INTRODUCTION TO NUMBER THEORY
Exam 3
April 27, 2009

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

(24) 1. Short Answer.

(3) a) Give a reduced residue system \((\text{mod } 12)\).

(3) b) How many solutions does the congruence \(8x \equiv 24 \pmod{28}\) have? (That is, how many distinct values \((\text{mod } 28)\))? 

(3) c) Find \(28! \pmod{29}\).

(3) d) State the Factor Theorem for congruences \((\text{mod } p)\).

(3) e) Suppose that the congruence \(f(x) \equiv 0 \pmod{5}\) has 2 distinct solutions and that \(f(x) \equiv 0 \pmod{7}\) has 3 distinct solutions. How many solutions does the congruence \(f(x) \equiv 0 \pmod{35}\) have?

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

(3) g) Let \(p = 2^k + 1\) be a Fermat prime. What are the possible orders for elements \((\text{mod } p)\). Explain.

(3) h) Let \(f(x)\) be a polynomial with integer coefficients and \(a\) an integer such that \(f(a) \equiv 0 \pmod{7}\) and \(7|f'(a)\). How many solutions does the congruence \(f(x) \equiv 0 \pmod{7^2}\) have with \(x \equiv a \pmod{7}\). Give all possibilities.
(10) 3. Find all integers $x$ with $200 < x < 400$ satisfying the system

$$x \equiv 2 \pmod{25}$$

$$x \equiv 1 \pmod{8}$$

(Do not use trial and error.)

(8) 4. Let $p, q$ be distinct primes greater than 5 and say the decimal expansion of $\frac{1}{25pq}$ is given by

$$\frac{1}{25pq} = .a_1a_2\ldots a_ia_1c_1c_2\ldots c_k$$

with $i, k$ minimal. Find the values $i, k$ given that $\text{ord}_p(10) = 6$ and $\text{ord}_q(10) = 8$. 
(10) 5. State and prove Euler's theorem (on raising numbers to a power (mod $m$)). You may assume a key lemma.

(10) 6. Given that $x = 3$ is a solution of the congruence $x^3 - x + 1 \equiv 0 \pmod{25}$, lift this value to a solution of the congruence $x^3 - x + 1 \equiv 0 \pmod{125}$. (You don't need to find other solutions.)
7. Prove that if \( p \) is a prime and \( x^2 \equiv 1 \pmod{p} \), then \( x \equiv \pm 1 \pmod{p} \).

8. In the RSA method of public cryptography, let \( p, q \) be distinct large primes, \( m = pq \), \( e \) the encoding exponent, \( d \) the decoding exponent, and \( M_0 \) the message to be sent, expressed as a number less than \( m \).
   a) What is the defining relationship between \( d \) and \( e \) ?

   b) Explain how to encode the message \( M_0 \), and then how to decode the encoded message.

   c) What is the key theorem needed for proving that the decoded message is the same as the original message.

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