MATH 580 — FIRST MIDTERM EXAM

January 30, 2006

NAME: Solutions

1. Do not open this exam until you are told to begin.
2. This exam has 9 pages including this cover. There are 11 problems.
3. Write your name on the top of EVERY sheet of the exam!
4. Do not separate the pages of the exam.
5. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
6. If you are unsure whether you can quote a result from class or the book, please ask.
7. Please turn **off** all cell phones.

PROBLEM	POINTS	SCORE
1	10	
2	10	
3	8	
4	10	
5	6	
6	10	
7	10	
8	10	
9	8	
10	8	
11	10	
TOTAL	100	

Name: _____

1. (3+3+4 points) Let $f : X \to Y$ be a function.

a. State the definition of injective.

The function f is injective if whenever $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$, then $x_1 = x_2$.

b. State the definition of surjective.

The function f is surjective if for each $y \in Y$ there exists an $x \in X$ so that $f(x) = y$.

c. Let $X = \{1, 2, 3, 4, 5\}$ and $Y = \{a, b, c\}$. Define a function $f : X \to Y$ by $f(1) = a$, $f(2) = b$, $f(3) = c$, $f(4) = 1$, and $f(5) = b$. Is the function f injective? Is it surjective? Be sure to justify your answer.

The function f is not injective because $f(1) = a = f(4)$ but $1 \neq 4$. The function f is surjective because $f(1) = a$, $f(2) = b$, and $f(3) = c$, i.e., every element of Y has an element of X mapping to it.

2. (10 points) Find the greatest common divisor of the integers 324 and 148. Find integers m and n so that the greatest common divisor is equal to $324n + 148m$.

We start by dividing 148 into 324 and obtain:

$$324 = 148(2) + 28.$$

Next we divide 28 into 148:

$$148 = 28(5) + 8.$$

We now divide 8 into 28:

$$28 = 8(3) + 4.$$

Finall we observe that 4 divides evenly into 8 with no remainder, therefore $\gcd(148, 324) = 4$. Now we back substitute with the above equations to find m and n:

$$4 = 324(16) + 148(-35).$$

3. (8 points) If $a|b$ and $c|d$, show that $ac|bd$.

Proof: Using the definition of divisibility we see that there exists $s, t \in \mathbb{Z}$ so that $as = b$ and $ct = d$. Multiplying these together we obtain $asct = bd$, i.e., $ac|bd$. ■

4. (3+3+4 points) **a.** Give a positive integer m so that $0 \leq m < 21$ and $m \equiv -4 (\mathrm{mod}\, 21)$.

The integer $m = 17$ works as $17 - (-4) = 21$, which is divisible by 21.

b. Find a positive integer n so that $0 \leq n < 21$ and $5n \equiv 1 (\mathrm{mod}\, 21)$.

Observe that $5(-4) = -20 \equiv 1 (\mathrm{mod}\, 21)$. Now we use part (a) to conclude that since $-4 \equiv 17 (\mathrm{mod}\, 21)$, we have that $5(17) \equiv 5(-4) \equiv 1 (\mathrm{mod}\, 21)$. Thus $n = 17$ is the integer we seek.

c. Solve the congruence $15x \equiv 6 (\mathrm{mod}\, 63)$.

Note here that $\gcd(15, 63) = 3 > 1$. Since $3|6$ as well, we can divide through by 3 to obtain the congruence

$$5x \equiv 2 (\mathrm{mod}\, 21).$$

In order to solve this, we need to find $5^{-1} (\mathrm{mod}\, 21)$. However, this is precisely what we found in part (b), namely, $5^{-1} = 17 (\mathrm{mod}\, 21)$. Thus, the solution to the congruence $5x \equiv 2 (\mathrm{mod}\, 21)$ is given by $x = 17(2) = 34 \equiv 13 (\mathrm{mod}\, 21)$. To check this is a solution, note that $5(13) = 65 \equiv 2 (\mathrm{mod}\, 21)$. Therefore, it only remains to construct the other solutions modulo 63. This is accomplished by adding multiples of 21: $13 + 21(0) = 13, 13 + 21(1) = 34, 13 + 21(2) = 55$. Thus, 13, 34 and 55 are the solutions of the original congruence.

5. (6 points) For any positive integer n, prove that $n^2 \equiv 0$ or $1 (\mathrm{mod}\, 3)$.

Proof: We know that any positive integer is congruent to 0, 1, or 2 modulo 3. Therefore, we just need to check what 0^2, 1^2, and 2^2 are modulo 3:

$$\begin{aligned} 0^2 &\equiv 0 \,(\mathrm{mod}\, 3) \\ 1^2 &\equiv 1 \,(\mathrm{mod}\, 3) \\ 2^2 &= 4 \equiv 1 \,(\mathrm{mod}\, 3). \end{aligned}$$

6. (10 points) Show that $3^n > n$ for all positive integers n.

Proof: We proceed by induction on n. We begin by checking the base case of $n = 1$: $3^1 = 3 > 1$. Now suppose that $3^k > k$ for some positive integer k. Observe that

$$\begin{aligned} 3^{k+1} &= 3(3^k) \\ &> 3k \qquad \text{by our induction hypothesis} \\ &= k + k + k \\ &> k + 1 \qquad \text{since } k \geq 1 \text{ shows that } k + k \geq 2 > 1. \end{aligned}$$

Thus we see that $3^{k+1} > k + 1$, so by induction we see that the statement holds for all $n \in \mathbb{N}$. ■

7. (3+3+4 points) **a.** Complete the following sentence: "An integer $p > 1$ is prime if "

An integer $p > 1$ is prime if and only if the only positive divisors of p are 1 and p.

b. Show that if $d|a$ and $d|b$, then $d|(am + bn)$ for all integers $m, n \in \mathbb{Z}$.

