Math 151

Fall 2008

Test 1 - Solutions

1. Solve the congruence $9x \equiv 2 \pmod{29}$.
   First we will find $b \in \mathbb{Z}$ *such that* $9b \equiv 1 \pmod{29}$. *We will use the Euclidean algorithm:* $29 = 9 \cdot 3 + 2, \quad 9 = 2 \cdot 4 + 1$
   $1 = 9 - 2 \cdot 4 = 9 - (29 - 9 \cdot 3) \cdot 4 = 9 \cdot 13 + 29 \cdot (-4)$
   Thus $9 \cdot 13 \equiv 1 \pmod{29}$. *Multiplying both sides of the given congruence by 13, we have* $13 \cdot 9x \equiv 13 \cdot 2 \pmod{29}$, *i.e.* $x \equiv 26 \pmod{29}$.

2. (a) List all the elements of $\mathbb{Z}_{15}^*$.
   $[1]_{15}$, $[2]_{15}$, $[4]_{15}$, $[7]_{15}$, $[8]_{15}$, $[11]_{15}$, $[13]_{15}$, $[14]_{15}$.

   (b) Find the multiplicative inverse of $[7]$ in $\mathbb{Z}_{15}^*$.
   Since $[7]_{15}^2 = [49]_{15} = [4]_{15}$, $[7]_{15}^3 = [28]_{15} = [13]_{15}$, $[7]_{15}^4 = [91]_{15} = [1]_{15}$, *the multiplicative inverse of* $[7]$ *in* $\mathbb{Z}_{15}^*$ *is* $[13]_{15}$.

3. Let $f : \mathbb{Z}_{15} \to \mathbb{Z}_3$ be given by $f([x]_{15}) = [2x]_3$.

   (a) Show that f is a well-defined function.
   If $[x_1]_{15} = [x_2]_{15}$, *then* $x_1 \equiv x_2 \pmod{15}$. *Then* $2x_1 \equiv 2x_2 \pmod{15}$, *therefore* $2x_1 \equiv 2x_2 \pmod 3$, *i.e.* $f([x_1]_{15}) = f([x_2]_{15})$, *so* f *is well-defined.*

   (b) Is f one-to-one?
   No. For example, $f([0]_{15}) = [0]_3 = [6]_3 = f([3]_{15})$ *while* $[0]_{15} \neq [3]_{15}$.

   (c) Is f onto?
   Yes. Every element of $\mathbb{Z}_3$ *is in the image:* $[0]_3 = f([0]_{15})$, $[1]_3 = [4]_3 = f([2]_{15})$, $[2]_3 = f([1]_{15})$.

4. Consider the set of real numbers $\mathbb{R}$. For x and y in $\mathbb{R}$, let $x \sim y$ if $(x + y) \in \mathbb{Z}$.

   (a) Is $\sim$ reflexive?
   No. For example, if $x = 0.1$, *then* $(x + x) \notin \mathbb{Z}$, *therefore* $x \not\sim x$.

   (b) Is $\sim$ symmetric?
   Yes. If $x \sim y$, *then* $(x + y) \in \mathbb{Z}$, *then* $(y + x) \in \mathbb{Z}$, *so* $y \sim x$.

   (c) Is $\sim$ transitive?
   No. For example, if $x = 0.1$, $y = 0.9$, *and* $z = 0.1$, *then* $(x + y) \in \mathbb{Z}$ *and* $(y + z) \in \mathbb{Z}$, *but* $(x + z) \notin \mathbb{Z}$. *So* $x \sim y$ *and* $y \sim z$, *but* $x \not\sim z$.

   (d) Is $\sim$ an equivalence relation?
   No, since it does not have all three of the above properties.

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

   (a) Find $\tau\sigma$.
   $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$.

   (b) Write σ as a product of disjoint cycles.
   $\sigma = (1, 4, 6, 2)(3, 5)$.

6. (Optional) Prove that the inverse of an even permutation is an even permutation, and that the inverse of an odd permutation is an odd permutation.
Let σ be an even permutation, then σ can be written as a product of an even number of transpositions, say, $\sigma = (a_1, b_1)(a_2, b_2) \ldots (a_n, b_n)$ (where n is even). Then $\sigma^{-1} = (a_n, b_n)^{-1} \ldots (a_2, b_2)^{-1}(a_1, b_1)^{-1}$. Since the order of each transposition is 2, each transposition is its own inverse, so $\sigma^{-1} = (a_n, b_n) \ldots (a_2, b_2)(a_1, b_1)$. Thus σ^{-1} can be written as a product of an even number of transpositions, i.e. is an even permutation.
Similartly, if σ is an odd permutation, then σ can be written as a product of an odd number of transpositions, say, $\sigma = (a_1, b_1)(a_2, b_2) \ldots (a_n, b_n)$ (where n is odd). Then $\sigma^{-1} = (a_n, b_n)^{-1} \ldots (a_2, b_2)^{-1}(a_1, b_1)^{-1} = (a_n, b_n) \ldots (a_2, b_2)(a_1, b_1)$. Thus σ^{-1} can be written as a product of an odd number of transpositions, i.e. is an odd permutation.