Section 19 Solutions

4. Find all the solutions of $x^2 + 2x + 4 = 0$ in $\mathbb{Z}_6$.

   Since $\mathbb{Z}_6$ has only 6 elements, we can try them all:
   $0^2 + 2 \cdot 0 + 4 = 4$
   $1^2 + 2 \cdot 1 + 4 = 1$
   $2^2 + 2 \cdot 2 + 4 = 0$
   $3^2 + 2 \cdot 3 + 4 = 1$
   $4^2 + 2 \cdot 4 + 4 = 4$
   $5^2 + 2 \cdot 5 + 4 = 3$
   Thus there is only one solution, $x = 2$.

10. What is the characteristic of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$?

    This is the smallest integer n for which $n(1,1) = (n,n) = (0,0)$.
    So you can see that integer n must be divisible by both 6 and 15.
    The smallest such integer is 30. Thus the characteristic is 30.

14. Notice that $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, so $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{Z})$.

20. Show that the characteristic of an integral domain D is either 0 or a prime number.

    First, let's rewrite the statement in the form If A then B.

    Here is the statement we must prove:
    If D is an integral domain, then its characteristic is either 0 or prime.
    Proof (By contradiction):
    Suppose that it is not true that the characteristic is either 0 or prime.
    Then the characteristic is a positive non-prime number.
    Thus the characteristic can be written as a product mn of two positive integers.
    Then $mn(1) = 0$, by definition of characteristic. This equation is
    $0 = 1 + 1 + 1 + ... + 1$ (mn times)
    $0 = (1 + 1 + ... + 1) + (1 + 1 + ... + 1) + ... + (1 + 1 + ... + 1)$ (m groups of n 1's)
    $0 = n1 + n1 + ... + n1$ (m times)
    $0 = n1 \cdot 1 + n1 \cdot 1 + ... + n1 \cdot 1$ ($a1 = a$)
    $0 = (n1)(1 + 1 + ... + 1)$ (distributive property)
    $0 = (n1)(m1)$
    But neither $n1$ nor $m1$ is 0 for each of m and n is smaller than the characteristic mn.
    This means D has zero divisors $m1$ and $n1$, contradicting the fact that D is an integral domain. This contradiction proves the theorem.