Instructions. Please be detailed in your solutions and proofs. The harder that I have to work to try to interpret what you are trying to say, the less partial credit you will get.

1. Write clear definitions of the following terms.

(a) Let $A$ be a non–empty set. Define what is meant by a relation, $R$, on the set $A$.

Answer: A relation on $A$ is a subset of $A \times A$.

(b) Let $A$ be a non–empty set. Define what is meant by an equivalence relation, $R$, on the set $A$.

Answer: An equivalence relation on $A$ is a relation, $R$, on $A$ such that
1. $R$ is reflexive (meaning that $(x, x) \in R$ for all $x \in A$)
2. $R$ is symmetric (meaning that if $(x, y) \in R$, then $(y, x) \in R$)
3. $R$ is transitive (meaning that if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$).

(c) Suppose that $A$ is a set of objects endowed with two binary operations called addition (and denoted by “+”) and multiplication (denoted by “∗”). Let $R = \{+, +, ∗\}$. Under what conditions is $R$ said to be a ring?

Answer: $R$ is said to be a ring if the following properties are satisfied:
1. The associative laws of addition and multiplication hold. That is, for any elements $a, b,$ and $c \in A$, we have $a + (b + c) = (a + b) + c$ and $a (bc) = (ab) c$.
2. The commutative law of addition holds. That is, for any elements $a$ and $b \in C$, we have $a + b = b + a$.
3. An additive identity exists. That is, there exists an element $0 \in A$ such that $a + 0 = a$ for $a \in A$.
4. Every element has an additive inverse. That is, for each $a \in A$, there is an element $−a \in A$ such that $a + (−a) = 0$.
5. The left and right distributive properties holds. That is, for any elements $a, b,$ and $c \in A$, we have $a (b + c) = a b + a c$ and $(b + c) a = b a + c a$.

(d) Suppose that $R$ is a ring and suppose that $a$ is an element of $R$ such that $a \neq 0$. What does it mean for $a$ to be a zero divisor?

Answer: $a$ is said to be a zero divisor if there exists an element $b \in R$ such that $b \neq 0$ and either $a \cdot b = 0$ or $b \cdot a = 0$.

(e) Suppose that $R$ is a ring with unity and suppose that $a$ is an element of $R$. What does it mean for $a$ to be a unit?

Answer: $a$ is said to be a unit if there exists an element $b \in R$ such that $a \cdot b = b \cdot a = 1$.

2. Suppose that $R$ is a ring with unity. Prove that no element of $R$ can be both a zero divisor and a unit.
3. Suppose that $m$ and $n$ are positive integers and suppose that $x_0$ is an integer. Prove that
\[
[x_0]_m \cap [x_0]_n = [x_0]_{\text{lcm}(m,n)}.
\]

**Proof:** Let $x \in [x_0]_m \cap [x_0]_n$. Then $x \equiv x_0 \pmod m$ meaning that $x = x_0 + ms$ for some integer $s$ and also $x_0 \equiv x_0 \pmod n$ meaning that $x = x_0 + nt$ for some integer $t$. This implies that $x-x_0 = ms = nt$ and hence that $x-x_0$ is a common multiple of $m$ and $n$. Since lcm $(m,n)$ divides any common multiple of $m$ and $n$, we conclude that lcm $(m,n)$ divides $x-x_0$. This means that there exists an integer $p$ such that $x-x_0 = p\text{lcm} (m,n)$ or, in other words, such that $x = x_0 + p\text{lcm} (m,n)$. Therefore $x \in [x_0]_{\text{lcm}(m,n)}$. We have now proved that
\[
[x_0]_m \cap [x_0]_n \subseteq [x_0]_{\text{lcm}(m,n)}.
\]

Next, suppose that $x \in [x_0]_{\text{lcm}(m,n)}$. Then $x = x_0 + p\text{lcm} (m,n)$ for some integer $p$. Since lcm $(m,n)$ is a multiple of $m$, we know that there exists an integer $r$ such that lcm $(m,n) = rm$. Likewise, since lcm $(m,n)$ is a multiple of $n$, we know that there exists an integer $q$ such that lcm $(m,n) = qn$. Therefore $x = x_0 + prn$, meaning that $x \in [x_0]_m$, and $x = x_0 + pqn$, meaning that $x \in [x_0]_n$. We conclude that $x \in [x_0]_m \cap [x_0]_n$. We have now proved that
\[
[x_0]_{\text{lcm}(m,n)} \subseteq [x_0]_m \cap [x_0]_n.
\]

This completes the proof.

