Math 3110 **Test #1** **February 22nd, 2010**

Name: ANSWER KEY

Don't merely state answers, prove your statements. **Be sure to show your work!**

1. (10 points) Let $S = \mathbb{R} - \{0\}$ (the set of non-zero reals). For $x, y \in S$, define $x \star y = x^{-1}y$. [Example: $5 \star 10 = 10/5 = 2$]

(a) Is S closed with respect to $\star$?

Yes. Suppose that $x, y \in S$. This means that x and y are non-zero real numbers. Thus $x^{-1} = 1/x$ is a non-zero real number and so $x \star y = x^{-1}y$ is a non-zero real number (a non-zero real times a non-zero real is a non-zero real). Thus $x \star y \in S$.

(b) The operation $\star$ is **not** associative. Give a example which shows this.

To show $\star$ fails to be associative, we need to find a single example where associativity does not work. Let's try (somewhat randomly) $3, 2, 1 \in S$. Then $(3 \star 2) \star 1 = (3^{-1}2) \star 1 = (2/3) \star 1 = (2/3)^{-1}1 = 3/2$ whereas $3 \star (2 \star 1) = 3 \star (2^{-1}1) = 3 \star (1/2) = 3^{-1}(1/2) = 1/6$. Thus $(3 \star 2) \star 1 \neq 3 \star (2 \star 1)$. Thus $\star$ is not associative.

Note: In general, $x \star y = x^{-1}y = y/x$ so $x \star (y \star z) = x \star (z/y) = (1/x)(z/y) = z/(xy)$ whereas $(x \star y) \star z = (y/x) \star z = (x/y)z = (zx)/y$. Thus any numbers x, y, z where $x \neq \pm 1$ would have worked.

2. (15 points) Here are 3 collections of subsets of $\mathbb{Z}$. 2 of these collections are **not** partitions – **explain why they fail to be partitions**. 1 of these collections is a partition – **describe the corresponding equivalence relation**.

(a) $\{-1, -2, -3, \dots\}$ and $\{1^2, 2^2, 3^2, 4^2, \dots\}$

A partition is a collection of non-empty, disjoint subsets, which when unioned together give the whole set. Notice that $\{-1, -2, \dots\} \cup \{1^2, 2^2, \dots\} = \{\dots, -3, -2, -1, 1, 4, 9, 16, \dots\}$ is missing a lot of integers [In particular, 0 is missing]. So these sets do not form a partition of $\mathbb{Z}$.

(b) $\{\dots, -6, -3, 0, 3, 6, 9, \dots\} = \{3k \mid k \in \mathbb{Z}\}$,
$\{\dots, -5, -2, 1, 4, 7, \dots\} = \{3k + 1 \mid k \in \mathbb{Z}\}$, and
$\{\dots, -4, -1, 2, 5, 8, \dots\} = \{3k + 2 \mid k \in \mathbb{Z}\}$.

If these sets are unioned together we get all of the integers. They are certainly non-empty sets. Finally, they are disjoint (they do not share any elments). Thus these sets partition $\mathbb{Z}$.

Although I did not expect this from anyone taking the test, I will give a more detailed proof.

First, it is obvious that all three sets are non-empty: $0, 1, 2$ are elements of each of the respective sets.

Next, suppose $m \in \mathbb{Z}$. Then the division algorithm states that there are **unique** integers $q, r \in \mathbb{Z}$ such that $m = 3q + r$ where $0 \leq r < 3$. Thus $m = 3q$, $3q + 1$, or $3q + 2$. So m belongs to one of these sets. Finally, since the remainder, r, is unique m belongs to **exactly one** of these sets (i.e. they are disjoint).

(c) $\{\dots, -3, -2, -1, 0\}$ and $\{0, 1, 2, 3, \dots\}$

Although the union of these sets is all of $\mathbb{Z}$, the sets are not disjoint (both contain 0). Thus these sets do not partition $\mathbb{Z}$.

