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?
   Solution: There are 12 months in a year, so we need to do our calculations mod 12. $35 \equiv 11 \mod 12$ (or $-1 \mod 12$), so that is January (the previous month.)
   (b) What month will it be in 219 months?
   Solution: $219 = 18 * 12 + 3$, so $219 \equiv 3 \mod 12$, three months after February gives us May.
   (c) What month will it be in 120,219 months?
   Solution: $120,000$ is a multiple of 12, so $210,219 \equiv 219 \mod 12 \equiv 3 \mod 12$ (as found in the previous part), so this is again May.
   (d) What month was it 89 months ago?
   Solution: $-89 \equiv -5 \mod 12 \equiv 7 \mod 12$, this gives us September.

(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?
Solution: $10,061,559,129,884/7 = 1,437,365,589,983.428571429$, and $10,061,559,129,884 - 7 * 1,437,365,589,983 = 3$, so

$$10,061,559,129,884 \equiv 3 \mod 7.$$

So the check digit is 3.

(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?

Solution:

digit	digit $*$ 3	mod 10	digit $*$ 6	mod 10
0	0	0	0	0
1	3	3	6	6
2	6	6	12	2
3	9	9	18	8
4	12	2	24	4
5	15	5	30	0
6	18	8	36	6
7	21	1	42	2
8	24	4	48	8
9	27	7	54	4

We see that the answers mod 10 are all distinct when we have multiplied by 3, whereas there are repeating answers when we multiply by 6 (because the answers would have to be even in that case – 10 and 6 have the common divisor 2). This means that one would catch fewer errors when one would use 6. For example, there is no distinction in the answers whether you had written 2 or 7.

The number that you choose should have no common divisors with 10, so other possibilities are 7 and 9.

(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".
Solution: You need to evaluate $2^{17} \mod 143$. We begin by taking a sequence of squares: $2^2 \equiv 4 \mod 143$, $2^4 \equiv 4^2 \mod 143 \equiv 16 \mod 143$, $2^8 \equiv 16^2 \mod 143 \equiv 256 \mod 143 \equiv 113 \mod 143 \equiv -20 \mod 143$, $2^{16} \equiv 400 \mod 143 \equiv 114 \mod 143$. Now, $2^{17} \equiv 2^{16} * 2 \mod 143 \equiv 114 * 2 \mod 143 \equiv 85 \equiv 143$. the coded messgae is "85".

(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 $113 * 17 = 120k + 1$.
Solution: $113 * 17 = 1921$, and $113 * 17 - 1 = 1920$, this divides evenly by 120, and $k = 1920/120 = 16$.

(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.)

Solution: You would need to evaluate $3^{113} \mod 143$. Just in case you are curious. You can do this by taking squares in the following way: $3^2 \equiv 9 \mod 143$, $3^4 \equiv 81 \mod 143$, $3^8 \equiv 81^2 \mod 143 \equiv 126 \mod 143 \equiv -17 \mod 143$, $3^{16} \equiv (-17)^2 \mod 143 \equiv 3 \mod 143$, $3^{32} \equiv 3^2 \mod 143 \equiv 9 \mod 143$, and $3^{64} \equiv 81 \mod 143$, so $3^{113} = 3^{64+32+16+1} = 3^{64} * 3^{32} * 3^{16} * 3 \equiv 81 * 9 * 3 * 3 \mod 143 \equiv 81^2 \mod 143 \equiv 126 \mod 143$. So the original message was "126".

(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.
Solution: $W = 15$ and $m = 8$. For e we need to take a number which has no common divisors with 8. I will illustrate a couple of different solutions.

If you take $e = 3$, you need to take d such that $e * d \equiv 1 \mod 8$. You can find d by simply taking multiples of $e = 3$ until the answer is $1 \mod 8$. The smallest possible value for d would be $d = 3$, since $3 * 3 = 9 \equiv 1 \mod 8$. So here we have $e = d = 3$.

If you take $e = 5$, you also find that $d = 5$, since $5*5 = 25 \equiv 1 \mod 8$.

If you take $e = 7$, $d = 7$ works as well.

Note that if you take $e = 9$, you can take $d = 1$. This means that the number did not get changed by the encoding process, so that is not a good encoder!

By the way, I would not recommend using these primes in any case. It is too easy to find out that if you encode twice you get the original number back.