Math 210

Second Hour Exam

Name _____

Notes:

1. Show your work. Answers given without indication of how you got the answer may not receive credit. **This is particularly important on this exam.**
2. Calculators are permitted on this exam. In problems involving calculating a number, however, it is sufficient to leave the calculation in a form in which it can be entered into a calculator (**except where a number is called for in the problem**). If you do use a calculator, you should include this "pre-calculator" expression as part of your answer.

Tuesday, March 1
Happy St. David's Day (Dydd Dewi Sant hapus iawn I bawb)!
100 pts.

I. Some definitions. Please give brief definitions of the following terms (5 pts. each)

a. Greatest common divisor (of two positive integers **m** and **n**)

b. A prime number

c. Relatively prime (said of two positive integers **m** and **n)**

d. A multiplicative inverse mod **n** (i.e., in Z_n)

II. Binary, octal, hexadecimal, arithmetic, and integer representation.

1. (15 pts.). Convert the decimal number 90 to

   a. Base 2

   b. Base 8

   c. Base 16

2. (15 pts.) Do the following arithmetic problems base 2 (without conversion, except to check your work). Please include enough of your work that I can see that you are doing this work base 2 (i.e., converting to base 10, doing the arithmetic, then converting back to base 2 is not sufficient).

a. 1101
- 11
---

b. 1101
*11 (multiplication)
---

c. 1101 divided by 11 (quotient and remainder)

3. (10 pts.) Briefly describe the following schemes for representing negative integers.

a. One's complement

b. Signed magnitude

c. Excess (bias) notation

d. Two's complement.

4. (10 pts) Find the internal (two's complement) representation of -90, writing your answer in hexadecimal. Assume a 32 bit word length.

III. Number theory for encryption. In the following exercises **it is particularly important to show your work**. Answers given without supporting work may not receive credit.

1. (10 pts.) Use the procedures developed in class to find the greatest common divisor of 15 and 77, finding integers **x** and **y** such that GCD(15, 77) = **x***15 + **y***77.

2. (10 pts.) Suppose that we know that $11*21 - 10*23 = 1$.

a. What is the greatest common divisor of 21 and 23?

b. Find the multiplicative inverse of 21 mod 23. Your answer should be a number between 0 and 23.

b. Solve the equation $21*x = 15 \bmod 23$. Again, your answer should be a number between 0 and 23.

IV. (10 pts.) Three questions on the RSA encryption algorithm.

a. What steps does Bob take to create a public and a private key for RSA encryption? What does Bob publish, and what does he keep private?

b. Alice wishes to send Bob a message in the form of a number x. What does Alice do to encrypt her message, and what does she send to Bob?

c. What does Bob compute to decrypt Alice's message?