4. Find the solution set of the system of congruence equations
\[
\begin{align*}
x & \equiv 7 \pmod 4 \\
x & \equiv 6 \pmod 9.
\end{align*}
\]

(You must express this solution set as a single congruence class.)

What is the smallest positive value of $x$ that satisfies this system?

**Solution:** By the Chinese Remainder Theorem, since gcd $(4,9) = 1$, we know that the solution set of this system of congruence equations is some congruence class modulo $4 \cdot 9 = 36$. The solution set of $x \equiv 7 \pmod 4$ is $[7]_4$ and the solution set of $x \equiv 6 \pmod 9$ is $[6]_9$. The solution set of the system is $[7]_4 \cap [6]_9$. To express this as a single congruence class, we must find a number $x_0$ such that $x_0 \equiv 7+4s$ for some integer $s$ and $x_0 \equiv 6+9t$ for some integer $t$. This leads us to solving the Diophantine equation $9t - 4s = 1$ for which it is easily seen that $(s,t) = (2,1)$ is a solution. Thus we can take $x_0 = 15$. The solution set of this system of congruence equations is $[15]_{36}$. The smallest positive solution is $x = 15$. 

2
5. List the zero divisors in \( Z_{12} \) and also list the units in \( Z_{12} \). Find the multiplicative inverse of each of the units in \( Z_{12} \).

**Answer:** The zero divisors in \( Z_{12} \) are \( 2, 3, 4, 6, 8, 9, \) and \( 10 \). The units are \( 1, 5, 7, \) and \( 11 \). The multiplicative inverse of \( 1 \) is \( 1 \) (because \( 1 \cdot 1 = 1 \)). The multiplicative inverse of \( 5 \) is \( 5 \) (because \( 5 \cdot 5 = 1 \)). The multiplicative inverse of \( 7 \) is \( 7 \) (because \( 7 \cdot 7 = 1 \)). The multiplicative inverse of \( 11 \) is \( 11 \) (because \( 11 \cdot 11 = 1 \)). Note that \( 2 \cdot 6 = 0, 3 \cdot 4 = 0, 6 \cdot 8 = 0, 4 \cdot 9 = 0, \) and \( 6 \cdot 10 = 0 \).

6. Let \( i \) be defined as usual (a number such that \( i^2 = -1 \)) and let \( Z_2[i] \) be the ring

\[ Z_2[i] = \{a + bi \mid a \in Z_2 \text{ and } b \in Z_2\} \]

(a) List all of the elements of \( Z_2[i] \).

**Answer:** The elements of \( Z_2 \) are \( 0 \) and \( 1 \) so the elements of \( Z_2[i] \) are \( 0, i, 1, \) and \( 1+i \).

(b) Construct addition and multiplication tables for \( Z_2[i] \).

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>( i )</th>
<th>( 1+i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>( i )</td>
<td>( 1+i )</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>( 1+i )</td>
<td>( i )</td>
</tr>
<tr>
<td>( i )</td>
<td>( i )</td>
<td>( 1+i )</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( 1+i )</td>
<td>( 1+i )</td>
<td>( i )</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>*</td>
<td>0</td>
<td>1</td>
<td>( i )</td>
<td>( 1+i )</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>( i )</td>
<td>( 1+i )</td>
</tr>
<tr>
<td>( i )</td>
<td>0</td>
<td>( i )</td>
<td>1</td>
<td>( 1+i )</td>
</tr>
<tr>
<td>( 1+i )</td>
<td>0</td>
<td>1</td>
<td>( 1+i )</td>
<td>0</td>
</tr>
</tbody>
</table>

(c) Is \( Z_2[i] \) an integral domain? Explain why or why not.

