MODERN ALGEBRA I GU4041

Homework 2, due September 21: Equivalence relations, modular arithmetic

1. In each of the following situations, X is a set and R is a relation. Determine whether it is an equivalence relation by checking whether it satisfies each of the necessary conditions (reflexive, symmetric, transitive). Justify your answer. If R is an equivalence relation, give a simple description of the set of equivalence classes.

(a) $X = \mathbb{Z}$, aRb if $a + b$ is odd.

(b) $X = \mathbb{R}^3$, vRw if there is a rotation of X centered at the origin that takes v to w.

(c) X is the set of triangles in the plane, ARB if A and B are similar triangles.

(d) X is the set of real-valued functions on $\mathbb{R}$, fRg if $f(n) - g(n) \geq 0$ for any integer $n \in \mathbb{Z} \subset \mathbb{R}$.

2. Continuing problem 1, let X be the set of continuous real-valued functions on the interval $[0, 1]$. If $f, g, \in X$, say fRg if

$$\int_0^1 f(x)dx = \int_0^1 g(x)dx.$$

Prove that R is an equivalence relation and define a bijection between the set of equivalence classes for R and the set $\mathbb{R}$ of real numbers.

3. Represent the elements of $\mathbb{Z}_{17}$ by the residue classes $[0], [1], [2], [3], [4], [5], \ldots, [16]$. Then we can write multiplication with these representatives:

$$[5][5] = [25]; \ [10] \cdot [5] = [9].$$

A residue class $[n]$ is called a *quadratic residue* (modulo 17) if there is another integer d between 0 and 16 such that $[d] \cdot [d] = [n]$.

(a) Show that $[8]$ is a quadratic residue modulo 17.

(b) Give an example of a residue class that is *not* a quadratic residue modulo 17.

(c) Show that if $[n]$ and $[m]$ are quadratic residues, then so is $[m \cdot n]$.

(d) Show that if $[n]$ is a quadratic residue and $[m]$ is not a quadratic residue, then $[m \cdot n]$ is not a quadratic residue. (Hint: Suppose $[n] = [d] \cdot [d]$ and suppose $[m]$ is not a quadratic residue. Since 17 is a prime number, Bezout's theorem shows that there is a number f such that $[d] \cdot [f] = [1]$. Use this to obtain a contradiction.)

4. Use the Euclidean algorithm to determine the GCD and LCM for each of the following pairs of integers. (i) $n = 107$, $m = 865$. (ii) $n = 185$, $m = 5291$.

5. Judson book, Exercises 24, 25, section 2.4.

Recommended reading

Gallagher's notes, sections 1 and 2, at `https://www.math.columbia.edu/~khovanov/modAlgSpring2017/Gallagher/`.