Assignment 3 - Due Monday February 2

(1) **Modular Arithmetic - Months and Months** It is now February.
   (a) What month will it be in 35 months?
   (b) What month will it be in 219 months?
   (c) What month will it be in 120,219 months?
   (d) What month was it 89 months ago?

(2) **Airline Tickets** An airline ticket identification number is a 14-digit number The check digit is the number between 0 and 6 that represents what the identification number is equivalent to using a mod 7 clock. Thus, the check digit is just the remainder when the identification number is divided by 7. What is the check digit for the airline identification number 1 006 1559129884?

(3) **Why Three?** In the UPC, why do they use 3 as the number to multiply every other digit by rather than for example 6? To get to the reason, multiply every digit from 0 to 9 by 3 and look at the answers mod 10. Do the same with 6 and compare the results. Are there other numbers besides 3 that would work effectively? What would be the first number you would try?

(4) **Encoding and Decoding** The two public numbers for an RSA code are given as $e = 17$ and $W = 143$.
   (a) Encode the message "2".
   (b) The corresponding decoder is 113. Check that this is correct: 143 is the product of the primes 11 and 13, and $(11-1)(13-1) = 120$. So we need to show that $113 * 17 \equiv 1 \mod 120$. Do this by finding a number k such that $113 * 17 = 120k + 1$.
   (c) Suppose that somebody has submitted the encoded message "3". Describe what you would need to do to find the original message. (You don't need to do the actual calculations.)

(5) **Creating a Code** Suppose you wish to devise an RSA coding scheme for yourself. You select $p = 3$ and $q = 5$. Compute $W = pq$ and $m = (p-1)(q-1)$. Find (by trial and error if necessary) possible values for e and d.