WORKSHEET #2 – MATH 311W

SEPTEMBER 17TH, 2012

Suppose that $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. Recall that we write $a \equiv_n b$ (or $a \equiv b$ modulo n) if $n|(a-b)$. In this worksheet, we'll explore this *relation* in more detail.

1. Suppose $a \equiv_n b$ and $c \in \mathbb{Z}$. Prove that

(a) $a + c \equiv_n b + c$.
(b) $a - c \equiv_n b - c$.
(c) $a \cdot c \equiv_n b \cdot c$.

2. Division doesn't even make sense of course, because $1/5$ isn't an integer. However, we can ask a more fundamental question. Given an equation $a \cdot x \equiv_n b$, does there exist an integer x that solves the equation? Find *all* solutions to the following equations or show that there is no solution.

(a) $2x \equiv_4 1$.
(b) $2x \equiv_4 0$.
(c) $2x \equiv_5 1$.
(d) $3x \equiv_5 2$.
(e) $x^2 \equiv_4 3$.

Now we move onto a harder topic. The *equivalence class of a modulo n*, denoted $[a]_n$ is defined to be the set $\{x | x \equiv_n a\}$.

3. Prove that if $y, z \in [a]_n$ then $y \equiv_n z$ and also that $[y]_n = [a]_n = [z]_n$. In this case, we say that x, y and a are all representatives of the same equivalence class.

4. Show that every equivalence class $[a]_n$ has a representative r (in other words, such that $[r]_n = [a]_n$) satisfying the property $0 \leq r < n$.

For any two equivalence classes $[a]_n$ and $[b]_n$, we *DEFINE* the following addition and multiplication operations.

$$[a]_n + [b]_n = [a+b]_n \text{ and } [a]_n \cdot [b]_n = [a \cdot b]_n \tag{$\dagger$}$$

We need to prove that these operations are *well defined.* This means that they do not depend on the choice of representative of the equivalence class. For example, consider the following function which is not well defined

$$f(x) = \text{ ``3rd digit in the decimal expansion of } x\text{''}.$$

Since $1.0 = 0.999\ldots$, we have that both $f(x) = 0$ and $f(x) = 9$. This is impossible, so our original f was not even a function. We *need* to worry about a similar thing here.

5. Show that the operations $+$ and $\cdot$ are well defined on equivalence classes by doing the following. Suppose that $[b]_n = [c]_n$. Prove that ($\dagger$) is well defined by proving that

$$[a]_n + [c]_n = [a]_n + [b]_n$$

and likewise with multiplication. Note, you CANNOT cancel the $[a]_n$ from both sides (yet). The "+" operation above is not the ordinary addition of numbers, it is addition of equivalence classes as defined in ($\dagger$).