** Determine whether the set $\mathbb{R} \cup \{\infty\}$ with addition and multiplication defined, for all $x$ and $y$ in $\mathbb{R} \cup \{\infty\}$, by $x \boxplus y := \min(x, y)$ and $x \boxtimes y := x + y$, forms a commutative ring. If it is not, then list all of the defining properties that do hold and all those that fail to hold.

*Solution.* The triple $(\mathbb{R} \cup \{\infty\}, \boxplus, \boxtimes)$ is not a commutative ring. The associativity of addition, commutativity of addition, the existence of an additive identity, the associativity of multiplication, the existence of a multiplicative identity, distributivity, and commutativity of multiplication hold: for any $x$, $y$, and $z$ in $\mathbb{R} \cup \{\infty\}$, we have

$$\begin{aligned} (x \boxplus y) \boxplus z &= \min\big(\min(x, y), z\big) = \min(x, y, z) = \min\big(x, \min(x, y)\big) = x \boxplus (y \boxplus z) \\ x \boxplus y &= \min(x, y) = \min(y, x) = y \boxplus x \\ x \boxplus \infty &= \min(x, \infty) = x \\ (x \boxtimes y) \boxtimes z &= (x + y) + z = x + (y + z) = x \boxtimes (y \boxtimes z) \\ x \boxtimes 0 &= x + 0 = x \\ x \boxtimes (y \boxplus z) &= x + \min(y, z) = \min(x + y, x + z) = (x \boxtimes y) \boxplus (x \boxtimes z) \\ x \boxtimes y &= x + y = y + x = y \boxtimes x \end{aligned}$$

The element $\infty$ is the additive identity and the element 0 is the multiplicative identity. However, the existence of an additive inverse does not hold: for any $x$ and $y$ in $\mathbb{R} \cup \{\infty\}$, we have

$$x \boxplus y = \infty \qquad \Leftrightarrow \qquad \min(x, y) = \infty \qquad \Leftrightarrow \qquad x = y = \infty\,.$$

In other words, only $\infty$ has an additive inverse. □

**Remark.** This algebraic structure is called the *min-plus algebra* or the *tropical semiring.*