Mathematics Department, University of Massachusetts Dartmouth

Discrete Mathemtics II

MTH182 – Section 03 – Spring 2015

Review for Exam 3

Exam 3 is Thursday, April 9 from 8:00-9:15am

Reading:	Discrete Mathematics, first edition, section Sections 7.1-7.5
	Problems sets 7, 8, and 9
	Chapter 7 supplementary exercises: 1, 3, 5, 7, 9, 11, 13

Summary of concepts

The following is a list of the major topics covered in this exam:

- Divisibility: "divides" notation, divisors, factors, multiples
- Prime and composite numbers
- The division algorithm: quotients, remainders, "div" and "mod" operations.
- Modular congruence
- Basic cryptography: private key ciphers and shift ciphers

What follows are a list of *suggested* exercises that will help you review for the exam. It is *not* a replacement for the week-by-week problem sets.

Chapter 7 Supplementary Exercises

1. Let $A = \{n \in \mathbb{Z} \ : \ n \geq 2\}$. For $a \in A$, define $f(a)$ to be the largest positive integer k such that $k < a$ and $k|a$. Then f is a function from $\mathbb{N}$ to $\mathbb{N}$.
  (**a**) What is $f(12)$
  (**b**) What is $f(27)$
  (**c**) What is $f(32)$
  (**d**) What is $f(33)$
  (**e**) Is f one-to-one?
  (**f**) Is f onto?

3. Let $a, b, c, d \in \mathbb{Z}$ be such that $a \neq 0$. Prove that if $a|(b + c + d)$, and a divides any two of b, c, and d, then a divides the third integer.

5. Let a and b be integers such that $a \neq 0$. Prove that if $a|b$, then $a^n|b^n$ for every positive integer n.

7. Prove that $3|(n^3 + 2n)$ for every positive integer n.

9. Express 234 as a product of primes.

11. Is $37 \equiv -19 \pmod 4$?

13. Prove or disprove:

(**a**) There exists an integer a such that $ab \equiv 0 \pmod 5$ for every integer b.

(**b**) If $a \in \mathbb{Z}$, then $ab \equiv 0 \pmod 5$ for every $b \in \mathbb{Z}$.

(**c**) For every integer a, there exists an integer b such that $ab \equiv 0 \pmod 5$.