Section 3.1.

1. (a) Closure of addition, because \(1 + 3 = 4\), which is not odd.
   (b) The existence of additive inverses, because 1 is a non-negative integer, but there is no non-negative integer which solves \(1 + x = 0\).

5. (a) Subring without identity
   (b) Subring with identity
   (c) Subring without identity
   (d) Commutative subring WITH identity: the identity is \(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\).
   (e) Commutative subring with identity
   (f) Commutative subring WITH identity: the identity is \(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\).

6. No. \(0 \in \mathbb{C} = 0\), but \(0 \notin \{1, -1, i, -i\}\).

12. Yes. We will check the 4 conditions of Theorem 3.2:
   (i) Suppose \(f, g \in S\). Then \((f + g)(2) = f(2) + g(2) = 0 + 0 = 0\), so \(S\) is closed under the addition of \(T\).
   (ii) Suppose \(f, g \in S\). Then \((f \cdot g)(2) = f(2) \cdot g(2) = 0 \cdot 0 = 0\), so \(S\) is closed under the multiplication of \(T\).
   (iii) \(0_T\) is the zero function \(z : \mathbb{R} \to \mathbb{R}\) such that \(z(r) = 0\) for all \(r \in \mathbb{R}\). Notice that \(z(2) = 0\), so \(z \in S\).
   (iv) Suppose \(f \in S\). Then the function \(g : \mathbb{R} \to \mathbb{R}\) defined by \(g(r) = -f(r)\) for all \(r \in \mathbb{R}\) is the solution to \(f + x = 0_T\). Notice that since \(f \in S\), \(f(2) = 0\), which means that \(g(2) = -f(2) = -0 = 0\), so \(g \in S\).
   By Theorem 3.2, \(S\) is a subring of \(T\).

14. We must check that all 8 axioms in the definition of a ring are satisfied. The first 5 axioms only involve addition, and the addition we are considering is the ordinary addition on \(\mathbb{Z}\), so we know these axioms hold.
   6. If \(a, b \in \mathbb{Z}\), then \(ab = 0 \in \mathbb{Z}\), so our ring is closed under multiplication.
   7. If \(a, b, c \in \mathbb{Z}\), then \(a(bc) = a(0) = 0 = (0)c = (ab)c\), so our new multiplication is associative.
   8. If \(a, b, c \in \mathbb{Z}\), then \(a(b + c) = 0 = 0 + 0 = ab + ac\), and \((a + b)c = 0 = 0 + 0 = ac + ac\), so our new multiplication is distributive.
   Thus, with the new definition of multiplication, \(\mathbb{Z}\) is a ring. In fact, for any \(a, b \in \mathbb{Z}\), \(ab = 0 = ba\), so it is a commutative ring.
18. We must check that all 8 axioms are satisfied: For any \( a, b, c \in \mathbb{Z} \),

1. \( a \oplus b = a + b - 1 \in \mathbb{Z} \), because \( a \oplus b = a + b - 1 = a + b - 1 + c - 1 = (a + b - 1) + c = (a + b) \oplus c \).

2. \( a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 1 - 1 = a + b - 1 + c - 1 = (a + b - 1) + c = (a + b) \oplus c \).

3. \( a \oplus b = a + b - 1 \in \mathbb{Z} \), because \( a \oplus b = a + b - 1 = a + b - 1 + c - 1 = (a + b - 1) + c = (a + b) \oplus c \).

4. 1 is the zero element in this ring, because \( a \oplus 1 = a + 1 - 1 = a \).

5. For each \( a \in \mathbb{Z} \), its additive inverse is \( 2 - a, because \( a \oplus (2 - a) = a + 2 - a - 1 = 1 \), and 1 is the zero element in this ring.

6. \( a \oplus b = a + b - ab \in \mathbb{Z} \), because \( a \oplus b = a + b - ab \in \mathbb{Z} \), and since \( ab \in \mathbb{Z} \), \( a \oplus b \in \mathbb{Z} \).

7. \( a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 1 - 1 = a + b - 1 + c - 1 = (a + b - 1) + c = (a + b) \oplus c \).

8. \( a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 1 - 1 = a + b - 1 + c - 1 = (a + b - 1) + c = (a + b) \oplus c \).

This proves that \((\mathbb{Z}, \oplus, \circ)\) is a ring. To verify that it is an integral domain, we must check that it is commutative: \( a \oplus b = a + b - ab = b + a - ba = b \circ a \).

And that there is a multiplicative identity: The multiplicative identity is 0, because \( a \circ 0 = a + 0 - a(0) = a \).

And finally, we observe that the zero element (1) and the multiplicative identity (0) are different, and if \( a \oplus b = 0_R = 1 \), then \( a + b - ab = 1 \), so \( a(1 - b) = 1 - b \). If \( b = 1 = 0_R \), then we are done. Otherwise, we can divide by \((1 - b)\), and find that \( a = \frac{1 - b}{1 - b} = 1 = 0_R \).

Thus, \((\mathbb{Z}, \oplus, \circ)\) is an integral domain.

27. We verify all 8 axioms of a ring: For any \((r, s), (r', s'), (r'', s'') \in R \times S\),

1. \((r, s) + (r', s') = (r + r', s + s') \in R \times S\).

2. \((r, s) + ((r', s') + (r'', s'')) = (r, s) + (r' + r'', s' + s'') = (r + r' + r'', s + s' + s'') = (r + r', s + s') + (r'', s'') = ((r, s) + (r', s')) + (r'', s'').\)

3. \((r, s) + (r', s') + (r'', s'') = (r + r', s + s') + (r'', s'') = (r + r', s + s') + (r'', s'')\).

