CSI 2101 Discrete Structures — Winter 2011
Prof. Lucia Moura — University of Ottawa

Homework Assignment #2 (100 points, weight 6.25%)
Due: Friday, March 18, at 4:00pm (in lecture)

Number Theory

1. (15 points) Show that if a, b, and m are integers such that $a \equiv b \pmod{m}$, then $gcd(a, m) = gcd(b, m)$.

2. (20 points)

   (a) Find the inverse of 13 modulo 2436, using the Extended Euclidean Algorithm. Show your steps.

   (b) Solve the congruence $13x \equiv 2 \pmod{2436}$, by specifying all the integer solutions x that satisfy the congruence.

3. (15 points) (Chinese Remainder Theorem) Find all solutions to the system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 1 \pmod{4}, \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

4. (25 points)

   (a) Use Fermat's little theorem to compute: 4^{101} **mod** 5, 4^{101} **mod** 7, 4^{101} **mod** 13.

   (b) Use your results from part (a) and the Chinese Remainder Theorem to compute 4^{101} **mod** 455. (note that $455 = 5 \times 7 \times 13$).

5. (25 points)
   Consider the RSA Cryptosystem. Bob's public keys are $n = 4757$ and $e = 299$. Alice uses these keys and sends Bob a message M encoded as $C = 1080$. However, since Bob used n too small, a malicious eavesdropper, Eve, is able to factor n as a product of two prime numbers: $n = 4757 = 71 \times 67$.
   Show how Eve can use this information to decode the message C in order to discover the original message M; show your work and give the original message M.

   Requirements:

   - In order to compute the inverse of a (mod m), when $gcd(a, m) = 1$, use the extended Euclidean algorithm. Show your work.
   - In order to compute b^a(mod m) you may use some fast exponentiation algorithm available over the internet, such as the one found at:
     `http://www.math.umn.edu/~garrett/crypto/a01/FastPow.html`