Test 1 - Solutions

1. Let $a, b, c \in \mathbb{Z}, c \neq 0$. Prove that $b|ac \iff b|a$.
   
   $(\Rightarrow)$ If $b|ac$ then $ac = mb$ for some integer $m$. Since $c \neq 0$, $a = mb$, i.e. $b|a$.
   
   $(\Leftarrow)$ If $b|a$ then $a = mb$ for some integer $m$. Then $ac = mbc$, i.e. $b|ac$.

2. Solve the congruence $30x \equiv 18 \pmod{27}$.
   Since $(30,27) = 3|18$, the congruence has 3 distinct solutions modulo 27, which are congruent modulo 9.
   
   Divide by $3$: $10x \equiv 6 \pmod{9}$. Now there are at least 2 different approaches.
   
   Approach 1: Since $10 \equiv 1 \pmod{9}$, the equation is equivalent to $x \equiv 6 \pmod{9}$.
   
   Approach 2 (the more standard one): Now $(10,9) = 1$, so the congruence has a unique solution modulo 9. To find a solution, we will find integers $a$ and $b$ such that $10a = 6 + 9b$, or $6 = 10a + 9(-b)$.
   
   First, $1 = 10 + 9(-1)$ can be found using the Euclidean algorithm or simply by observation since the numbers are small. Now multiply both sides by 6: $6 = 10 \cdot 6 + 9(-6)$.
   Then $10 \cdot 6 \equiv 6 \pmod{9}$, so $x = 6$ is a solution, so the answer is $x \equiv 6 \pmod{9}$.

3. Find
   
   (a) the multiplicative order
   (b) the multiplicative inverse
   
   of $[3]$ in $\mathbb{Z}_{11}^*$
   
   $3^2 = 9$
   
   $3^3 = 27 \equiv 5 \pmod{11}$
   
   $3^4 = 5 \cdot 3 = 15 \equiv 4 \pmod{11}$
   
   $3^5 \equiv 4 \cdot 3 = 12 \equiv 1 \pmod{11}$
   
   Therefore the multiplicative order of $[3]_{11}$ is 5, and the multiplicative inverse of $[3]_{11}$ is $[4]_{11}$.

4. Is $f : \mathbb{Z}_{12} \to \mathbb{Z}_8$ given by $f([x]_{12}) = [3x]_8$ a well-defined function? Explain why or why not.
   
   No, because e.g. $[0]_{12} = [12]_{12}$ but $f([0]_{12}) = [0]_8$ and $f([12]_{12}) = [3 \cdot 12]_8 = [36]_8 = [4]_8$.

5. Consider the set of real numbers $\mathbb{R}$. For $x$ and $y$ in $\mathbb{R}$, let $x \sim y$ if $(x - y) \in \mathbb{Z}$. Show that $\sim$ is an equivalence relation, and describe the equivalence classes.
   
   Reflexive law: for each $x$, $x \sim x$ since $x - x = 0 \in \mathbb{Z}$.
   
   Symmetric law: if $x \sim y$, then $(x - y) \in \mathbb{Z}$, then $(y - x) = -(x - y) \in \mathbb{Z}$, so $y \sim x$.
   
   Transitive law: if $x \sim y$ and $y \sim z$, then $(x - y) \in \mathbb{Z}$ and $(y - z) \in \mathbb{Z}$, then $x - z = (x - y) + (y - z) \in \mathbb{Z}$, so $x \sim z$.
   
   The equivalence class of $x$ is the set of all real numbers $y$ such that $y - x = m \in \mathbb{Z}$, i.e. $y = x + m$:

   $[x] = \{ \ldots, x-3, x-2, x-1, x, x+1, x+2, x+3, \ldots \}$. There are infinitely many equivalence classes, one class for each number $a \in [0,1)$.

6. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$.

   (a) Find $\tau \sigma$.
   $\tau \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$

   (b) Draw the associated diagram for $\sigma$.
   
   (c) Write $\sigma$ as a product of disjoint cycles.
   $\sigma = (13)(254)$

**Optional:** Does there exist an integer number $m$ such that for any prime number $p$, $m \equiv p - 1 \pmod{p}$?

If such a number exists, find it. If not, prove that there is no such number.

Yes. $m = -1$ satisfies that property.