

# MATH 110 SAMPLE MIDTERM

Saturday, April 16, 2005

Name: \_\_\_\_\_

Numeric Student ID: \_\_\_\_\_

I agree to abide by the terms of the honor code:

Signature: \_\_\_\_\_

**Instructions:** Print your name, and student ID number in the space provided. You may not use notes, or textbooks, or calculators. Read each question carefully. As ever, try to be as precise as possible when writing your proofs. Correct answers without justification will receive little or no credit. There are 5 questions. There is an 80 minute time limit on this exam. Good luck.

Question	Score	Maximum
1		15
2		15
3		10
4		10
5		10
Total		60

1. (a) Find the gcd of the pair of integers (399,119).

(b) Find all possible integer solutions  $(x, y)$  to the equation

$$399x + 119y = \gcd(399, 119).$$

(c) Does the congruence

$$119x \equiv 14 \pmod{399}$$

have a solution? If not, why not. If so, provide at least one solution mod 399.

2. In the following questions,  $\phi(n)$  denotes the Euler phi function.

(a) Compute  $\phi(225)$ .

(b) Do there exist natural numbers  $n$  and  $m$  such that  $\phi(mn) \neq \phi(n)\phi(m)$ ?  
Explain why or give a counterexample.

(c) Find the smallest integer  $N$  such that  $\phi(n) \geq 5$  for all  $n \geq N$ .

3. The binomial coefficient  $\binom{m}{n}$  is defined by

$$\binom{m}{n} = \frac{m!}{(m-n)! n!}$$

Determine the running time (using big-O notation) needed to compute this binomial coefficient in terms of  $m$  and  $n$ . Is this a polynomial time algorithm? Why or why not?

4. In this question, you ONLY need to determine whether or not the system of equations has at least one solution. If yes, mark “Y”, if no, mark “N.”

(a)  $x \equiv 1 \pmod{6}$   
 $x \equiv -1 \pmod{18}$

(b)  $2x \equiv 1 \pmod{1234567891011}$

(c)  $x \equiv 3 \pmod{29}$   
 $x \equiv 5 \pmod{47}$

(d)  $x^{22} \equiv 1 \pmod{23}$

(e)  $x^2 \equiv 4 \pmod{7}$

5. An affine map is used to encrypt a message in the eleven letter alphabet

$\{ A D E G H I N R S T W \}$

resulting in the following ciphertext:

AIWENDSGTRA

Decode this message knowing that N and R in the ciphertext correspond to  $T$  and  $E$ , respectively, in the plaintext.