Math 103: other homework problems

Several problems were not used during the second instantiation of this course. I wanted to reduce the workload for students, and I also decided *not* to attempt to compute multiplicative inverses mod a prime. Although this is discussed in the (nominal) text, when I tried it the first semester, my lack of success in teaching it was notable.

A secret sharing problem

This problem was assigned together with the first writing assignment on medical record privacy. I assigned it in order to get the students to think a bit about secret sharing. I believe the problem was a bit too difficult.

A farm is managed by two committees. There's a combination lock for watering which is kept secret. Each committee must contribute part of the secret combination, which is 203.

The corn committee consists of Albert, Betty, and Charlie. At least two of the three people on this committee must consent to open the lock.

The wheat committee consists of Betty, Debbie, Edward, Fran, Gilda, and Harry. At least four of these six people must consent to open the lock.

Give everyone mentioned numbers which will allow this to occur. Note that what you could do is "share a secret number" over the corn committee, and then "share another secret number" over the wheat committee, and make the combination (203) the sum of the two numbers.

You might also want to make Betty's life easier by arranging that she only needs to remember one x value and one y value which would work in either committee's considerations.

You should tell me:

- Your polynomial for the corn committee, and the numbers you give each member of the corn committee.
- Your polynomial for the wheat committee, and the numbers you give each member of the wheat committee. Note that the degree of this polynomial should be …*

You don't need to make up anything very complicated. I just want the numbers and the polynomials so I can check your understanding of the "protocol".

Homework on multiplicative inverses

These problems would be useful if students knew or understood multiplicative inverses. Problem 2 asked people about a certain transposition cipher, and problem 3 was an early attempt to have people work together.

1. Do problem # 6 on page 30 of the text.

FINALLY, AN ASSIGNMENT FROM THE BOOK! IF YOU WANT EVERYTHING ON ONE PAGE, HERE'S THE PROBLEM:

---

* When we shared a secret so that *two* people were necessary, the degree used was 1: $ax + b$. When we shared a secret so that *three* people were necessary, the degree used was 2: $ax^2 + bx + c$. Now we will need …

6. (a) Compute integers x and y with the property that

$$1 = 17x + 55y.$$

(b) Compute $(2/17)$ mod 55 and $(2/55)$ mod 17.
I THINK THE TEXTBOOK WANTS SOLUTIONS TO $17x = 2 \bmod 55$ AND $55x = 2 \bmod 17$.
TRY MULTIPLYING THE EQUATION YOU GET BY 2.

2. A secret message is being sent in a transposition cipher. A integer a between 1 and 12 is selected. The following process is used: the message is divided into chunks of 12 letters each. In each chunk, we imagine the letters L_1, L_2, …, L_{12} interchanged according to the following rule:

The letter in the j^{th} position gets changed to the $(a \cdot j)^{\text{th}}$ position, where multiplication is done mod **13**.

The following 12 letter message is encrypted using this procedure (it is the beginning of a secret about making bread):

Plaintext `BETTER BATTER` (but no spaces will be used in encryption!)

Ciphertext `E T E B R T T B R E T A`

Question: what is the key, a, in this case? Support your answer with some reasoning.

3. Your number is 1432†. Assume that the following statement is true:

9001 is a prime number.

a) Find the multiplicative inverse of your number mod 9001. Hand in your work for this. Also, verify that your answer is correct, by showing that the product of your answer and the number you began with is 1 more than an integer multiple of 9001. (So you just need to write the equations, with all the integers shown. I hope/assume that arithmetic will be done "by silicon".)

b) There were two different numbers given out. Two different inverses will be found. The product of the two inverses will be an encoded** pair of letters indicating a recent foe of Rutgers. The first team of people (at least two on a team, please) to identify this pair of letters via e-mail to me will win a prize! Some evidence supporting your solution should also be given in the message. Please identify all members of your team in the message.

---

† There were two versions of this assignment. Half the class was to get the version with 8414 here. Alternately, I was going to pass around two sign-up sheets, as shown on the next page.

** AS BEFORE:
The alphabet has 26 letters. Suppose we associate each letter with a two-digit number in the simplest way: `A` $\to$ 01, `B` $\to$ 02, … , `Z` $\to$ 26. Thus the word `WIGGLE` would be associated to the number 230907071205 (`W` is the 23^{rd} letter of the alphabet, `I` is the 9^{th} letter of the alphabet, etc.).

Your number is: 1432

Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________

RECORD YOUR NUMBER AS YOU SIGN THIS RECEIPT!!!

Your number is: 8414

Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________
Name ____________________