3. (15 points) One-to-one and onto.

(a) Let $f : A \to B$ and $g : B \to A$. Suppose that $g \circ f$ is bijective. Prove **ONE** of the following:

i. f is injective (i.e. one-to-one). ii. g is surjective (i.e. onto).

Proof of i. Suppose that $f(x) = f(y)$. Then $g(f(x)) = g(f(y))$ so that $g \circ f(x) = g \circ f(y)$. However, $g \circ f$ is bijective. Thus it is one-to-one (injective). Therefore, $x = y$. Thus f is one-to-one as well.

Proof of ii. Suppose that $y \in A$ (the codomain of g). We know that $g \circ f$ is bijective. Thus $g \circ f$ is onto (surjective). Therefore, there exists some $z \in A$ such that $g \circ f(z) = y$. Let $x = f(z) \in B$. We have that $g(x) = g(f(z)) = g \circ f(z) = y$. Therefore, $g \circ f$ is onto.

(b) Let $h : \mathbb{Z} \to \mathbb{Z}$ be defined by $h(x) = 2x$. Is h one-to-one? Is h onto? **Prove your answers.**

Suppose $h(x) = h(y)$ for some integers x, y. Then $2x = 2y$ and so $x = y$. Thus h is one-to-one.

On the other hand, h is not onto. Notice that the range of h is all **even** integers (not all integers) so the range is not equal to the codomain. OR more concretely, suppose $h(x) = 1$. Then $2x = 1$ and so $x = 1/2$. But $1/2 \notin \mathbb{Z}$. Therefore, 1 is not in the range of h. Thus h is not onto.

Note: $h(x) = 2x$ is both one-to-one and onto if we change its domain and codomain to $\mathbb{R}$ (the real numbers).

4. (20 points) Quick Proofs

(a) Using induction, show that $n < 2^n$ for all **non-negative** integers n. *Hint:* $1 + 2^n \leq 2^n + 2^n$.
YOU MUST USE INDUCTION!

Base case $n = 0$: $0 < 1 = 2^0$ thus the inequality holds for $n = 0$ (the smallest **non-negative** integer).

Inductive step: Suppose that $n < 2^n$ for some non-negative integer n. Then $n+1 < 2^n+1$ since we assumed $n < 2^n$. Then $n + 1 < 2^n + 1 < 2^n + 2^n = 2(2^n) = 2^{n+1}$ since $1 < 2^n$ for all non-negative integers n (we will just use this fact, however, it too can be proven using induction).

Thus we showed that $n < 2^n$ for $n = 0$ and that $n < 2^n$ implies $n + 1 < 2^{n+1}$ for each non-negative integer n. Therefore, by induction, $n < 2^n$ for all non-negative integers n.

(b) Let $f : A \to B$ and $S_1, S_2 \subseteq A$. Show that $f(S_1) \cup f(S_2) \subseteq f(S_1 \cup S_2)$.

Suppose $x \in f(S_1) \cup f(S_2)$. Then either $x \in f(S_1)$ or $x \in f(S_2)$. This means that either there exists some $s \in S_1$ such that $x = f(s)$ or there exists some $s \in S_2$ such that $x = f(s)$. Therefore, there exists some $s \in S_1$ or $s \in S_2$ such that $x = f(s)$. Thus there exists some $s \in S_1 \cup S_2$ such that $x = f(s)$. Therefore, by definition, $x \in f(S_1 \cup S_2)$.

So we have shown that all the elements in $f(S_1) \cup f(S_2)$ are also in $f(S_1 \cup S_2)$. Therefore, $f(S_1) \cup f(S_2) \subseteq f(S_1 \cup S_2)$.

