Math 3110 **Test #1 — ANSWER KEY** **February 19th, 2009**

1. (15 points) Define a binary operation "$\star$" on $\mathbb{Z}$, as follows $x \star y = -xy$ (for all $x, y \in \mathbb{Z}$). So, for example, $2 \star (-3) = -2(-3) = 6$.

(a) Is $\mathbb{Z}_{>0}$ (the set of positive integers) closed with respect to $\star$? Justify your answer.

Answer: No. Consider $2 \in \mathbb{Z}_{>0}$, $2 \star 2 = -2(2) = -4 \notin \mathbb{Z}_{>0}$ so $\mathbb{Z}_{>0}$ is not closed under $\star$.

(b) Is $\star$ is an associative? Why or why not?

Let $a, b, c \in \mathbb{Z}$. $(a \star b) \star c = (-ab) \star c = -(-ab)c = abc$ and $a \star (b \star c) = a \star (-bc) = -a(-bc) = abc$ therefore $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in \mathbb{Z}$.

Answer: Yes. $\star$ is associative.

(c) Show that -1 is an identity for $\star$.

Let $a \in \mathbb{Z}$. $-1 \star a = -(-1)a = a$ and $a \star (-1) = -a(-1) = a$ therefore $(-1) \star a = a = a \star (-1)$ for all $a \in \mathbb{Z}$.

2. (14 points) Consider $\mathbb{Z}$ with some relation R. Also, let $a, b \in \mathbb{Z}$.

(a) Let $a\mathrm{R}b$ if and only if $a \leq b$. R is **not** an equivalence relation. Why?

R $= \leq$ is reflexive (since $x \leq x$) and transitive (since $x \leq y$ and $y \leq z$ implies that $x \leq z$), but $\leq$ is **not** symmetric.
$1 \,\mathrm{R}\, 2$ since $1 \leq 2$. But $2 \not\mathrm{R}\, 1$ since $2 \not\leq 1$. So R is not an equivalence relation since it is not symmetric.

(b) Let $a\mathrm{R}b$ if and only if $a - b$ is divisible by 2. Then R is an equivalence relation.
Describe the equivalence classes.

$a - b$ divisible by 2 is the same as $a \equiv b \pmod 2$. So the equivalence classes are the even integers $(= [0] = \{\dots, -2, 0, 2, 4, \dots\})$ and the odd integers $(= [1] = \{\dots, -1, 1, 3, \dots\})$.
Alternatively, notice that $a - b$ divisible by 2 means that a and b are off by an even number. And since even + even = even and odd + even = odd, we get two equivalence classes. Namely, $\mathbb{E} = 2\mathbb{Z} = \{2n \,|\, n \in \mathbb{Z}\}$ (the even integers) and $\mathbb{O} = \mathbb{Z} - 2\mathbb{Z} = 2\mathbb{Z} + 1 = \{2n + 1 \,|\, n \in \mathbb{Z}\}$ (the odd integers).

3. (15 points) Let $f : A \to A$ and $g : A \to A$ for some (non-empty) set A.

(a) Define "f is onto".

Quick Answer: Range = Codomain (that is $f(A) = A$).

Longer Answer: For all $y \in A$ there exists an $x \in A$ such that $f(x) = y$.

(b) Suppose that f and g are both one-to-one. Show that $f \circ g$ is one-to-one.

The Wordy Proof:
Let $x, y \in A$ and suppose that $(f \circ g)(x) = (f \circ g)(y)$. Then $f(g(x)) = f(g(y))$ (by the definition of function composition) and thus $g(x) = g(y)$ (since f is one-to-one). But g is one-to-one, therefore, $x = y$. Thus for all $x, y \in A$, $(f \circ g)(x) = (f \circ g)(y)$ implies that $x = y$, so $f \circ g$ is one-to-one.

A Less Wordy Proof:
$x, y \in A$ suppose $(f \circ g)(x) = (f \circ g)(y)$ implies $f(g(x)) = f(g(y))$ implies $g(x) = g(y)$ (since f injective) implies $x = y$ (since g injective). Therefore, $f \circ g$ is injective.

(c) Let $h : \mathbb{Z} \to \mathbb{Z}$ where $h(x) = 2x + 1$. Is h one-to-one? Is h onto?

Let $x, y \in \mathbb{Z}$ and suppose that $h(x) = h(y)$. Then $2x + 1 = 2y + 1$ and so $2x = 2y$ thus $x = y$. Therefore, h is one-to-one.

Obviously, h is not onto since its range is the set of odd integers. [A "proof" h is not onto: suppose $h(x) = 0$ then $2x + 1 = 0$ and so $x = -1/2$. But $-1/2 \notin \mathbb{Z}$ and therefore 0 is not in the range of h so h is not onto.]

4. (14 points) Prove **one** of the following (choose I. or II.):

I. Let U be a set, $A \subseteq U$, and $B \subseteq U$. Show that $(A \cap B)' = A' \cup B'$.
(Recall $X' = U - X$ is the complement of X in U.)

II. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all $n \geq 1$.

I. Let $x \in (A \cap B)'$ therefore $x \notin A \cap B$ so x is not in both A and B. So either x is not in A or x is not in B. This implies that $x \in A'$ or $x \in B'$ so that $x \in A' \cup B'$. Therefore, $(A \cap B)' \subseteq A' \cup B'$.

