CS 310-0
Homework Assignment No. 7

Due Fri 5/26/2000

1. Find the smallest positive integer a such that the equation $60 * x = a$ has a solution in $\mathbb{Z}_{160}$. Solve it.

2. Find all elements x in $\mathbb{Z}_{15}$ such that $x^2 = 3x - 2$.

3. Compute $6^{12} \bmod 41$. Then solve the equation $x^3 = 4$ in $\mathbb{Z}_{41}$.

4. Prove that there are no positive integers x, y, z such that $3 \not| xyz$ and $x^3 + y^3 = z^3$. (Hint: think modulo 9.)

5. Let N be the number $N = 7 \uparrow\uparrow 5 = 7^{7^{7^{7^{7}}}}$. Find the two rightmost digits of N in base 10. (Hint: find $N \bmod 100$.)

6. In a bookstore there are 2,000 books. After selling some of them the store owner notices that they can be arranged in shelves of 13 books, leaving 12 left. If he puts 15 books on each shelf then he has 2 left. Arranging them in shelves of 16 books then there are 8 left. How many books were sold?

7. We have intercepted a secret message from the enemy encrypted with the RSA algorithm. The encoding is $A = 01, B = 02, C = 03, \ldots, Z = 26$, and the public encryption key used by the enemy is $(n, e) = (31732031, 29553281)$. For instance, the word DOG would be encrypted as follows. First it is encoded: $DOG = 041507$. Then it is encrypted: $041507^{29553281} \bmod 31732031 = 5470487$. The encrypted message that we have intercepted is $m' = m^e \bmod 31732031 = 18091168$. Your mission (if you wish to accept it) is to decrypt (and decode) the message. In order to do that, use the following steps (you will need some computer algebra system such as Maple to do the computations):[1]
   1) Find the prime factors p and q of $n = 31732031$.
   2) Find $\phi(n)$.
   3) Find $d = e^{-1} \bmod \phi(n)$. The decryption key is (n, d).
   4) Decrypt the secret message by computing $m = {m'}^{d} \bmod n$.

[1] In Maple you may use "ifactor" to find the prime factors of n, and "mod" for computations modulo n. Remember to use the ampersand in expressions of the form "$a\&\hat{}b \bmod n$" in Maple (so that Maple uses the efficient algorithm to compute powers modulo n.) Basically, the computations to be performed are: find p and q with "ifactor(n)", find $\phi(n) =$ "$(p-1)*(q-1)$", find $d =$ "$e\&\hat{}(-1) \bmod \phi(n)$", find $m =$ "$m'\&\hat{}d$ mod $\phi(n)$". Finally, decode m.