Math 3110 **Test #1 — ANSWER KEY** **September 30th, 2009**

1. (18 points): Define a binary operation "$\star$" on $\mathbb{Z}$, as follows $x \star y = x + xy + y$ (for all $x, y \in \mathbb{Z}$). So, for example, $(-2) \star (-3) = (-2) + (-2)(-3) + (-3) = 1$.

(a) Show $\star$ is associative.

Let $x, y, z \in \mathbb{Z}$. Then $(x \star y) \star z = (x+xy+y) \star z = x+xy+y+(x+xy+y)z+z = x+y+z+xy+xz+yz+xyz$ and $x \star (y \star z) = x \star (y + yz + z) = x + x(y + yz + z) + y + yz + z = x + y + z + xy + xz + yz + xyz$. Since the two expressions match, we have that $(x \star y) \star z = x \star (y \star z)$. Therefore, $\star$ is associative.

(b) Show 0 is the identity for $\star$.

Let $x \in \mathbb{Z}$. $x \star 0 = x + x0 + 0 = x$ and $0 \star x = 0 + 0x + x = x$. Thus 0 is an identity for $\star$.

(c) Is the set of negative integers $\mathbb{Z}_{<0}$ closed with respect to $\star$? Why or why not?

No. The example above $(-2) \star (-3) = (-2) + (-2)(-3) + (-3) = 1 \notin \mathbb{Z}_{<0}$ shows that the set of negative integers is not closed under the operation $\star$.

2. (20 points): Consider the set $S = \{a, b, c, d, e, f, g\}$. Recall that $\mathcal{P}(S) = \{A \mid A \subseteq S\}$ is the *power set* of S (i.e. the set of all subsets).

(a) Which of the following are true?

i. $\{a, b, c\} \in \mathcal{P}(S)$ **True**. Since $\{a, b, c\} \subseteq S$, this set is an element of the power set of S.

ii. $a, b, c \in \mathcal{P}(S)$ **False**. $a, b, c \in S$. These are elements of S not subsets, so they do not belong to the power set of S.

iii. $\phi = \{\} \in \mathcal{P}(S)$ **True**. The empty set is a subset of S. Thus it is an element of the power set of S.

iv. $\phi = \{\} \subset \mathcal{P}(S)$ **True**. In fact, the empty set is a subset of **EVERY** set.

v. $\{a, b, c\} \subseteq \mathcal{P}(S)$ **False**. $\{a, b, c\}$ is an element of the power set of S, not a subset of the power set. A subset of the power set of S would be a collection of subsets of S (like the next part).

vi. $\{\{a, b\}, \{d, e, f\}\} \subseteq \mathcal{P}(S)$ **True**. Each element of this set is a subset of S which means each element this set is an element of the power set of S. So by definition it is a subset of the power set of S.

(b) Define a relation on $\mathcal{P}(S)$ by A is related to B if and only if $A \subseteq B$. Is this an equivalence relation? Why or why not?

No. This relation is reflexive (since for all $A \in \mathcal{P}(S)$, $A \subseteq A$) and it's transitive (since if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$). But the relation is **not symmetric** since $A \subseteq B$ does not imply that $B \subseteq A$. For example, $\{a\} \subseteq \{a, b, c\}$ but $\{a, b, c\} \not\subseteq \{a\}$.

3. (22 points): Let $f : A \to A$ and $g : A \to A$ for some (non-empty) set A.

(a) Suppose that f and g are both onto. Prove that $f \circ g$ is onto.

Given an arbitrary element of the codomain (that is A), we need to find an element of the domain (again A) which maps to it. To do this we need to "peel off" f first (using the fact that it's onto) and then "peel off" g (using the fact that it's onto as well).

Suppose $y \in A$. We know that f is onto, so there exists some $a \in A$ such that $f(a) = y$. We also know that g is onto, so there exists some $x \in A$ such that $g(x) = a$. Thus $(f \circ g)(x) = f(g(x)) = f(a) = y$ so $f \circ g$ maps x to y. Therefore y is in the range. Since y was arbitrary, we have shown that the range of $f \circ g$ is all of A and thus $f \circ g$ is onto.

(b) Let $h : \mathbb{Z} \to \mathbb{Z}$ where $h(x) = \begin{cases} x/2 & x \text{ is even} \\ x & x \text{ is odd} \end{cases}$.
Is h one-to-one? Is h onto?

Let's try some "experiments" first. $h(-2) = -1$, $h(-1) = -1$, $h(0) = 0$, $h(1) = 1$, $h(2) = 1$, $h(3) = 3$, $h(4) = 2$.

