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) $a \cdot c \equiv_n b \cdot c$.

Solution: For (a), we know $n|(a-b)$. But $a - b = (a+c) - (b+c)$ so $n|((a+c)-(b+c))$ and the result follows.

For (b), again we know $n|(a-b)$ and so then $n|((a-c)-(b-c))$ and the result follows.

Finally for (c), since $n|(a-b)$, then certainly $n|(c(a-b))$ but thus $n|(c \cdot a - c \cdot b)$ and the result follows.

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) $x^2 \equiv_4 3$.

Solution: For (a), there are no solutions. For this, based on the theorem in the book we simply must observe that $2 = \gcd(2, 4)$ can never divide 1 since this latter integer is odd.

For (b), certainly $x = 2$ is a solution. In fact, any even integer is a solution since if $x = 2k$, then $2 \cdot (2k) = 4k \equiv_4 0$. Odd x do not yield solutions though.

For (c), there is a solution again if and only if $1 = \gcd(2, 5)$ divides 1, but this always happens, so there is a solution. Since 2 is invertible modulo 5, and $[2]^{-1} = 3$, we see that x is a solution to $2x \equiv_5 1$ if and only if $x = 3 \cdot 2 \cdot x \equiv_5 3$. Thus the solutions are $\{\ldots, -2, 3, 8, 13, 18, \ldots\}$.

For (d), we work as above. We see that x is a solution to $3x \equiv_5 2$ if and only if $x = 2 \cdot 3x \equiv_5 2 \cdot 2 = 4$ (again, this is reversible since 2 is invertible). Thus the solutions are $\{\ldots, -1, 4, 9, 14, 19, \ldots\}$.

For (e), it's a little more complicated. There are no solutions and here's how you see it. If x is even, then $x = 2k$ so that $x^2 = 4k^2 \equiv_4 0$ and so can't be 3. On the other hand, if x is odd, $x = 2k + 1$, then $x^2 = 4k^2 + 4k + 1 \equiv_4 1$ which is also not 3, so no matter what x is, x^2 can't be equivalent to 3 modulo 4.

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.

Solution: For the first part, we observe that $[y]_n$ is everything with the same remainder as y (when divided by n). Likewise $[z]_n$ is everything with the same remainder as z (when divided by n). But y and z and a all have the same remainder, and so $y \equiv_n z$ and also $[y]_n = [a]_n = [z]_n$ as desired.

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

Solution: Write $a = qn + r$ with $0 \leq r < n$. Then $r \equiv_n a$ since n divides $qn = a - r$. Thus we have found our r.

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 ($\dagger$).

Solution: We need to show that $[a + c]_n = [a]_n + [c]_n$ is equal to $[a + b]_n = [a]_n + [b]_n$. It is sufficient to show that $n|((a+b) - (a+c))$ but this follows immediately since $(a+c) - (a+b) = c - b$ and we know $n|(c - b)$ since $[b]_n = [c]_n$. This proves the result for “+”.

For multiplication, we need to show that $[a]_n \cdot [c]_n = [a \cdot c]_n$ is equal to $[a]_n \cdot [b]_n = [a \cdot b]_n$. Thus we need to show that n divides $ac - ab = a(c - b)$. But we already know that n divides $c - b$ (since $[c]_n = [b]_n$) and thus n divides $ac - ab$ as well. This completes the proof.