CSU200 Discrete Structures   Professor Fell   Fall 2004
Written Homework 2   Due: Friday, 10/6/2004
at the start of class

We expect your homework to be neat, organized, and legible. If your handwriting is unreadable, please type. We will NOT accept pages that are ripped from a spiral notebook. Please use 8.5" by 11" loose-leaf or printer paper.

1. The **ISBN** (International Standard Book Number) is a 10 digit code $x_1 x_2 \cdots x_{10}$ that is assigned to a book and appears on the back cover of most new books. The ISBN for "Discrete Mathematics, second edition" by Hein is 0-7637-2210-3. In general, the 10 digits consist of a block identifying the language, the publisher, the particular book, and a 1-digit check digit that is a digit or the letter X which stands for 10. The check digit is picked so that the sum

$$\left(1\cdot x_1 + 2\cdot x_2 + 3\cdot x_3 + 4\cdot x_4 + 5\cdot x_5 + 6\cdot x_6 + 7\cdot x_7 + 8\cdot x_8 + 9\cdot x_9 + 10\cdot x_{10}\right) \bmod 11 = 0.$$

The check digit is used to check errors in the digits or misplaced digits.
For the Hein book, we have

$$1\cdot 0 + 2\cdot 7 + 3\cdot 6 + 4\cdot 3 + 5\cdot 7 + 6\cdot 2 + 7\cdot 2 + 8\cdot 1 + 9\cdot 0 + 10\cdot 3$$
$$= \left(0+14+18+12+35+12+14+8+0+30\right) \bmod 11 = \left(3+7+1+2+1+3+8\right) \bmod 11 = 0.$$

a) Give the name and ISBN number for 2 other books and check (showing your work as I did above) that the check sum is correct.

b) The first 9 digits of the ISBN for "Signal Processing in C" by Reid and Passin are 0-471-52713-. What is the check digit?

c) The ISBN for my well-work copy of "The Diamond Age" by Neal Stephenson is 0-553-5D331-4. The D stands for a digit that got rubbed out. What is this digit?

(Note: This problem is based on problems 54, 55, 56, 57 on page 168 of "Discrete Mathematics and its Applications," by Rosen.)

2. **The equation $ax \bmod n = b$ has a solution *x* if and only if gcd(*a*,*n*) divides *b*.**
Use this fact to prove that:

If $n > 1$ and we define the function $f(x) = (ax+b) \bmod n$ for all x in $\mathbb{Z}_n = \{0,1,\cdots,n-1\}$ then $f(x) \neq x$ for any x in $\mathbb{Z}_n$ if and only if gcd(*a*-1, *n*) does not divide *b*.

3. If we let the letters A, . . ., Z correspond to the integers, 0, . . ., 25, we can create a simple cipher of the form *c(x)* = *(ax + b)* mod 26.

a. Use the statement at the start of problem 2 to prove that the values of *c(x)* will be distinct if and only if gcd(*a*, 26) = 1.

b. For each value of *b* (0 ≤ *b* ≤ 25) find all values of *a* (0 ≤ *a* ≤ 25) that insure that all the values *c(x)* for 0 ≤ *x* ≤ 25 are distinct and *c(x)* ¹ *x* for any *x* (0 ≤ *x* ≤ 25).