Mathematics 243, section 2 – Mathematical Structures
Information on Exam 2
October 25, 2017

*General Information*

The second exam this semester will be given next week, either on Thursday evening, November 2 or in class on Friday morning, November 3. (We'll discuss the options on October 27 and decide.) The exam will cover the material we have discussed since the first exam (Problem Sets 4,5,6), through class on Friday, October 27 ("Fermat's Little Theorem").

1) Functions/Mappings, injectivity and surjectivity
2) Integer division – know the statement of the Division Algorithm (Theorem 4.8 in the text) and its proof,
3) Greatest common divisors and Euclid's algorithm for $\gcd(a, b)$. Know the proof of Theorem 4.20 – Every nonzero subgroup of the integers under addition has the form $d\mathbf{Z}$ for some $d > 0$, and how $d$ satisfies the properties of a gcd (see Definitions 4.21 and 4.23).
3) Prime numbers, Euclid's Lemma (Theorems 5.13 and 5.12), prime factorizations and the "Fundamental Theorem of Arithmetic (Theorems 5.17 and 5.18).
4) Congruence mod $n$ and the integers mod $n$: the set of congruence classes $\mathbf{Z}/n\mathbf{Z}$ and the addition and multiplication mod $n$ operations.

*Some Review Problems*

From the course notes:

1) Chapter 4: 4.7, 4.9, 4.10
2) Chapter 5: 5.5, 5.8a, 5.9, 5.14, 5.15, 5.16
3) Chapter 6: 6.3, 6.4, 6.7, 6.9b,c

*Review Session*

I will be happy to run a review session before the exam. Tuesday evening (October 31) is probably the best time for this for me, especially if we do the exam on Thursday evening.

*Sample Exam Questions*

Note: This list is longer than the actual exam will be to show the range of different kinds of questions that might appear.

I. Let $[a] \in \mathbf{Z}/18\mathbf{Z}$ and let $m_{[a]} : \mathbf{Z}/18\mathbf{Z} \to \mathbf{Z}/18\mathbf{Z}$ be the mapping defined by $m_{[a]}([x]) = [a] \cdot [x] = [a \cdot x]$.

A) Is $m_{[12]}$ an injective mapping? Why or why not? Is it a surjective mapping? Why or why not?
B) Is $m_{[5]}$ an injective mapping? Why or why not?
C) Prove that $m_{[a]}$ is injective if and only if $[a]$ has a multiplicative inverse in $\mathbf{Z}/18\mathbf{Z}$.
D) Prove the $m_{[a]}$ is injective if and only if $m_{[a]}$ is surjective.

II.
A) Given integers $a$, and $b > 0$, prove that there exist unique integers $q$ and $r$ such that $a = qb + r$ and $0 \leq r < b$. (You may apply the Well-Ordering Principle without justifying that.)
B) Find the quotient $q$ and the remainder $r$ as in part A for $a = 4578$ and $b = 235$.

III.
A) Prove that if $S = \langle a, b\rangle = \{x \in \mathbf{Z} : x = ma + nb, m, n \in \mathbf{Z}\}$, then the smallest positive integer $d$ in $S$ satisfies the properties:
1. $d$ divides $a$ and $d$ divides $b$.
2. If $c$ divides $a$ and $c$ divides $b$, then $c$ divides $d$.

B) Find the integer $d = \gcd(488, 376)$ and express $d$ in the form $d = m \cdot 488 + n \cdot 76$ for integers $m, n$.
C) Prove that if there is a solution of the congruence $ax \equiv b \pmod{n}$ (where $n > 1$), then $\gcd(a, n)|b$.

IV.
A) Show that for all $n \geq 1$, $8|(9^n - 1)$. (Hint: Show first that $9^{k+1} - 1 = 9^k \cdot 8 + (9^k - 1)$.)
B) Restate the result of part A as a congruence.
C) (Extra Credit-type question) Suppose we used base 9 rather than base 10 to represent integers. How could you test numbers for divisibility by 8 using the base 9 digits? How could you test numbers for divisibility by 10 using the base 9 digits?

V. Show that $[x]$ has a multiplicative inverse in $\mathbf{Z}/n\mathbf{Z}$ (that is, a $[y]$ such that $[x][y] = [1] = [y][x]$) if and only if $\gcd(x, n) = 1$.

VI.
A) Find all integer solutions of the congruence $12x \equiv 7 \bmod 331$.
B) Find all solutions $[x]$ of the equation $[17][x] + [4] = [2]$ in $\mathbf{Z}/29\mathbf{Z}$.
C) Which $[x] \in \mathbf{Z}/18\mathbf{Z}$ have multiplicative inverses?