CSE 321: Discrete Structures Spring 2004

PROBLEM SET 4
Due Friday, April 30, 2004, in class

Instructions: Same as for Problem Set 1.

All exercise numbers refer to the number in Rosen's book, 5th Edition.

1. Section 3.3, Exercise 40.

2. Find the rightmost digit (digit in unit place) when the following numbers are written in decimal:

   (a) 32^{631}

   (b) $7^{7^{14}}$

   (c) $1! + 2! + 3! + \cdots + 100!$

   (If you follow the method I outlined in class, you should never have to compute a product greater than $5 \cdot 5$.)

3. (a) Let a, b be positive integers. Define $S_{a,b}$ to be the set of all **positive** integers that can be written in the form $sa + tb$ for integers s, t. Prove that the smallest element in $S_{a,b}$ (why should it exist?) is in fact equal to $\gcd(a, b)$.

   (b) Prove that the linear equation $ax + by = c$ where a, b, c are integers and $a \neq 0$ and $b \neq 0$ has a solution in integers (x, y) if and only if $\gcd(a, b)|c$.
   (Do not forget to show both directions of the "if and only if")

4. Use Euclid's algorithm to compute the following showing all the intermediate steps.

   (a) $\gcd(2274, 174)$

   (b) The inverse of $144 \mod 233$.

5. In this exercise, you will explore an instance how modular arithmetic can be used for error detection. The specific example we will work with is the ISBN (International Standard Book Number) system to identify books published worldwide.

   The ISBN of a book is usually found on the last cover page (for instance, for your textbook, the ISBN is 0072424346). The current standard uses a 10-digit code where the first nine digist identify the book and the last digit is a *check digit* to detect mistakes in, say, typing or communicating ISBNs. An ISBN can thus be viewed as a sequence of 10 digits $x_1 x_2 \ldots x_{10}$ where for all $i = 1, 2, \ldots, 9$, x_i is one of the digits $0, 1, 2, \ldots, 9$. The check digit x_{10} has 11 possible values $\{0, 1, 2, \ldots, 10\}$ (if the check digit happens to be a 10, it is denoted by the roman numeral X).

   Modular arithmetic is used to assign a check bit to a particular book in the following way. Suppose the first nine digits $x_1, x_2, \ldots, x_9$ of an ISBN have been chosen (the exact way these

are assigned by publishers is not important to us here). The check digit x_{10} is determined by the following congruence:

$$1x_1 + 2x_2 + \cdots + 8x_8 + 9x_9 + 10x_{10} \equiv 0 \pmod{11} .$$

(If you are curious, you can check that the ISBN 0072424346 for your textbook satisfies the above!)

Now to your exercises.

(a) Let $x_1x_2 \cdots x_9x_{10}$ be the correct ISBN of a book. Suppose that, during the billing procedure, a single error has been made in entering the ISBN; i.e, in the i'th place for some i, y_i is printed instead of x_i where $x_i \neq y_i$. Prove that this error can be *detected*; formally, show that the resulting 10 digit sequence is not a valid ISBN.

(b) Same as above, except now consider the error where two *unequal* digits x_i, x_j are swapped, that is an error of the form

$$x_1x_2 \cdots x_ix_{i+1} \cdots x_jx_{j+1} \cdots x_9x_{10} \longrightarrow x_1x_2 \cdots x_jx_{i+1} \cdots x_ix_{j+1} \cdots x_9x_{10}$$

where $x_i \neq x_j$.

6. Section 3.4, Exercise 44.

7. Let a, b and c be integers and m be a positive integer.

(a) Prove that $ab \equiv ac \pmod{m}$ if and only if $b \equiv c \pmod{\frac{m}{\gcd(a,m)}}$.
(Again, do not forget to show both directions of the "if and only if".)

(b) Show that if $ab \equiv ac \pmod{m}$ and $\gcd(a, m) = 1$, then $b \equiv c \pmod{m}$.

(c) (Just for fun, *no need to turn anything in*) Using part (b) above, and working through Section 2.6, Exercises 17(a,b), prove Fermat's Little Theorem which states: If p is a prime number, then $a^p \equiv a \pmod{p}$ for all integers a.