Discrete Structures

IIIT Hyderabad

Monsoon 2020

Tutorial 7

October 7, 2020

Introduction

1. Questions
   - Question 0
   - Question 1
   - Question 2
   - Question 3
   - Question 4
   - Question 5

Question 0

Consider elliptic curve $E_5(2,1)$ or in equation form as -

$$y^2 = x^3 + 2x + 1$$

If $P = (1,3)$ and $Q = (3,2)$ lie on the above curve, find $-2P + 2Q$.
Sol: We calculate 2P first.

$$\begin{aligned}
\lambda &= \frac{3 \cdot 1 + 2}{6} \\
&= 0 \\
x_R &= 0 - x_P - x_P \\
&= -2 = 3 \\
y_R &= 0(x_P - x_R) - y_P \\
&= -3 = 2
\end{aligned}$$

We calculate 2Q next.

$$\begin{aligned}\lambda &= \frac{3 \cdot 3 + 2}{4} \\ &= 2 \\ x_R &= 2 - x_Q - x_Q \\ &= -4 = 1 \\ y_R &= 2(x_Q - x_R) - y_Q \\ &= 2\end{aligned}$$

We get (3,2) thus, -2P is (3,-2) or (3,3) and 2Q is (1,2). Now we calculate -2P + 2Q.

$$\begin{aligned}\lambda &= \frac{2 - 3}{1 - 3} \\ &= 3 \\ x_R &= 3 - x_{-2P} - x_{2Q} \\ &= -1 = 4 \\ y_R &= 3(x_{-2P} - x_R) - y_{-2P} \\ &= -6 = 4\end{aligned}$$

Thus we get (4,4).

Question 1

What are the sets in the partition of the integers arising from congruence modulo 4?

Sol: We know the four congruence classes are $[0]_4, [1]_4, [2]_4, [3]_4$, i.e., integers which give remainder $0, 1, 2, 3$ when divided by 4:

$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$

$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

Question 2

Determine which one of these are equivalence and list their equivalence classes (if applicable). Also if it isn't an equivalence relation tell which property does it lack:

1. $\{(a, b)|a$ and b are the same age$\}$
   Sol: Equivalence. $[a]_R = \{b \in A|b$ has the same age as $a\}$
2. $\{(a, b)|a$ and b have the same parent$\}$
   Sol: Equivalence. $[a]_R = \{b \in A|b$ has the same parent as $a\}$
3. $\{(a, b)|a$ and b have met$\}$
   Sol: Not transitive.
4. $\{(a, b)|a$ and b speak a common language$\}$
   Sol: Not transitive

Question 3

3.1 Which of the following are partitions of $S = \{1, 2, 3, 4, 5, 6\}$:

1. $\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}$
   Sol: False. $\{1, 2\} \cap \{2, 3, 4\} \neq \phi$
2. $\{1\}, \{2, 3, 6\}, \{5\}, \{4\}$
   Sol; True. $\bigcup_{i=1}^{4} A_i = S$ and $A_i \cap A_j = \phi \ \forall i, j$

3.2 Which of the following are partitions of the set of real numbers:

1. Set of intervals $[k, k+1], k = \ldots -2, -1, 0, 1, \ldots$
   Sol: False. $[1, 2] \cap [2, 3] \neq \phi$, i.e. $[k, k+1] \cap [k+1, k+2] = \{k\} \ \forall k$
2. Set of intervals $(k, k+1), k = \ldots -2, -1, 0, 1, \ldots$
   Sol: False. $\bigcup_{k \in \mathbb{Z}} (k, k+1) \neq \mathbb{R}$. Actually it is the set $\mathbb{R} - \mathbb{Z}$
3. The sets $\{x + n | n \in \mathbb{Z}\}$ for all $x \in [0, 1)$
   Sol: True. x covers the real numbers between any 2 integers, and n expands it to all integers. Also $\{x + n_1\} \cap \{x + n_2\} = \phi \ \forall n_1, n_2 \in \mathbb{Z}$

