Math 299 **Recitation 10** **Nov 14, 2013**

1. Prove that the following system of equations has no integer solutions.

$$11x - 5y = 7$$
$$9x + 10y = -3$$

Hint: Consider each of the equations mod 5.

Solution: Assume, by way of contradiction that $(x, y) \in \mathbb{Z}^2$ is a solution to the above system then

$$x \equiv 2 \mod 5$$
$$4x \equiv 2 \mod 5$$

The first equation (multiplying both sides by 4) implies $4x \equiv 3 \mod 5$, which contradicts the second equation. Thus the assumption that the system has an integer solution leads to a contradiction. Therefore, we can conclude that the above system has no integer solutions.

2. Prove: An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Solution: Let $x \in \mathbb{Z}$ and a_i be the i^{th} digit in its decimal representation, i.e., $x = \sum_{i=0}^{k} a_i 10^i$, where $0 \leq a_i \leq 9$ for all $i = 0, ..., k$. Note that $10^i \equiv 1 \mod 3$ for all $i \in \mathbb{N}$. Thus,

$$x \equiv \sum_{i=0}^{k} a_i \mod 3.$$

Use this to show that $3 \mid x$ if and only if $3 \mid \sum_{i=0}^{k} a_i$.

3.

(a) Find the multiplicative inverse of each nonzero element in $\mathbb{Z}_7$. *Solution:*

$$\bar{1}^{-1} = \bar{1}, \quad \bar{2}^{-1} = \bar{4}, \quad \bar{3}^{-1} = \bar{5}, \quad \bar{4}^{-1} = \bar{2}, \quad \bar{5}^{-1} = \bar{3}, \quad \bar{6}^{-1} = \bar{6}.$$

Check that, for example, $\bar{2} \cdot \bar{4} = \bar{1}$.

(b) Does every nonzero element in $\mathbb{Z}_{12}$ have a multiplicative inverse?

(c) Formulate a conjecture about which elements in $\mathbb{Z}_{12}$ will have a multiplicative inverse and which won't by considering the case of $\mathbb{Z}_4$ and $\mathbb{Z}_6$.

(d) Can you generalize your conjecture to $\mathbb{Z}_n$ for any $n \in \mathbb{N}$, $n \geq 2$?

Solution: If $\gcd(x, n) \neq 1$, then x will not have a multiplicative inverse in $\mathbb{Z}_n$.

Have students reach this conjecture on their own. It might help if the construct the multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_6$ and see which elements have multiplicative inverses.

(e) Find the multiplicative inverse of 7 mod 31. (*Hint:* Use the Euclidean Algorithm to solve $7x + 31y = 1$ for integers (x, y)).

Solution:

$$\begin{aligned} 31 &= 7 \cdot 4 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Therefore, going backward, we find $1 = 7 - 2 \cdot 3 = 7 - 2(31 - 7 \cdot 4) = 7 \cdot 9 + 31 \cdot (-2)$. Thus, $\bar{7}^{-1} = \bar{9}$.

4. For (a, b), $(c, d) \in \mathbb{R}^2$ define $(a, b) \simeq (c, d)$ to mean $a^2 + b^2 = c^2 + d^2$. Prove that $\simeq$ is an equivalence relation in $\mathbb{R}^2$, i.e. prove that it satisfies *reflexivity, symmetry* and *transitivity.*

Solution:

Reflexivity: We need to show $(a, b) \simeq (a, b) \, \forall (a, b) \in \mathbb{R}^2$. This is clear, since it is equivalent to $a^2 + b^2 = a^2 + b^2$.

Symmetry: We need to show that if $(a, b) \simeq (c, d)$ then $(c, d) \simeq (a, b)$. This is immediately evident using the definition of $\simeq$ and the symmetry of "=".

Transitivity: We need to show that if $(a, b) \simeq (c, d)$ and $(c, d) \simeq (e, f)$, then $(a, b) \simeq (e, f)$. Assume $(a, b) \simeq (c, d)$ and $(c, d) \simeq (e, f)$, then, by definition, $a^2 + b^2 = c^2 + d^2$ and $c^2 + d^2 = e^2 + f^2$. By transitivity of "=" this implies $a^2 + b^2 = e^2 + f^2$, which in its turn means that $(a, b) \simeq (e, f)$.

5. Let S be a set with an equivalence relation $\simeq$, and let $[a]$ denote the class of a (sometimes denoted as $\overline{a}$). Recall the Theorem: We have $[a] = [b]$ if and only if $[a] \cap [b] \neq \emptyset$.

For (a, b), $(c, d) \in \mathbb{R}^2$ define the equivalence relation $(a, b) \simeq (c, d)$ by: $a^2 + b^2 = c^2 + d^2$. Use the Theorem to prove: **a.** $[(0, 2)] = [(1, \sqrt{3})]$ **b.** $[(0, 2)] \cap [(1, 1)] = \emptyset$

Solution:

a. Note that $0^2 + 2^2 = 1^2 + (\sqrt{3})^2$, therefore, $(0, 2) \simeq (1, \sqrt{3})$. By definition of equivalence class, this implies that $(1, \sqrt{3}) \in [(0, 2)]$. Thus, $(1, \sqrt{3}) \in [(0, 2)] \cap [(1, \sqrt{3})]$, in particular, $[(0, 2)] \cap [(1, \sqrt{3})] \neq \emptyset$. The above theorem implies that $[(0, 2)] = [(1, \sqrt{3})]$.

b. Note that $0^2 + 2^2 \neq 1^2 + 1^2$, therefore, $(0, 2) \not\simeq (1, 1)$. By definition of equivalence class, this implies that $(1, 1) \notin [(0, 2)]$ and therefore $[(0, 2)] \neq [(1, 1)]$.

The theorem contains a biconditional statement, one of the directions asserts that if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$. The contrapositive of this statement is as follows. "If $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$."

Since we have shown that $[(0, 2)] \neq [(1, 1)]$, this implies $[(0, 2)] \cap [(1, 1)] = \emptyset$.