CMSC 441
Section 0201
Spring 2008
Homework 8

Reading Assignment:

1) Listen to Camille Saint-Saens' Danse Macabre
2) Read Chapter 31 of the text, pages 849-861 and the handout on the extended Euclidean algorithm http://www.csee.umbc.edu/~lomonaco/s08/441/handouts/Extended-Euclidean-Algorithm.pdf
3) Study ahead by reading Section 5 of Chapter 31 of the text.

Homework:

1) Use the extended Euclidean algorithm to find $g = GCD(a_1, a_2)$ integers s_1 and s_2 such that $s_1 a_1 + s_2 a_2 = g$, where

i) $(a_1, a_2) = (99, 78)$

ii) $(a_1, a_2) = (899, 493)$

2) Also find $\lambda = LCM(a_1, a_2)$ for i) and ii) in 1) above.

3) Find the multiplicative inverse of $7 \pmod{1023}$ using the extended Euclidean algorithm.

4) Let a and b be integers, and let $n = 1 + \lfloor \lg(b) \rfloor$ denote the number of bits in the binary expansion of b. Moreover, let

$$b = \sum_{j=0}^{n-1} b_j 2^j$$

be the binary expansion of b. The method of repeated squaring is defined by the following formula

$$a^b = a^{\sum_{j=0}^{n-1} b_j 2^j} = \prod_{j=0}^{n-1} \left(a^{\left(2^j\right)} \right)^{b_j}$$

An algorithm implementing this formula is given below:

```
Repeated_Squaring( a , b )
        Prod ← 1
        Sq ← a
        for j ← 0 to n − 1
                do if ( b_j = 1 )
                        then Prod ←Prod*Sq
                sq ← Sq*Sq
        return( Prod )
end
```

Compute $(73)^{57} \pmod{101}$ by the method of repeated squaring.