

# Review for Exam 1 - Math 100, Spring 2005

January 24, 2005

## 1 General

**Where and when:** Feb 4, usual classroom, usual time - try to get there 5 minutes early

**What you need:** Pencil or pencils, Student ID. You will not be permitted to use a calculator or have anything else on your desk besides the exam, solution sheet, pencils, and your ID.

**Form:** Multiple choice, 20 problems

**Coverage:**

Stein: Chapters 2 and 3

Gemignani: Sections 1.1,1.2,1.4,1.5,2.1,2.2,2.3

All lectures through January 28

**Breakdown:** (Approximate)

Computation with primes, facts about primes, definitions involving primes:  
7-8 problems

Constituents of a proof: 6-7 problems

Notation (including  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \in, \{x : \dots\}, \forall, \exists, \vee, \implies$ ): 4-5 problems

“Informal” logic (e.g., as in Gemignani Ch 1 and 2): 2-3 problems

**Note** that there is overlap, so these numbers do not add to 20!

## 2 Typical questions:

1) **Question:** Which is a prime number?

- (a) 1002 (b) 101 (c) 93 (d) 187

2) **Question:** Which is the LCM of 225 and 525?

- (a) 75 (b) 1575 (c) 105 (d) None of these

3) **Question:** Which is the GCD of 225 and 525?

- (a) 75 (b) 1575 (c) 105 (d) None of these

**Note:** If I ask you what the GCD or LCM of 2 numbers is, I don't care how you get the answer. However, there *will be* at least one problem which tests your ability to use the Euclidean Algorithm.

4) **Question:** Suppose  $M$  and  $N$  are relatively prime, that is,  $\text{GCD}(M, N) = 1$ . Which of the following is a true statement?

- (a) there is no common multiple for  $M$  and  $N$  (b)  $\exists r, s \in \mathbb{Z} (rM + sN = 1)$   
(c)  $M$  or  $N$  is prime (d) All of these

5) **Question:** Which of the following is *not* a consequence of the Fundamental Theorem of Arithmetic?

- (a) Every integer greater than 1 has at least one prime factorization (b) Any two prime factorizations of an integer greater than 1 are the same except for the order of multiplication (c) there are infinitely many primes

6) **Question:** What is the structure of a *proof by contradiction*?

- (a) A sequence of statements, each of which is either a hypothesis, an axiom, or a logical consequence of earlier statements in the proof. (b) First assume that the conclusion is false, and derive from this a patently false statement. (c) Try many values of  $N$ , and then make a conjecture. (d) Find a counterexample, this proves that the theorem is false.

7) **Question:** What is the structure of a *direct proof*?

- (a) A sequence of statements, each of which is either a hypothesis, an axiom, or a logical consequence of earlier statements in the proof. (b) First assume that the conclusion is false, and derive from this a patently false statement. (c) Try many values of  $N$ , and then make a conjecture. (d) Find a counterexample to prove that the theorem is false.

**8) Question:** To see if a large number  $N$  is prime, we check to see if  $2, 3, 5, \dots$  are factors. At what point can we stop and be sure that  $N$  is prime?

- (a) Not until we've tried all primes less than  $N$ . (b) After we've tried all primes less than or equal to  $N/2$  (c) After we've tried all primes less than or equal to  $\sqrt{N}$

**9) Question:** What is the best translation for the statement  $\forall M, N \in \mathbb{Z}^+ M|N$  and  $N|M \implies M = N$ ?

- (a) For any two positive integers, if each divides the other than they are the same. (b) There exist two positive integers, each of which divides the other and which are the same. (c) We select  $M$  and  $N$  so that each is a multiple of the other and they are the same. (d) If  $M = N$  then  $M$  divides  $N$  and vice versa.

**Last problems:** You will get several problems like the next few, which ask you to identify the constituents of a theorem and proof. First, I will give you a statement and/or proof of a theorem, then follow it with some questions. (The theorem(s) on the exam will be different than this one.)

**Theorem** Let  $p$  be prime and  $a, b$  be positive integers, then there is an integer  $x$  such that " $as \equiv b \pmod{p}$ ", that is, such that  $p|(b - ax)$ .

**Proof:** (I'll number the steps of the proof for later reference)

- (i) Since  $p$  is prime,  $\text{GCD}(p, a)=1$   
(ii) Therefore,  $\exists r, s \in \mathbb{Z}$  such that  $pr + as = 1$   
(iii) Then  $pr = 1 - as$   
(iii) Then  $(pr)b = b - (as)b$   
(iv) Put  $x = sb$ , then  $p(rb) = b - ax$   
(v) Then  $p|(b - ax)$  (which is what we are trying to prove)□

**(The questions relating to this theorem and proof are on the next page)**

- 10) Question:** Which of the following is a *hypothesis* of this theorem?
- (a)  $\text{GCD}(p, a) = 1$  (b)  $p | (b - ax)$ . (c)  $p$  is a prime (d)  $\exists r, s \in \mathbb{Z}$  such that  $pr + as = 1$
- 11) Question:** Which of the following is a *conclusion* of this theorem?
- (a)  $\text{GCD}(p, a) = 1$  (b)  $p | (b - ax)$ . (c)  $p$  is a prime (d)  $\exists r, s \in \mathbb{Z}$  such that  $pr + as = 1$
- 12) Question:** Line (ii) of the proof...
- (a) is a hypothesis; (b) Follows from line (1) by a lemma we proved in class; (c) follows from line (1) by fundamental rules of arithmetic; (d) follows from the definition of |
- 13) Question:** Line (iii) of the proof...
- (a) is a hypothesis; (b) Follows from earlier lines by a lemma we proved in class; (c) follows from earlier lines by fundamental rules of arithmetic; (d) follows from the definition of |
- 14) Question:** Line (v) of the proof...
- (a) is a hypothesis; (b) Follows from earlier lines by a lemma we proved in class; (c) follows from earlier lines by fundamental rules of arithmetic; (d) follows from the definition of |