Math 4310 Homework 2 - Due February 8

Problem 1. Prove the following facts about congruences. (a) If $n \geq 1$ and a, b are integers, and $a \equiv b \pmod{n}$, then we have an equality of GCDs $\gcd(a, n) = \gcd(b, n)$.

(b) If p is a prime number and $x \in \mathbb{Z}$ satisfies $x^2 \equiv 1 \pmod{p}$, then either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Problem 2. Determine if the following functions are well-defined.

(a) The function $\mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/25\mathbb{Z}$ given by $[a] \mapsto [5a]$.

(b) The function $\mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/25\mathbb{Z}$ given by $[a] \mapsto [2a]$.

(c) The function $\mathbb{Q} \to \mathbb{Q}$ given by $a/b \mapsto (4a + 3)/4$.

(d) The function $\mathbb{Q} \to \mathbb{Q}$ given by $a/b \mapsto (a^2 + b^2)/ab$.

Problem 3. Prove the following facts about fields and vector spaces (using the axioms directly).

(a) If F is a field, it has a *unique* additive identity. (The definition I gave requires that there *exists* an additive inverse 0 satisfying $a + 0 = a$, but we need to justify that there isn't a second element $0'$ satisfying $a + 0' = a$).

(b) If F is a field, for each $a \in F$ there exists a *unique* additive inverse $-a$.

(c) If F is a field and $a \in F$, its additive inverse $-a$ is equal to $(-1) \cdot a$.

(c) If F is a field and V is a vector space, and $a \in F$ and $v \in V$ are elements such that $av = 0$, then either $a = 0$ in F or $v = 0$ in V.

Problem 4. If $\sim$ is an equivalence relation on a set A, we showed that if $a, b \in A$ then the set of equivalence classes $A/\sim$ is a set of subsets of A satisfying the following two properties:

- Two distinct elements of $A/\sim$ are disjoint subsets of A: if $[a], [b]$ are different equivalence classes then $[a] \cap [b] = \emptyset$.
- The union of all of the elements of $A/\sim$ (which are all subsets of A) equals A itself.

If $\mathcal{P}$ is any set of subsets of A satisfying these two properties (that distinct elements of $\mathcal{P}$ are disjoint, and the union of all elements of $\mathcal{P}$ is all of A) we call $\mathcal{P}$ a *partition*.

Summarizing the above, we can say that every equivalence relation $\sim$ gives rise to a partition of A (namely the set $A/\sim$). Prove the converse: for any partition $\mathcal{P}$, there is an equivalence relation $\sim$ that gives rise to $\mathcal{P}$, i.e. such that $\mathcal{P} = A/\sim$.

Problem 5. In the Fields handout we defined the *characteristic* of a field as the smallest integer $n > 0$ such that $n_F = 0$ (and defined the characteristic to be zero if there was no such n). Prove that the characteristic of a field is always either 0 or a prime number.

Problem 6. Let $\mathcal{F}(\mathbb{R}, \mathbb{R})$ be the set of all functions $\mathbb{R} \to \mathbb{R}$; we can make this set into a commutative ring by defining addition and multiplication pointwise, i.e. if $f, g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ we define $f + g, fg \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ by

$$(f + g)(x) = f(x) + g(x) \qquad (fg)(x) = f(x)g(x).$$

Is $\mathcal{F}(\mathbb{R}, \mathbb{R})$ a field? What about the subset $\mathcal{C}(\mathbb{R}, \mathbb{R})$ consisting only of continuous functions?

(No extended glossary this week)