From our calculations here we can see that $h(-2) = -1 = h(-1)$. Therefore, h is **not one-to-one**. On the other hand, it looks like h might be onto. In fact, it seems that the even inputs are the ones which "make" h onto. So let's use the even part of the formula to try to prove h is onto.

Scratch work: $x/2 = y \Rightarrow x = 2y$.

Proof: Suppose $y \in \mathbb{Z}$. Note that $2y$ is even. Therefore, we use the even part of the formula for h and get $h(2y) = (2y)/2 = y$. Thus y is in the range of h. Therefore, the range of h contains all integers which means h is **onto**.

4. (12 points): Let $f : A \to B$. Also, let $S_1, S_2 \subseteq A$ and $T \subseteq B$. Prove **one** of the following:

$$f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2) \qquad \text{OR} \qquad f(f^{-1}(T)) \subseteq T$$

I. $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$

Suppose $x \in f(S_1 \cap S_2)$. This implies there exists some $s \in S_1 \cap S_2$ such that $f(s) = x$. But $s \in S_1$ so that $x = f(s) \in f(S_1)$ and $s \in S_2$ so that $x = f(s) \in f(S_2)$. Therefore, $x \in f(S_1) \cap f(S_2)$.

Note: These sets are not always equal. Take for example, $f(x) = x^2$. $f(\{-1\} \cap \{1\}) = f(\phi) = \phi$ (empty). Whereas, $f(\{-1\} \cap f(\{1\}) = \{1\} \cap \{1\} = \{1\}$ (not empty). In fact, these sets are equal for all choices of S_1 and S_2 if and only if f is one-to-one (try to prove it).

II. $f(f^{-1}(T)) \subseteq T$

Suppose $x \in f(f^{-1}(T))$. This implies there exists some $y \in f^{-1}(T)$ such that $f(y) = x$. Remember that by definition, $y \in f^{-1}(T)$ if and only if $f(y) \in T$. Therefore, $x = f(y) \in T$.

Note: Again, these sets don't have to be equal. In fact, they are equal for all choices of T if and only if f is onto (challenge – try to prove this). To see that they don't need to be equal take $f(x) = x^2$ (mapping from $\mathbb{R}$ to $\mathbb{R}$. $f^{-1}(\{-1\}) = \phi$ (no real number squared is -1). So $f(f^{-1}(\{-1\})) = f(\phi) = \phi \subsetneq \{-1\}$.

5. (12 points): Prove by induction that 5 divides $6^n - 1$ for all positive integers n.
YOU MUST USE INDUCTION.

When $n = 1$ we see that $6^1 - 1 = 5$ which is divisible by 5 (thus the base case holds).

Assume 5 divides $6^n - 1$ for some positive integer n. So there exists some $k \in \mathbb{Z}$ such that $6^n - 1 = 5k$. Consider $6^{n+1} - 1 = 6(6^n) - 1 = 6(6^n - 1 + 1) - 1 = 6(5k + 1) - 1 = 6(5k) + 6 - 1 = 6(5k) + 5 = 5(6k + 1)$. Thus if 5 divides $6^n - 1$, it must also divide $6^{n+1} - 1$.

Therefore, by induction 5 divides $6^n - 1$ for all positive integers n.

6. (16 points): Division and Euclid.

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

$a \mid b$ implies that there exists some $k \in \mathbb{Z}$ such that $ak = b$ and $c \mid d$ implies that there exists some $\ell \in \mathbb{Z}$ such that $c\ell = d$. Therefore, $(ac)(k\ell) = (ak)(c\ell) = bd$ thus $ac \mid bd$.

(b) Use the Euclidean Algorithm to compute the $d = (96, 42)$ (the GCD of 96 and 42). Then use the Euclidean Algorithm (running it backwards) to find $x, y \in \mathbb{Z}$ such that $42x + 96y = d$.

Divide 96 by 42 and get: $96 = 2 \cdot 42 + 12$.

Divide 42 by 12 and get: $42 = 3 \cdot 12 + 6$.

Divide 12 by 6 and get: $12 = 2 \cdot 6 + 0$.

Since 6 is the last non-zero remainder, the Euclidean algorithm says that 6 is the greatest common divisor of 96 and 42.

Now, reading backwards, we see that $6 = (-3) \cdot 12 + 1 \cdot 42$ and $12 = (-2) \cdot 42 + 1 \cdot 96$. Replace the 12 in the first equality with the right-hand-side of the second equality and get $6 = (-3) \cdot ((-2) \cdot 42 + 1 \cdot 96) + 1 \cdot 42$ so that $6 = 6 \cdot 42 + (-3) \cdot 96 + 1 \cdot 42$. Therefore, $7 \cdot 42 + (-3) \cdot 96 = 6$ ($x = 7$ and $y = -3$).