

Name _____

INTRODUCTION TO NUMBER THEORY

Exam 3

April 28, 2000

The point value of each problem is given in the margin.

(10) 1. Find the least complete solution of the congruence

$$15x \equiv 100 \pmod{35}.$$

(20) 2. Short answer.

a) Give a reduced residue system modulo 20.

b) Let p be a prime. How many solutions $(\text{mod } p^3)$ does the congruence $px \equiv b \pmod{p^3}$ have if $p|b$?

How about if $p \nmid b$?

c) Evaluate $\left(\frac{37}{19}\right) =$

d) If m is an odd number such that $2^{m-1} \equiv -1 \pmod{m}$ can we make any conclusion as to whether m is a prime or not? Explain.

(12) 3. Find an integer x with $100 < x < 200$ such that $4x \equiv 1 \pmod{11}$, and $x \equiv 2 \pmod{9}$.

(10) 4. Say the decimal expansion of $3/140$ is given by

$$\frac{3}{140} = .a_1a_2 \dots a_i \overline{c_1c_2 \dots c_k}$$

with i, k minimal. Find the values of i, k .

(10) 5. a) What is the order of $4 \pmod{11}$?

b) Find the remainder in dividing 4^{46} by eleven.

(12) 6. Given that $x \equiv 2 \pmod{11}$ is the only solution of the congruence $x^3 + 3 \equiv 0 \pmod{11}$ find all solutions of the congruence $x^3 + 3 \equiv 0 \pmod{121}$.

(12) 7. State and prove Euler's Theorem.

(14) 8. In the RSA method of public cryptography suppose that you have chosen $p = 5$, $q = 11$, $e = 7$.

a) Calculate the least common multiple $[p - 1, q - 1] =$

b) Calculate the decode exponent d .

c) Suppose that someone has sent you the encrypted message M_1 , that is $M_1 \equiv M_0^e \pmod{pq}$, $0 < M_1 < pq$, and M_0 is the original message, $0 < M_0 < pq$. Explain how you will decipher the message.

d) Which quantities are made public?

e) In practice, the primes chosen are much larger. What is it that allows the RSA method to be secure and yet be public?