Exam II – 11/18/09

Math 406

Name:

1. (15 points) Using the Chinese Remainder Theorem, find all solutions to the following system:

$$7x \equiv 4 \pmod{11}$$
$$x \equiv 3 \pmod{7}.$$

2. (20 points) If the ciphertext message produced by RSA encryption with the key $(e, n) = (139, 2747)$ is 1439, what is the plaintext message? (Give the answer as a block of 4 digits. Use the back of this page if necessary.)

3. (a) (10 points) Find $\text{ord}_{14}5$.

(b) (5 points) Find all the primitive roots for 14. (Hint: first determine the number of primitive roots.)

4. (10 points) Let p be a prime number. Show that for all integers a, b, we have $(a+b)^p \equiv a^p + b^p \pmod{p}$. Does this remain true if p is replaced by an arbitrary integer n? (Explain.)

5. (a) (10 points) Let m, n be positive integers. Prove that $m \mid n \Rightarrow \phi(m) \mid \phi(n)$.

(b) (5 points) Is it true that $m \mid n \Rightarrow \sigma(m) \mid \sigma(n)$? Prove, or disprove with a counterexample.

(c) (5 points) Is it true that $m \mid n \Rightarrow \mu(m) \mid \mu(n)$? Prove, or disprove with a counterexample.

6. (10 points) Let p be a prime number. Show that $(2p-1)! \equiv p \pmod{p^2}$. (Use the back of this page if necessary.)