1. Suppose \([a], [b] \in \mathbb{Z}_6\) so that \([a] \cdot [b] = [0]\). Can you conclude that either \([a] = [0]\) or \([b] = [0]\)? Why or why not?

**Answer:** No, you can’t conclude that either \([a]\) or \([b]\) is \([0]\). For example, if \([a] = [2]\) and \([b] = [3]\), then \([2] \cdot [3] = [2 \cdot 3] = [6] = [0]\).

2. List all the possible equivalence relations on the set \(A = \{a, b\}\). (For organizational purposes, it may be helpful to write the relations as subsets of \(A \times A\).)

**Answer:** Thinking of an equivalence relation \(R\) on \(A\) as a subset of \(A \times A\), the fact that \(R\) is reflexive means that 
\[\{(a, a), (b, b)\} \subseteq R.\]

Clearly, one possibility is just to let \(R = \{(a, a), (b, b)\}\), which is automatically reflexive, symmetric, and transitive.

Now, if I want to add an element to \(R\), my only possibilities are \((a, b)\) and \((b, a)\). But \(R\) being symmetric means that if I add one I have to add both, so I could also let \(R = \{(a, a), (b, b), (a, b), (b, a)\}\). This is reflexive and symmetric by construction and it is automatically transitive since \(R\) only contains 2 elements.

These are the only two possibilities, so I see that the only equivalence relations on \(A\) are 
\[\{(a, a), (b, b)\}\] and 
\[\{(a, a), (b, b), (a, b), (b, a)\}\].

3. Define the relation \(R\) on \(\mathbb{Z}\) by \(x R y\) if \(x^2 \equiv y^2 \pmod{4}\). Is \(R\) an equivalence relation? If so, what are the equivalence classes of \(R\)?

**Answer:** Yes, \(R\) is an equivalence relation. To prove this, I need to show that \(R\) is reflexive, symmetric, and transitive.

**Reflexive:** Let \(x \in \mathbb{Z}\). Then \(x^2 \equiv x^2 \pmod{4}\), so \(x R x\).

**Symmetric:** Let \(x, y \in \mathbb{Z}\) so that \(x R y\). This means that \(x^2 \equiv y^2 \pmod{4}\), which obviously means that \(y^2 \equiv x^2 \pmod{4}\) and hence that \(y R x\), so \(R\) is symmetric.

**Transitive:** Let \(x, y, z \in \mathbb{Z}\) so that \(x R y\) and \(y R z\). Then \(x^2 \equiv y^2 \pmod{4}\) and \(y^2 \equiv z^2 \pmod{4}\), so we have that 
\[x^2 \equiv y^2 \equiv z^2 \pmod{4},\]
so \(x R z\) and we conclude that \(R\) is transitive.

Now, to figure out the equivalence classes, let’s think about the four possibilities for an integer: it can be congruent to 0, 1, 2, or 3 modulo 4.

- If \(a \equiv 0 \pmod{4}\), then \(a^2 \equiv 0^2 \equiv 0 \pmod{4}\).
- If \(a \equiv 1 \pmod{4}\), then \(a^2 \equiv 1^2 \equiv 1 \pmod{4}\).
- If \(a \equiv 2 \pmod{4}\), then \(a^2 \equiv 2^2 \equiv 0 \pmod{4}\).
- If \(a \equiv 3 \pmod{4}\), then \(a^2 \equiv 3^2 \equiv 1 \pmod{4}\).

Therefore, all even integers are in the same equivalence class and all odd integers are in a different equivalence class, and these are the only two equivalence classes.

4. Define the relation \(R\) on \(\mathbb{R}\) by \(x R y\) if \(xy > 0\). Is \(R\) an equivalence relation? If so, what are the equivalence classes of \(R\)?

**Answer:** No. Since \(0 \cdot 0 = 0\) is not greater than 0, we know that \(0 R 0\), so \(R\) is not reflexive.
5. Suppose \( R_1 \) and \( R_2 \) are equivalence relations on a set \( A \). Define the relation \( R \) on \( A \) by \( x R y \) if \( x R_1 y \) and \( x R_2 y \). Give the first two steps of the proof that \( R \) is an equivalence relation by showing that \( R \) is reflexive and symmetric.

**Proof. Reflexive:** Let \( a \in A \). Then since \( R_1 \) and \( R_2 \) are reflexive, \( a R_1 a \) and \( a R_2 a \), so \( a R a \) and \( R \) is reflexive.

**Symmetric:** Let \( a, b \in A \) so that \( a R b \). This means that \( a R_1 b \) and \( a R_2 b \). Since \( R_1 \) and \( R_2 \) are symmetric, this implies that \( b R_1 a \) and \( b R_2 a \), so \( b R a \) and \( R \) is symmetric. \( \square \)

6. Let \( A = \{1, 2, 3, 4\} \) and \( B = \{a, b, c\} \). Find a function \( f : A \to B \) which is either injective or surjective, but not both.