Proof: Using that $d|a$ we see that there exists $s \in \mathbb{Z}$ so that $ds = a$ and similarly there exists $t \in \mathbb{Z}$ so that $dt = b$. Thus we see that

$$\begin{aligned} am + bn &= dsm + dtn \\ &= d(sm + tn). \end{aligned}$$

Thus, $d|(am + bn)$. ■

c. Let a and b be integers with $\gcd(a, b) = d > 1$. Suppose there exists $m, n \in \mathbb{Z}$ so that $p = am + bn$ for some prime number p. Prove that $d = p$.

Proof: Note that since $d = \gcd(a, b)$, we have that $d|a$ and $d|b$. Thus, it follows from part b that $d|(ma + nb)$. In particular, we see that $d|p$. But since $d > 1$ and $d|p$, we must have that $d = p$. ■

8. (3+7 points) Let $f : X \to Y$ and $A, B \subseteq X$.

a. Define $f(A)$.

$$\begin{aligned} f(A) &= \{f(a) \mid a \in A\} \\ &= \{y \in Y \mid \exists\, a \in A \text{such that } f(a) = y\} \end{aligned}$$

b. Prove that if f is injective then $f(A) \cap f(B) = f(A \cap B)$.

Proof: Let $y \in f(A) \cap f(B)$, i.e., $y \in f(A)$ and $y \in f(B)$. Since $y \in f(A)$ we know there exists an $a \in A$ so that $f(a) = y$. Similarly, we have that there exists a $b \in B$ so that $f(b) = y$. This shows that $f(a) = y = f(b)$. The fact that f is injective implies that $a = b$. Thus, $a \in A$ and $a \in B$, i.e., $a \in A \cap B$ and $f(a) = y$. Hence $y \in f(A \cap B)$. Thus we have that $f(A) \cap f(B) \subseteq f(A \cap B)$. Let $y \in f(A \cap B)$. So there exists $x \in A \cap B$ so that $f(x) = y$. Since $x \in A \cap B$, $x \in A$ and $x \in B$. Thus we see that $y \in f(A) \cap f(B)$. Hence $f(A \cap B) \subseteq f(A) \cap f(B)$ and thus we have $f(A) \cap f(B) = f(A \cap B)$. ■

9. (8 points) Show that for a and b positive integers, $\gcd(a, b) = \gcd(a, a + b)$.

Proof: Recall that if $e|a$ and $e|b$, then necessarily we have that $e|\gcd(a, b)$. What we will show is that $\gcd(a, b)|\gcd(a, a+b)$ and $\gcd(a, a+b)|\gcd(a, b)$ and so they are equal. Let $d = \gcd(a, b)$ and $e = \gcd(a, a + b)$. First observe that since $d|a$ and $d|b$, we have that $d|a + b$. Thus $d|e$. Observe also that $e|a$, so it only remains to show that $e|b$. Since $e = \gcd(a, a + b)$ we have that $e|a$ and $e|(a+b)$. So there exists $m, n \in \mathbb{Z}$ so that $em = a$ and $en = a+b$. Combining these two equations we have $en = em + b$, i.e., $b = e(n - m)$. Thus $e|b$ and hence $e|d$ and so $d = e$. ■

10. (8 points) In set theory two sets A and B are considered to be "the same" if there is a bijective function (injective and surjective) $f : A \to B$. Let $\mathbb{E}$ be the set of even integers and $\mathbb{O}$ be the set of odd integers. Show under this definition of two sets being the same that $\mathbb{E}$ is the same as $\mathbb{O}$.

Proof: Recall that any even integer can be written in the form $2k$ and any odd integer can be written in the form $2k+1$ for some integer k. Define the function $f : \mathbb{E} \to \mathbb{O}$ by $f(2k) = 2k+1$. This function clearly takes the set of even integers into the set of odd integers. Now we just need to show the function is injective and surjective.
Let $2n$ and $2m$ be even integers so that $f(2n) = f(2m)$, i.e., $2n+1 = 2m+1$. Subtracting 1 from each side we have $2n = 2m$. Thus f is injective.
Now let $2n+1$ be an odd integer. Then $2n$ is an even integer and $f(2n) = 2n+1$, so f is surjective. ■

11. (10 points) A group of 7 young children decide to each go to a different neighborhood to trick-or-treat for Halloween. Upon finishing, they gather and mix all of their candy in a large pile. When they tried to divide the candy equally amongst themselves, there were 6 left over. This caused two of the children to become impatient and leave to go home without any candy. After the two left, the kids again tried to divide the candy equally amongst themselves and found there were 2 pieces left over. What is the smallest number of pieces of candy that could have been in the original pile? (You must use the methods of this course to find the solution, guess and check will receive 0 points.)

This amounts to solving the simultaneous congruences

$$\begin{aligned} x &\equiv 6 (\mathrm{mod}\, 7) \\ x &\equiv 2 (\mathrm{mod}\, 5). \end{aligned}$$

We apply the Chinese remainder theorem to find the smallest value of x that satisfies both congruences. Since $\gcd(5,7) = 1$, we know there exist integers $m, n \in \mathbb{Z}$ so that $1 = 5m+7n$. The solution x to the congruence is then given by $x = 6(5m) + 2(7n)$. Thus, our next step is to find m and n. One can use the Euclidean algorithm to find them, or just observe that $5(3) + 7(-2) = 1$. Thus, $x = 6(15) + 2(-14) = 62 (\mathrm{mod}\, 35)$. Thus, 62 is a solution, but the smallest solution is obtained when we reduce this modulo 35 to obtain $x = 27$. Note that one can check easily that 27 does indeed satisfy both congruences.