Mathematics 2200H – Mathematical Reasoning
TRENT UNIVERSITY, Fall 2023

Assignment #8
Equivalence Classes and Linear Equations
Due on Friday, 10 November.[*]

Recall that $\equiv$ is an *equivalence relation* on a set S if it is a binary relation on S that is:

1. *reflexive* – for all $s \in S$, $s \equiv s$,
2. *symmetric* – for all s, $t \in S$, $s \equiv t$ if and only if $t \equiv s$, and
3. *transitive* – for all s, t, $u \in S$, if $s \equiv t$ and $t \equiv u$, then $s \equiv u$.

The $\equiv$-*equivalence class* of $s \in S$ is $[s]_\equiv = \{\, t \in S \mid s \equiv t \,\}$.

1. Suppose S is a set, $\equiv$ is an equivalence class on S, and a, $b \in S$. Show that either $[a]_\equiv = [b]_\equiv$ or $[a]_\equiv \cap [b]_\equiv = \emptyset$. *[4]*

In the following, we (technically) work in $\mathbb{Z}_n$, the integers modulo n. (This needs $n \geq 2$ to avoid trivialities.) Recall that, officially, $\mathbb{Z}_n = \{\, [a]_n \mid a \in \mathbb{Z} \,\}$, where $[a]_n$ is the equivalence class of a for the equivalence relation $\equiv_n$ given by $a \equiv_n b$ if and only if $a = b + kn$ for some $k \in \mathbb{Z}$. ecall also that we defined addition and multiplication in $\mathbb{Z}_n$ by $[a]_n + [b]_n = [a+b]_n$ and $[a]_n \cdot [b]_n = [a \cdot b]_n$; these operations are then associative and commutative, and also satisfy the distributive laws.

In practice, as we do below, it is common to write $a = b \pmod{n}$ or $a \equiv b \pmod{n}$ for $a \equiv_n b$, where a, $b \in \mathbb{Z}$, and ignore the equivalence class notation, simply writing a for $[a]_\equiv$.

2. Suppose a, $b \in \mathbb{Z}$ with $\gcd(a, n) = d$. Show that if $d \nmid b$, then the equation $ax = b \pmod{n}$ has no solution $x \in \mathbb{Z}_n$. *[3]*

3. Suppose a, $b \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Show that the equation $ax = b \pmod{n}$ has exactly one solution $x \in \mathbb{Z}_n$. *[3]*

NOTE. In fact, the result in **3** can be extended to say that if $\gcd(a, n) = d$ and $d \mid b$, then $ax = b \pmod{n}$ has exactly d solutions in $\mathbb{Z}_n$.

---

[*] Please submit your solutions via Blackboard's Assignments module, preferably as a single pdf. If submission on Blackboard fails, please submit your solutions to the instructor on paper or via email to `sbilaniuk@ trentu.ca` as soon as you can.