**Answer:** Define \( f : A \to B \) by the following subset of \( A \times B \):

\[
\{ (1, a), (2, a), (3, b), (4, c) \}.
\]

Then \( f \) is surjective since all elements of \( B \) are in the range of \( f \): \( f(1) = a \), \( f(3) = b \), and \( f(4) = c \). However, \( f \) is clearly not injective since \( f(1) = f(2) = a \).

7. Define the function \( g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \) by \( g(m, n) = 2n - 4m \).

(a) Is \( g \) injective? Prove or give a counterexample.

**Answer:** No. Notice that \( g(1, 2) = 2(2) - 4(1) = 0 \) and that \( g(2, 4) = 2(4) - 4(2) = 0 \), so \( g \) is not injective.

(b) Is \( g \) surjective? Prove or give a counterexample.

**Answer:** No. Notice that, regardless of what \( m \) and \( n \) are, \( g(m, n) = 2n - 4m = 2(n - 2m) \) is even. Therefore, since \( 1 \) is odd, there is no \( (m, n) \in \mathbb{Z} \times \mathbb{Z} \) so that \( g(m, n) = 1 \), and hence \( g \) is not surjective.

8. Define the function \( h : \mathbb{Z}_8 \to \mathbb{Z}_8 \) by \( h([a]) = [a^3] \).

(a) Is \( h \) injective? Prove or give a counterexample.

**Answer:** No. Since \( h([2]) = [2^3] = [8] = [0] \) and \( h([0]) = [0^3] = [0] \), we can see that \( h \) is not injective.

(b) Is \( h \) surjective? Prove or give a counterexample. (*Hint: Why does your answer to part (a) provide the answer to this question without doing any additional work?*)

**Answer:** No. We can use the result proved in class which said that if \( A \) is a finite set and \( f : A \to A \), then \( f \) is injective if and only if \( f \) is surjective. In this case, we saw in (a) that \( h \) isn’t injective; since \( \mathbb{Z}_8 \) is finite, this means that \( h \) cannot be surjective.

9. Suppose \( A, B, \) and \( C \) are sets and that \( f : A \to B \) and \( g : B \to C \) are functions. If \( g \circ f \) is surjective, is \( f \) necessarily surjective? Prove or give a counterexample.

**Answer:** No. Consider \( A = B = \{1, 2\} \), \( C = \{1\} \) and define \( f : A \to B \) by \( f(1) = f(2) = 1 \) and \( g : B \to C \) by \( g(1) = g(2) = 1 \). Then \( (g \circ f)(a) = 1 \) for all \( a \in A \) and \( g \circ f \) is obviously surjective, but \( f \) is not surjective since there is no \( a \in A \) so that \( f(a) = 2 \).

10. Define the sequence \( a_1, a_2, a_3, \ldots \) by

\[
a_1 = 1, \quad a_2 = 2, \quad \text{and} \quad a_n = 2a_{n-1} - a_{n-2} \text{ for all } n \geq 3.
\]

Prove that \( a_n = n \) for all \( n \in \mathbb{N} \).
Proof. The goal is to prove this using strong induction. For \( n \in \mathbb{N} \), let \( P(n) \) be the statement that \( a_n = n \). Then I want to show that \( P(n) \) is true for all \( n \in \mathbb{N} \).

**Base Case:** Clearly \( P(1) \) and \( P(2) \) are true, since \( a_1 = 1 \) and \( a_2 = 2 \).

**Inductive Step:** Let \( k \in \mathbb{N} \) and assume \( P(i) \) is true for all \( 1 \leq i \leq k \). In other words, we assume that \( a_i = i \) whenever \( 1 \leq i \leq k \).

Now, the goal is to use this information to prove \( P(k + 1) \), which says that \( a_{k+1} = k + 1 \). By definition,

\[
a_{k+1} = 2a_k - a_{k-1}.
\]

But now, by the strong inductive hypothesis, \( P(k) \) and \( P(k - 1) \) are true, so \( a_k = k \) and \( a_{k-1} = k - 1 \). Hence,

\[
a_{k+1} = 2a_k - a_{k-1} = 2(k) - (k - 1) = 2k - k + 1 = k + 1,
\]

and I’ve proved that \( a_{k+1} = k + 1 \), so \( P(k + 1) \) is true.

Having proved both the base case and the (strong) inductive step, the strong principle of mathematical induction allows me to conclude that \( P(n) \) is true for all \( n \in \mathbb{N} \), as desired. \( \square \)