4. \((0_R, 0_S) = 0_R, 0_S = ((r + 0_R, s + 0_S) = (r, s)\).

5. \((r, s) + (r', s') = (r + r', s + s') = (r + r', s + s') + (r'', s'') = (r + r', s + s') + (r'', s'')\).

6. \((r, s)[(r', s') + (r'', s'')] = (r, s)(r' + r'', s + s'') = (r, s)(r', s') + (r, s)(r'', s'') = (r, s)(r', s') + (r, s)(r'', s'')\).

If \( R \) and \( S \) are both commutative, then \((r, s)(r', s') = (r', s')(r, s) = (r', s')(r, s)\). And if \( R \) and \( S \) both have identities \( 1_R, 1_S \) respectively, then \((1_R, 1_S)\) is the identity in \( R \times S \), because \((r, s)(1_R, 1_S) = (1_R, 1_S)(r, s)\).

29. (a) False. Consider \( R = S = \mathbb{Z} \). Then \((1, 0)(0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0) \), but neither \((1, 0)\) nor \((0, 1)\) is \((0, 0) = 0_{\mathbb{Z} \times \mathbb{Z}}\).

(b) False. Consider \( R = S = \mathbb{Q} \). Then \((1, 0) \neq 0_{\mathbb{Q} \times \mathbb{Q}}\), but there is no \((r, s) \in \mathbb{Q} \times \mathbb{Q} \) such that \((1, 0)(r, s) = (1, 1)\), because \((1, 0)(r, s) = (1r, 0s) = (r, 0)\).

3.2.

3. (a) No. Suppose \( z \) and \( 0_R \) were both zero elements in \( R \). Then \( 0_R + z = 0_R \), because \( z \) is a zero element. But also, \( 0_R + z = z \), because \( 0_R \) is a zero element. Thus, \( 0_R = z \).

(b) No. Suppose \( w \) and \( 1_R \) were both identity elements. Then \( 1_R \cdot 1_R = 1_R \), because \( 1_R \) is an identity element. But also \( 1_R \cdot w = 1_R \), because \( w \) is an identity element. Thus, \( 1_R = w \).
12. Suppose \([a]\) is a unit in \(\mathbb{Z}_n\). Then there exists a \([b] \in \mathbb{Z}_n\) such that \([a][b] = [1]\). Then, \(n(ab - 1)\), which means that \(nk = ab - 1\) for some \(k \in \mathbb{Z}\). In particular then, \(b(a) + (-k)(n) = 1\), so by Theorem 1.3, \((a, n) = 1\). Conversely, suppose that \((a, n) = 1\). Then \(n \nmid a\), so \([a] \neq [0]\) in \(\mathbb{Z}_n\). And by Theorem 1.3, there exist \(u, v \in \mathbb{Z}\) with \(ua + vn = 1\). Notice that \((u, n) = 1\), by Theorem 1.3, so \([u] \neq [0]\) in \(\mathbb{Z}_n\). And \(ua - 1 = vn\), which implies that \(ua \equiv 1 (mod n)\). Then, \([u][a] = [1] = [a][u]\), where neither of \([a]\) nor \([u]\) is \([0]\) in \(\mathbb{Z}_n\), so \([a]\) is a unit.

(b) NOTE: This statement is not true for \([a] = [0]\), which is not a unit, and is not a zero-divisor. It is true, however, for non-zero elements.

(c) Suppose \([a] \neq [0]\) is not a unit. Then by (a) above, \((a, n) \neq 1\). Say \((a, n) = d\). Then there exist \(u, v, k \in \mathbb{Z}\) with \(au + nv = d\), and \(dk = n\). Now, multiplying the first equality by \(k\) gives, \(a(ku) + knv = dk = n\), so \(a(ku) = n(k - kv)\), which means that \([a][ku] = [0]\). Conversely, suppose \([a]\) is a zero-divisor. Then there exists a \([b] \neq [0]\) such that \([a][b] = [0]\). Now, by way of contradiction, suppose that there were a \([c]\) such that \([a][c] = [1]\). Then multiplying by \([b]\) would show that \(([a][b])[c] = [1][b]\), so \([0][c] = [b]\), so \([0] = [b]\), a contradiction.

19. Consider \(S = \left\{ \begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}\), a subring of \(R = M_2(\mathbb{R})\). Then \(1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\), but \(1_S = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\). (See Exercise 5 in Section 3.1).

(b) Suppose both \(R\) and \(S\) are fields. Let \(0_S \neq s \in S\). Since \(S \subset R\), \(s \in R\) as well. Then, since \(S\) is a field, \(s^{-1} \in S\). Since \(s\) and \(s^{-1}\) are both in \(R\), \(s \cdot s^{-1} = 1_R\). But \(S\) is closed under multiplication, so \(1_R = s \cdot s^{-1} \in S\) as well. Then, since \(1_R \in S\) is the multiplicative identity for all elements of \(R\), in particular it is the multiplicative identity for all elements of \(S\), so \(1_R = 1_S\).

(c) Suppose \(S\) has identity. If \(1_R = 1_S\), then we are done. So let us suppose \(1_R \neq 1_S\). Then \(1_S - 1_R = t \neq 0_R\). Multiplying this equation by \(1_S\) on both sides gives \(1_S \cdot 1_S = 1_S \cdot 1_R = 1_S \cdot t\). But \(1_S \cdot 1_S = 1_S\), and \(1_S \cdot 1_R = 1_S\) since \(1_R\) times anything is that same thing. Thus, \(1_S - 1_S = 1_S \cdot t\). This simplifies to \(0_R = 1_S \cdot t\), which shows that \(1_S\) is a zero-divisor in \(R\).