Conversely, supppose that $x \in A' \cup B'$ this implies that either $x \notin A$ or $x \notin B$. Thus x cannot be a member of both A and B. This means that $x \notin A \cap B$ which means $x \in (A \cap B)'$. Therefore, $(A \cap B)' \subseteq A' \cup B'$.

So we can conclude that $(A \cap B)' = A' \cup B'$.

II. Informally Consider the base case $n = 1$: $1 = 1^2$. So the base case holds.

Now suppose that $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ for some $k \geq 1$. Then $1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1)$. But $k^2 + (2(k + 1) - 1) = k^2 + 2k + 1 = (k + 1)^2$. Therefore, $1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2$. So if the equation holds for some positive integer k, then it also holds for $k + 1$. Therefore, by induction, the equation holds for all $n \geq 1$.

II. A Formal Approach Let $S = \{n \in \mathbb{Z}_{>0} \mid 1 + 3 + 5 + \cdots + (2n - 1) = n^2\}$. Notice that $1 = 1^2$ so that $1 \in S$.

Now suppose that $k \in S$. Thus $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ (where $k \geq 1$). Then $1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1)$ (we just added $(2(k + 1) - 1)$ to both sides of the previous equation). Note that $k^2 + (2(k + 1) - 1) = k^2 + 2k + 1 = (k + 1)^2$. Thus $1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2$ which means that $k + 1 \in S$.

We have shown that $1 \in S$ and $k \in S$ implies that $k + 1 \in S$. Therefore, S is an inductive set and so (by induction) $S = \mathbb{Z}_{>0}$. This means that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ holds for all $n \geq 1$.

5. (14 points) Division.

(a) Let $a, b \in \mathbb{Z}$. Define $a \mid b$.

$a \mid b$ if and only if there exists $n \in \mathbb{Z}$ such that $an = b$.

Alternatively, $a \mid b$ if and only if b is an integer multiple of a.

(b) Let $a, b, c \in \mathbb{Z}$. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

$a \mid b$ and $b \mid c$ so there exist integers m and n such that $am = b$ and $bn = c$. Therefore, $a(mn) = (am)n = bn = c$ and so c is an integer multiple of a (since mn is an integer). Therefore, $a \mid c$.

6. (14 points) The Euclidean Algorithm and Congruences.

(a) Use the Euclidean algorithm to find $(20, 12) = d$. Then use the Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that $12x + 20y = d$.

$$\begin{array}{r|l} & 1 \\ \hline 12 & 20 \\ & -12 \\ \hline & 8 \end{array} \qquad \begin{array}{r|l} & 1 \\ \hline 8 & 12 \\ & -8 \\ \hline & 4 \end{array}$$

So we have that $12 - 8 = 4$ substituting in $20 - 12 = 8$ we get $12 - (20 - 12) = 4$ and thus...
Answer: $2 \cdot 12 + (-1) \cdot 20 = 4$

(b) Consider the equation: $12x \equiv 3 \pmod{20}$. If possible, find a solution x such that $0 \leq x < 20$. Otherwise, explain why there is no such solution.

Solving this equation is equivalent to finding $x, q \in \mathbb{Z}$ such that $12x + 20q = 3$. This is only possible if 3 is a multiple of $(12, 20) = 4$. So since 4 does not divide 3 there is **no solution**.

(c) Consider the equation: $12x \equiv 8 \pmod{20}$. If possible, find a solution x such that $0 \leq x < 20$. Otherwise, explain why there is no such solution.

Solving this equation is equivalent to finding $x, q \in \mathbb{Z}$ such that $12x + 20q = 8$. We already know (from part (a)) that $2 \cdot 12 + (-1) \cdot 20 = 4$ multiplying through by 2 we get $4 \cdot 12 + (-2) \cdot 20 = 8$. Therefore, $4 \cdot 12 \equiv 8 \pmod{20}$. So $x = 4$ is a solution.
Note: This is not the only solution. Dividing $12x + 20q = 8$ by 4 we have an equivalent equation $3x + 5q = 2$ which is $3x \equiv 2 \pmod{5}$. $3^{-1} \bmod 5$ is 2 (since $3 \cdot 2 \equiv 1 \pmod{5}$). So (working mod 5), $x = 3^{-1}3x = 3^{-1}2 = 2 \cdot 2 = 4$. Thus $x = 4 + 5q$ is a solution for any $q \in \mathbb{Z}$. In particular, $x = 4, 9, 14, 19$ are all of the solutions of $12x \equiv 8 \pmod{20}$ where $0 \leq x < 20$.

7. (14 points) Workin' mod 4.

(a) Fill out the following tables (don't worry about brackets for equivalence classes.)

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$ Addition Table

$(\mathbb{Z}_4, \times)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_4$ Multiplication Table

(b) What is $-1 \pmod 4$? $1 + 3 = 0 \pmod 4$ so $-1 = 3$.

(c) What is $3^{-1} \pmod 4$? $3 \cdot 3 = 1 \pmod 4$ so $3^{-1} = 3$.

(d) Compute $3^{-1}(3 + 2) - 1 \pmod 4$.

$(\underline{3^{-1}})(3 + 2) - 1 = \underline{3}(\underline{\underline{3 + 2}}) + (-1) = 3(\underline{1}) + (-1) = 3 + (\underline{-1}) = 3 + \underline{3} = 2 \pmod 4$
..or..
$3^{-1}(5) - 1 = 3(5) - 1 = 15 - 1 = 14 = 2 \pmod 4$