TEST 3

(Math 258)

1. (a) The expression $a \equiv b \bmod m$ means: (40 pts)

   A. $a = bm$ B. $m \mid a + b$ C. $m \mid a - b$ D. $a \mid b + m$

   (b) Prove that if a|bc, where $a, b, c \in Z_{>0}$, and **gcd**(a,b) = 1, then $a|c$.

   (c) Prove or disprove: If $ac \equiv bc \bmod m$, where $a, b, c, m \in Z_{>0}$, then $a \equiv b \bmod m$.

   (d) True or False: The expression $a \equiv b \bmod m$ means that a and b are equal in Z_m.

   (e) True or False: 10 = 2 in Z_4 .

   (f) True or False: Z_4 is a field .

   (g) Is F = {1, -1, i, - i } an Abelian group with "+" ?

   (h) Find the smallest field with 2 elements.

2. Use the *Extended Euclidean Algorithm* to write the gcd(277,123) as a linear combination of 277 and 123. Use that relation to find the inverse of 123 in Z_{277}. (20 pts)

3. (a) Encrypt the message "MATH IS FUN" by translating the letters into numbers, applying the encryption function given below, and then translating the numbers back into letters. The function is: $f(x) = (p+13) \bmod 26$. (10 pts)

(b) Decrypt the encrypted message below, using the Caesar cipher:

WHVW WRGDB

4. Show that if a is an odd integer, then $a^2 \equiv 1 \bmod 8$. (10 pts)

5. Solve the congruence $4x \equiv 5 \bmod 9$. List at least three integers that are solutions of the congruence. (10 pts)

6. Solve the system of congruences: (10 pts)

$$x \equiv 2 \bmod 3$$
$$x \equiv 1 \bmod 4$$
$$x \equiv 3 \bmod 5.$$