5. (20 points) Divisibility

(a) Use the Euclidean algorithm to find $(4, 11) = d$ (i.e. GCD of 4 and 11). Then use your work to backtrack through the algorithm and find integers x and y such that $4x + 11y = d$

11 divided by 4 is 2 remainder 3: $11 = (2)4 + 3$. Next, 4 divided by 3 is 1 remainder 1: $4 = (1)3 + 1$. Finally, 3 divided by 1 is 3 remainder 0. The Euclidean algorithm says that the last non-zero remainder is the GCD. Thus the GCD of 4 and 11 is 1.

Next, we will use the facts: $(-1)3 + 4 = 1$, $(-2)4 + 11 = 3$ to find a linear combination of 4 and 11 which gives us 1. Start with $(-1)3 + 4 = 1$ and replace 3 with $(-2)4 + 11$. This gives us $(-1)[(-2)4 + 11] + 4 = 1$ so that $(3)4 + (-1)11 = 1$.

(b) Suppose $ax + by = 6$ for some integers a, b, x, y. What are the possible value(s) of (a, b)?

We have a theorem which states (for $a, b \in \mathbb{Z}$ not both 0): $\{ax + by \mid x, y \in \mathbb{Z}\} = \{kd \mid k \in \mathbb{Z}\}$ where d is the GCD of a and b. In words, every linear combination of a and b is a multiple of the GCD and conversely every multiple of the GCD can be written as a linear combination of a and b.

Therefore, 6 must be a multiple of the gcd of a and b. Thus we can conclude that the GCD of a and b is $1, 2, 3$, or 6.

(c) Let $a, b, c \in \mathbb{Z}$ such that a and b are relatively prime, $a \,\big|\, c$, and $b \,\big|\, c$. Show that $ab \,\big|\, c$.

Since a and b are relatively prime (i.e. their GCD is 1), there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Next, since a and b divide c, there exists $k, \ell \in \mathbb{Z}$ such that $ak = c$ and $b\ell = c$. Thus $c = c \cdot 1 = c(ax + by) = cax + cby = (\ell b)ax + (ka)by = ab(\ell x + ky)$. Thus ab divides c since $\ell x + ky \in \mathbb{Z}$.

6. (20 points) Workin' mod 6

(a) Finish filling out the following addition and multiplication tables for $\mathbb{Z}_6$ (operations are addition and multiplication "mod 6"):

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) For each $x \in \mathbb{Z}_6$, either find x^{-1} or write "DNE" (if the multiplicative inverse does not exist).

$0^{-1} = \text{DNE}$	$1^{-1} = 1$	$2^{-1} = \text{DNE}$	$3^{-1} = \text{DNE}$	$4^{-1} = \text{DNE}$	$5^{-1} = 5$

For example, there is no number such that $2x = 1 \bmod 6$, so 2 has no multiplicative inverse. On the other hand, $5 \cdot 5 = 1 \bmod 6$ so 5 is its own multiplicative inverse.

(c) For each $x \in \mathbb{Z}_6$, either find $-x$ or write "DNE" (if the additive inverse does not exist).

$-0 = 0$	$-1 = 5$	$-2 = 4$	$-3 = 3$	$-4 = 2$	$-5 = 1$

Every number has an additive inverse (mod anything). For example, $2 + 4 = 0 \bmod 6$ so 2 is the additive inverse of 4 and 4 is the additive inverse of 2.

(d) Compute $2^{-1}(5 - 1) + 3$ or explain why this is undefined.

This is undefined since 2 has no multiplicative inverse mod 6 (i.e. 2^{-1} does not exist).

(e) Compute $5^{-1}(3 + 4) - 2$ or explain why this is undefined.

$5^{-1}(3 + 4) - 2 = 5(3 + 4) - 2 = 5(1) - 2 = 5 - 2 = 3$ (using $5^{-1} = 5$ and $3 + 4 = 1 \bmod 6$).

Alternatively $5^{-1}(3 + 4) - 2 = 5(7) - 2 = 35 - 2 = 33 = 3 \bmod 6$. We can perform the all of the operations (with the exception of division) using regular integer arithmetic.