**Answer:** \( Z_2[i] \) is not an integral domain because it contains a zero divisor \( (1+i) \).

(d) Is \( Z_2[i] \) a field? Explain why or why not.

**Answer:** \( Z_2[i] \) is not a field because it is not an integral domain.

(a) Let \( z \) be the complex number

\[ z = \frac{-3\sqrt{3}}{2} + \frac{3}{2}i. \]

Compute \( z^3 \) directly (without using de Moivre’s formula). Show your calculation in detail.

**Solution:** First note that

\[ z = \frac{-3}{2} \left( \sqrt{3} - i \right) \]

so

\[ z^2 = \frac{9}{4} \left( \sqrt{3} - i \right)^2 \]

\[ = \frac{9}{4} \left( 3 - 2\sqrt{3}i - 1 \right) \]

\[ = \frac{9}{4} \left( 2 - 2\sqrt{3}i \right) \]

\[ = \frac{9}{2} \left( 1 - \sqrt{3}i \right) \]
so

\[ z^3 = z^2 \cdot z \]
\[ = \frac{9}{2} \left( 1 - \sqrt{3}i \right) \cdot \left( \frac{-3}{2} \right) \left( \sqrt{3} - i \right) \]
\[ = -\frac{27}{4} \left( \sqrt{3} - i - 3i - \sqrt{3} \right) \]
\[ = -27i \]

(b) Write \( z \) in the polar form

\[ z = |z| \left( \cos (\theta) + \sin (\theta) i \right) \]

(where \( |z| \) is the modulus of \( z \) and \( \theta \) is some argument of \( z \)) and then compute \( z^3 \) by using de Moivre’s formula.

Solution: Since

\[ |z| = \sqrt{\left( \frac{-3\sqrt{3}}{2} \right)^2 + \left( \frac{3}{2} \right)^2} = 3, \]

we see that

\[ z = 3 \left( \frac{-\sqrt{3}}{2} + \frac{1}{2} i \right) = 3 \left( \cos (150^\circ) + \sin (150^\circ) i \right). \]

By de Moivre’s formula,

\[ z^3 = 3^3 \left( \cos (450^\circ) + \sin (450^\circ) i \right) \]
\[ = 27 \left( 0 + i \right) \]
\[ = 27i. \]

(c) Find all three cube roots of the number 27i. Write each answer in the standard form \( a + bi \). (Be detailed in your explanation of this. Include a picture that shows the location of these three cube roots in the complex plane.)

Solution: Since

\[ 27i = 27 \left( 0 + i \right) = 27 \left( \cos (90^\circ) + \sin (90^\circ) i \right), \]

the cube roots of \( z \) are

\[ z_1 = 3 \left( \cos \left( \frac{90^\circ + 360^\circ \cdot 0}{3} \right) + \sin \left( \frac{90^\circ + 360^\circ \cdot 0}{3} \right) i \right) \]
\[ = 3 \left( \cos (30^\circ) + \sin (30^\circ) i \right) \]
\[ = \frac{3\sqrt{3}}{2} + \frac{\sqrt{3}}{2} i, \]

\[ z_2 = 3 \left( \cos \left( \frac{90^\circ + 360^\circ \cdot 1}{3} \right) + \sin \left( \frac{90^\circ + 360^\circ \cdot 1}{3} \right) i \right) \]
\[ = 3 \left( \cos (150^\circ) + \sin (150^\circ) i \right) \]
\[ = \frac{-3\sqrt{3}}{2} + \frac{3}{2} i, \]
and

\[ z_3 = 3 \left( \cos \left( \frac{90^\circ + 360^\circ \cdot 2}{3} \right) + \sin \left( \frac{90^\circ + 360^\circ \cdot 2}{3} \right) i \right) \]

\[ = 3 \left( \cos (270^\circ) + \sin (270^\circ) i \right) \]

\[ = -3i. \]