McGill University
Math 240: Discrete Structures 1
Assignment 4: due Friday, November 11, 2005

Reading: Text 2.4: The Integers and Division, 2.5: The Integers and Algorithms, 2.6 Applications of Number Theory

Questions:

1. (a) Using the Euclidean Algorithm, find $m, n \in \mathbb{Z}$ such that $1 = 13422m + 10001n$.
   (b) Using (a), show that $\gcd(13422, 10001) = 1$.
   (c) Using (a), find $c \in \mathbb{N}$ with $c < 13422$ such that $10001c \equiv 1 \bmod 13422$. Is c unique? Why?
   (d) Using (c), find all solutions of the congruence $10001x \equiv 2341 \bmod 13422$.
   (e) Using (a), find all solutions of the system of congruences

$$x \equiv 25 \bmod 10001$$
$$x \equiv 36 \bmod 13422.$$

   Find the smallest solution with $x > 0$.

2. Using the Chinese Remainder Theorem, find all solutions to the system of congruences

$$x \equiv 2 \bmod 5$$
$$x \equiv 3 \bmod 7$$
$$x \equiv 4 \bmod 12.$$

3. Suppose that $b \equiv a^{67} \bmod 91$ and that $\gcd(a, 91) = 1$.
   (a) Find $k \in \mathbb{N}$ such that $b^k \equiv a \bmod 91$.
   (b) If $b = 53$ and $0 < a < 91$, what is a?

4. (a) Use Fermat's Little Theorem to compute

$$3^{302} \bmod 5, \quad 3^{302} \bmod 7, \quad 3^{302} \bmod 11.$$

   (b) Use your results from part (a) and the Chinese Remainder Theorem to compute

$$3^{302} \bmod 385.$$