Worksheet for Week 9

These questions are standard, but a little challenging and long, so they should be just fine for this week.

1. Let p be a prime number and let a, b be integers. Then prove that $p \mid ab \iff (p \mid a)$ or $(p \mid b)$.

   Hint: Bezout's lemma may be useful for one direction.

2. (old exam question) A relation R on $\mathbb{Z}$ is defined by aRb if $7a^2 \equiv 2b^2 \pmod 5$. Prove that R is an equivalence relation. Determine the distinct equivalence classes $[0]$ and $[1]$, simplify your answer as much as possible.

   Hint: The previous example will be useful here.

3. (old exam question) Let R be a relation on $\mathbb{R}$ defined as

   $$R = \left\{(x, y) : \cos^2(x) + \sin^2(y) = 1\right\}.$$

   Prove that R is an equivalence relation, and for $\theta \in \mathbb{R}$, write the equivalence class $[\theta]$.

   Hint: For the last part of the question, you can try to visualize it on the unit circle.

4. Define a relation, S, on $\mathbb{Z} \times \mathbb{N}$ as

   $$(x, y)S(a, b) \Leftrightarrow xb = ya.$$

   Show that S is an equivalence relation. Moreover, find the equivalence class of $(1, 3)$.

   Hint: How can you rewrite the relation equality?

   Before the following examples, watch videos 29 and 30 in `https://personal.math.ubc.ca/~PLP/auxiliary.html`.

5. Suppose P is a partition of a set A. Define a relation R on A by declaring xRy if and only if $x, y \in X$ for some $X \in P$. Prove R is an equivalence relation on A. Then prove that P is the set of equivalence classes of R.

   Hint: It may be useful to draw couple disjoint sets with elements and help them visualize it that way if need be.

6. Given $n \in \mathbb{N}$, let $[a]_n$ denote the equivalence class of a under the relation "congruence modulo n" on the integers. We define the *multiplicative inverse* of $[a]_n$ to be the equivalence class $[b]_n$ such that $[a]_n[b]_n = [1]_n$, if such an equivalence class exists. (Multiplicative inverses are nice because they allow us to perform "dividing by $[a]_n$" by multiplying by the multiplicative inverse of $[a]_n$).

   (a) Write down the multiplication table for the equivalence classes of the relation "congruence modulo 5". Show that every equivalence class $[k]_5$, where $k \not\equiv 0 \pmod 5$, has a multiplicative inverse.

   We see that multiplicative inverses of $[1]_5, [2]_5, [3]_5, [4]_5$ are $[1]_5, [3]_5, [2]_5, [4]_5$ respectively.

   (b) Prove that if $n \in \mathbb{N}$ is prime, then every nonzero integer modulo n has a multiplicative inverse.

   Hint: Again, Bezout's lemma.

7. (If there is time) Suppose that $n \in \mathbb{N}$ and $\mathbb{Z}_n$ is the set of equivalence class of congruent modulo n on $\mathbb{Z}$. In this question we will call an element $[u]_n$ invertible if it has a multiplicative inverse.

   Now, define a relation R on $\mathbb{Z}_n$ by xRy iff $xu = y$ for some invertible $[u]_n \in \mathbb{Z}_n$.

   (a) Show that R is a equivalence relation.

(b) Compute the equivalence classes of this relation for $n = 6$.

Hint: First find the invertible elements in $\mathbb{Z}_6$.

Before the following week, watch videos 31 and 32 in `https://personal.math.ubc.ca/~PLP/auxiliary.html`.