

INTRODUCTION TO NUMBER THEORY

Exam 3

April 27, 2007

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

(8) 1. Find the least complete solution of the congruence, (that is all solutions mod 21).

$$6x \equiv 27 \pmod{21}.$$

2. Short answer.

(3) a) If $f(x)$ is a polynomial of degree 5 what is the greatest number of solutions the congruence $f(x) \equiv 0 \pmod{7}$ can have?

(Assume $f(x)$ is not identically zero $\pmod{5}$.)

What is the greatest number of solutions $f(x) \equiv 0 \pmod{35}$ can have?

(Assume that $f(x)$ is not identically zero $\pmod{5}$ or $\pmod{7}$.)

(3) b) If $f(x)$ is a polynomial of degree d and p is a prime such that the congruence $f(x) \equiv 0 \pmod{p}$ has 2 distinct solutions \pmod{p} , one singular, one nonsingular, how many solutions can the congruence $f(x) \equiv 0 \pmod{p^2}$ have? (Give all possibilities.)

(3) c) What are the possible values for the order of $a \pmod{23}$, if $23 \nmid a$?

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

- (10) 3. In order to count the number of pennies in a large jar they are first stacked into groups of 5, with 1 left over. Next, they are stacked into groups of 6, with 2 left over. Finally, they are stacked into groups of 7 and none are left over. It is known that there are between 200 and 400 pennies in the jar. How many are there?

- (10) 4. Say the decimal expansion of $66/325$ is given by

$$\frac{66}{325} = .a_1a_2 \dots a_i \overline{c_1c_2 \dots c_k}$$

with i, k minimal. Find the values of i, k . (Use the theory to obtain i, k . You can check your answer by long division or on your calculator.)

(10) 5. If $(a, m) = 1$, $k = \text{ord}_m(a)$ and $a^n \equiv 1 \pmod{m}$, prove that $k|n$.

(10) 6. Use the method of lifting solutions to find all solutions of the congruence

$$x^3 \equiv 7 \pmod{25}.$$

(10) 7. State and prove Euler's Theorem (on raising numbers to a power \pmod{m} .)

(10) 8. In the RSA method of public cryptography suppose that you have chosen $p = 5$, $q = 13$, $e = 5$, $m = pq = 65$.

a) Calculate the decode exponent d . Recall, d is the multiplicative inverse of e modulo the least common multiple $[p - 1, q - 1]$.

b) Suppose that we start with a message M_0 (expressed as a number) with $0 < M_0 < m$, $(M_0, m) = 1$. Explain how to encode the message and then how to decode the message.

c) What is it that allows the RSA method to be secure and yet public?