

Mathematics 243, section 1 – Algebraic Structures  
Information on Exam 2  
October 25, 2006

*General Information*

The second exam this semester will be given next Wednesday, November 1. The exam will cover the material we have discussed since the first exam, through class on Wednesday, October 25. This is the material from sections 1.7, 2.1, 2.2, 2.3, 2.4, 2.5, and 2.6. The topics to review are:

- 1) Relations, especially equivalence relations, and their properties
- 2) Properties of  $\mathbf{Z}$
- 3) Proof by mathematical induction
- 4) Divisibility. Know the statement of the Division Algorithm (Theorem 2.10 in the text) and its proof,
- 5) Prime numbers, prime factorizations and the Unique Factorization Theorem (Theorem 2.18),
- 6) Greatest common divisors and Euclid's algorithm for  $\gcd(a, b)$ . Know the proof of Theorem 2.12 (existence of  $\gcd(a, b)$  in  $S = \{x \in \mathbf{Z} : x = ma + nb, \text{ for some } m, n \in \mathbf{Z}\}$ , and uniqueness of  $\gcd$ ).
- 7) Congruence mod  $n$  and the integers mod  $n$ : the set of congruence classes  $\mathbf{Z}_n$  and the addition and multiplication mod  $n$  operations.

*Some Review Problems*

From Gilbert and Gilbert:

- 1) Section 1.7: 4, 7, 8, 12
- 2) Section 2.2: 4, 6, 13, 14, 27, 32, 33, 45
- 3) Section 2.3: problems like 1-11, proofs like 17-25, 34, 37
- 4) Section 2.4: problems like 2, 3, 14, 15, 16, 20
- 5) Section 2.5: problems like 3-24, 30, 34
- 6) Section 2.6: problems like 3,4,5,6,7

*Review Session*

I will be happy to run a review session before the exam. Monday evening (October 30) is probably the best time for this.

*Sample Exam Questions*

I. Show using mathematical induction that

$$1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n - 1)2^n + 2$$

for all integers  $n \geq 1$ .

II. Let  $R$  be the relation on  $\mathbf{Z}$  defined by  $xRy$  if (and only if  $5|(x^2 - y^2)$ ).

- A) Is  $R$  an equivalence relation? Prove your assertion.
- B) Show that  $xRy$  if and only if  $x \equiv y \pmod{5}$  or  $x \equiv -y \pmod{5}$ . (Hint: Euclid's Lemma)

III.

- 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  $b = 235$ .

IV.

- A) Give the definition of the *greatest common divisor* of the integers  $a, b$ .
- B) Prove that if  $S = \{x \in \mathbf{Z} : x = ma + nb, m, n \in \mathbf{Z}\}$ , then the smallest positive integer in  $S$  is  $\gcd(a, b)$ .
- C) Find the integer  $d = \gcd(488, 376)$  and express  $d$  in the form  $d = m \cdot 488 + n \cdot 376$  for integers  $m, n$ .
- D) Prove that if there is a solution of the congruence  $ax \equiv b \pmod{n}$  (where  $n > 1$ ), then  $\gcd(a, n) | b$ .

V.

- 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?

VI.

- A) Find all integer solutions of the congruence  $12x + 3 \equiv 7 \pmod{31}$ .
- B) Find all solutions  $[x]$  of the equation  $[17][x] + [4] = [5]$  in  $\mathbf{Z}_{29}$ .
- C) Show that  $[x]$  has a multiplicative inverse in  $\mathbf{Z}_n$  (that is, a  $[y]$  such that  $[x][y] = [1] = [y][x]$ ) if and only if  $\gcd(x, n) = 1$ .
- D) Which  $[x] \in \mathbf{Z}_8$  have multiplicative inverses?