

# Math 328K Final Exam

May 17, 2010

Name \_\_\_\_\_

## Directions:

1. No books, notes, calculators.
2. You should write out your proofs as in the homeworks, with enough detail that someone else in the class who hasn't seen the problem before would be able to understand your answer. Use complete English sentences where appropriate. Use "connecting phrases" between statements to describe the sequence of your argument. I am interested in both the clarity and correctness of your argument. Please ask if any instructions are unclear.
3. You may not make more than one attempt at a problem. If you make several attempts, you must indicate which one you want counted.
4. You may leave as soon as you are finished, but once you leave the exam, you may not make any changes to your paper.
5. This test has 11 problems. You have 3 hours to complete the exam.

1. (20 points)

(a) State the Fundamental Theorem of Arithmetic.

(b) Prove the following:

**Lemma.** *Let  $p$  and  $q_1, q_2, \dots, q_n$  all be primes and let  $k$  be a natural number such that  $pk = q_1q_2 \cdots q_n$ . Then  $p = q_i$  for some  $i$ .*

(c) In five lines or less, explain how this Lemma was used in the proof of the Fundamental Theorem of Arithmetic.

2. (16 points) Give **two different proofs** of the following theorem. For example, your first proof may involve Diophantine equations and your second proof may use the Fundamental Theorem of Arithmetic. Make sure you clearly indicate where each proof begins and ends.

**Theorem.** *Let  $a, b, c,$  and  $n$  be integers with  $n > 0$ . If  $ac \equiv bc \pmod{n}$  and  $(c, n) = 1$ , then  $a \equiv b \pmod{n}$ .*

3. (25 points) For  $n \geq 0$ , the  $n^{\text{th}}$  Fermat number is defined to be  $F_n = 2^{2^n} + 1$ . So  $F_0 = 3$ ,  $F_1 = 5$ ,  $F_2 = 17$ , and so on. Prove the following:

**Lemma.** For every natural number  $n \geq 1$ :

$$F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1} = F_n - 2.$$

**Lemma.** Suppose  $n$  and  $m$  are distinct integers greater than or equal to 0. Then  $F_n$  and  $F_m$  are relatively prime.

Use the lemmata above to prove the following.

**Theorem.** There exist infinitely many prime numbers.

4. (15 points)

(a) Find  $(172, 20)$

(b) Find an  $x$  and  $y$  such that  $172x + 20y = (172, 20)$

(c) Explain how you would find all integer solutions to  $172x + 20y = (172, 20)$  and then explicitly find a solution that is different from the solution you found in part (b).

5. (10 points) Please answer each question in **five lines or less**.

(a) State Euler's Theorem and give a summary of the proof.

(b) State Fermat's Little Theorem and explain how this theorem is a consequence of Euler's Theorem.

6. (20 points) You want to construct an RSA public-key cryptography system based on the primes  $p = 5$  and  $q = 11$ . Answer the following questions.

(a) Among the numbers 7, 8, and 10, which one is appropriate as an encoding exponent? Explain your answer.

(b) Which two numbers do you make public?

(c) Suppose you want to send the message 8. What number do you send?

(d) What is your decoding exponent  $D$ ?

(e) Explain how you would decode the encrypted message. (Don't worry about carrying out the operation.)

7. (10 points) Suppose we have already proven the following theorem.

**Theorem.** Let  $a_1, a_2, n_1,$  and  $n_2$  be integers with  $n_1 > 0, n_2 > 0,$  and  $(n_1, n_2) = 1.$  Then the system

$$\begin{aligned}x &\equiv a_1 \pmod{n_1} \\x &\equiv a_2 \pmod{n_2}\end{aligned}$$

has a unique solution modulo  $n_1n_2.$

Prove the Chinese Remainder Theorem.

**Theorem** (Chinese Remainder Theorem). Suppose  $n_1, n_2, \dots, n_L$  are positive integers that are pairwise relatively prime, that is,  $(n_i, n_j) = 1$  for  $i \neq j, 1 \leq i, j \leq L.$  Then the system of  $L$  congruences

$$\begin{aligned}x &\equiv a_1 \pmod{n_1} \\x &\equiv a_2 \pmod{n_2} \\&\vdots \\x &\equiv a_L \pmod{n_L}\end{aligned}$$

has a unique solution modulo the product  $n_1n_2n_3 \cdots n_L.$

8. (15 points)

(a) Let  $a$  and  $n$  be natural numbers with  $(a, n) = 1$ . Define the *order of  $a$  modulo  $n$* , denoted  $\text{ord}_n(a)$ .

(b) Prove the following.

**Theorem.** *Suppose  $p$  is prime and  $a$  is a natural number such that  $(a, p) = 1$ . Suppose  $k$  is a natural number that is relatively prime to  $\text{ord}_p(a)$ . Then  $\text{ord}_p(a^k) = \text{ord}_p(a)$ .*

9. (10 points) Prove the following:

**Theorem.** *Let  $n$  and  $m$  be natural numbers that are relatively prime, and let  $a$  be an integer. If  $x \equiv a \pmod{n}$  and  $x \equiv a \pmod{m}$ , then  $x \equiv a \pmod{nm}$ .*

10. (10 points) Prove the following:

**Theorem.** *Suppose  $p$  and  $q$  are distinct primes. Then  $\phi(pq) = \phi(p)\phi(q)$ .*

11. (5 points) In the answer below, I have attempted to show that  $3^{360} \equiv 1 \pmod{91}$ . Unfortunately my answer contains a mistake. Find and explain the mistake. Give a correct solution to the Exercise.

**Exercise.** Find the number  $x$  in the canonical complete residue system modulo 91 such that  $3^{360} \equiv x \pmod{91}$ .

**Answer:** Note that  $(3, 91) = 1$ , since 91 and 3 are both prime. Therefore we can apply Fermat's Little Theorem and conclude that  $3^{90} \equiv 1 \pmod{91}$ . Since  $3^{360} = (3^{90})^4$ , we see that  $3^{360} \equiv 1^4 \pmod{91}$ . So  $3^{360} \equiv 1 \pmod{91}$ . So 1 is the number in the canonical complete residue system modulo 91 that is congruent to  $3^{360}$ .