Question 3

3.3 Verify whether it is a partitions of the set $\mathbb{Z} \times \mathbb{Z}$ of ordered pair of integers:
The set of pairs (x, y), where $3 \mid x$ and $3 \mid y$; the set of pairs (x, y), where $3 \mid x$ and $3 \nmid y$; the set of pairs (x, y) where $3 \nmid x$ and $3 \mid y$; the set of pairs (x, y) where $3 \nmid x$ and $3 \nmid y$
Sol: First partition: $(x, y) = (3p, 3q)\ p, q \in \mathbb{Z}$; Second partition: $(x, y) = (3p, 3q + r)\ p, q \in \mathbb{Z}, r = 1, 2$; Third partition: $(x, y) = (3p + r, 3q)\ p, q \in \mathbb{Z}, r = 1, 2$; Fourth partition: $(x, y) = (3p + r_1, 3q + r_2)\ p, q \in \mathbb{Z}, r_1, r_2 = 1, 2$.
Now, $P_i \cap P_j = \phi\ \forall i, j$ because $3m \neq 3n + r, r = 1, 2\ \forall m, n \in Z$ (now either x or y or both won't be satisfied in the intersect condition).
To show that the union of the partitions leads to $\mathbb{Z} \times \mathbb{Z}$ can be done in many ways. Consider constructing base examples and show that all possible integers can be represented by adding 3. Another way may be to pair up the partitions as ones where $x = y$ and $x \neq y$ and show that they represent that for all $x, y \in \mathbb{Z}$ and that their union gives all cases of $\mathbb{Z} \times \mathbb{Z}$

Question 4

4.1 Let R be the relation on the set of all people who have visited a particular Web page such that xRy if and only if person x and person y have followed the same set of links starting at this Web page (going from Web page to Web page until they stop using the Web). Find out the properties of the relation R.

4.2 a Let n be a positive integer. Show that the relation R on the set of all polynomials with real-valued coefficients of all pairs (f, g) such that $f^{(n)}(x) = g^{(n)}(x)$ is an equivalence relation. (Here $f^{(n)}(x)$ is the nth derivative of $f(x)$)

4.2 b Which functions are in the same equivalence class as the function $f(x) = x^4$, where $n = 3$?

Question 4 Solutions

4.1 Sol: Given, A = Set of all people who have visited a particular Web page

Reflexive Let $x \in A$

Since x always follows the same set of links like itself. Thus $(x, x) \in R$, Thus R is reflexive.

Symmetric Let $(x, y) \in R$.

This means that x and y follows the same link, then y and x follows the same links. Thus $(y, x) \in R$. Thus R is symmetric.

Transitive Let $(x, y) \in R$ and $(y, z) \in R$

This means that x and y followed the same link, and y and z followed the same link. Thus x and z followed the same links. Thus $(x, z) \in R$. Thus R is transitive

Thus R is an equivalence relation.

Question 4 Solutions

4.2 a Sol: Given, A = All polynomial functions with real-valued coefficients

Reflexive Let $f \in A$

Since $f^{(n)}(x) = f^{(n)}(x)$ for all $x \in R$. Thus $(f, f) \in R$. Thus R is reflexive.

Symmetric Let $(f, g) \in R$. This means $f^{(n)}(x) = g^{(n)}(x)$, By symmetry of the equality, we get $g^{*n)}(x) = f^{(n)}(x)$ which implies $(g, f) \in R$. Thus R is symmetric

Transitive Let $(f, g) \in R$ and $(g, h) \in R$. Then $f^{(n)}(x) = g^{(n)}(x) = h^{(n)}$. Thus $(f, h) in R$, Thus R is transitive.

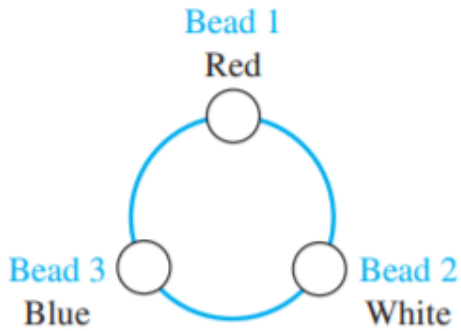
Therefore R is an equivalence relation.

4.2 b Sol: Given $f(x) = x^4$, then $f^{(2)}(x) = 12x^2$. Now for any $g(x)$ we have $g^{(2)}(x) = 12x^2$. Thus $g(x) = x^4 + ax + b$ (by integrating). Thus:

$$[f]_R = \{g \in A | g^{(2)} = 12x^2\} = \{g \in A | g(x) = x^4 + ax + b\}$$

*Question 5

Each bead on a bracelet with three beads is either red, white or blue:



Define the relation R between bracelets as: (B_1, B_2) where B_1 and B_2 are bracelets, belongs to R if and only if B_2 can be obtained from B_1 by rotating it or rotating it and then reflecting it.

- Show that R is an equivalence relation
- What are the equivalence classes for R