Mathematics 2200H – Mathematical Reasoning
Trent University, Fall 2025

Assignment #9
Equivalence Classes and Modular Arithmetic
Due on Friday, 14 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]*

Solution. We need to show that $[a]_\equiv = [b]_\equiv$ or $[a]_\equiv \cap [b]_\equiv = \emptyset$ is true; it is sufficient to show that if the latter alternative fails, then the former is true.

Suppose, then, that $[a]_\equiv \cap [b]_\equiv \neq \emptyset$, *i.e.* there is some $c \in S$ such that $c \in [a]_\equiv \cap [b]_\equiv$. Since $c \in [a]_\equiv$, we have $c \equiv a$, and since $c \in [b]_\equiv$, we also have $c \equiv b$. It follows by the symmetry and transitivity of $\equiv$ that $a \equiv b$. Now, for all $x \in S$, since we have $a \equiv b$ and $\equiv$ is transitive, $x \equiv a$ if and only if $x \equiv b$. Then $x \in [a]_\equiv \iff x \equiv a \iff x \equiv b \iff x \in [b]_\equiv$, so $[a]_\equiv = [b]_\equiv$ by the Axiom on Extensionality. $\square$

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]*

Solution. Since $\gcd(a, n) = d$ is a divisor of a and n, there exist s, $t \in \mathbb{Z}$ such that $a = sd$ and $n = td$.

Suppose, by way of contradiction, that we did actually have a solution x to $ax = b \pmod{n}$, *i.e.* $ax = b + rn$ for some $r \in \mathbb{Z}$. Then we would have $b = ax - rn = sdx - rtd = d(sx - rt)$, which would imply that $d \mid b$, contradicting the given fact that $d \nmid b$. Thus $ax = b \pmod{n}$ cannot have a solution. $\square$

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]*

Solution. We need to show two things. First, that $ax = b \pmod{n}$ has a solution, and, second, that it has only one solution modulo n.

By the result in question 1 of Assignment #7, since $\gcd(a, n) = 1$, there exist s, $t \in \mathbb{Z}$ such that $as + nt = 1$, so $as = 1 - nt$. Let $x = sb$. Then $ax = asb = (1 - nt)b = b - btn$, so $ax = b \pmod{n}$. Thus the equation $ax = b \pmod{n}$ has a solution.

Now suppose that x and y are two solutions to the equation, *i.e.* $ax = b \pmod{n}$ and $ay = b \pmod{n}$. It follows that $a(x-y) = ax - ay = b - b = 0 \pmod{n}$. Recall from the previous paragraph that $as + nt = 1$, so $as = 1 \pmod{n}$. Then

$$\begin{aligned} x - y &= 1(x-y) \pmod{n} \\ &= as(x-y) \pmod{n} \\ &= sa(x-y) \pmod{n} \\ &= s \cdot 0 \pmod{n} \\ &= 0 \pmod{n}, \end{aligned}$$

from which it follows that $x = y \pmod{n}$.

Thus if $a, b \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then the equation $ax = b \pmod{n}$ has exactly one solution x modulo n, as required. ■

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 $\mathbb{Z}_n$.