M314 REVIEW EXERCISES 15.03.17

You're encouraged to discuss these problems with other students in the class.

1. Find common solutions to these systems of linear congruences:
   a) $x \equiv -4 \ (mod\ 13)$
      $x \equiv 5002 \ (mod\ 5)$

   b) $x \equiv 3 \ (mod\ 4)$
      $x \equiv 0 \ (mod\ 6)$

   c) $4x \equiv 2 \ (mod\ 6)$
      $3x \equiv 5 \ (mod\ 8)$

2. Fermat's Little Theorem: for any prime p, and for all integers a we have $a^{p-1} \equiv 1 \ (mod\ p)$.
   a) For some prime p and integer $0 \geq a < p$, what is the congruence class of $a^p \ (mod\ p)$?

   b) Figure out what day of the week it will be in 2016^{2016} many days.

3. Your public key is $(p, e) = (13, 7)$. Your secret key is $d = 7$. Let one of your fellow students use your public key to send you an encrypted version of a number $2 \leq m < p$ and decrypt it using your secret key. Verify if the decrypted message is correct.

   If you know someone's public key (p, e) where p is prime, to encrypt a message m, evaluate $m^e \ (mod\ p)$. Give this to them. They have a secret key d and can decrypt your message by evaluating $(m^e)^d \ (mod\ p) = m$, because e, d were generated so that $e \cdot d \equiv 1 \ (mod\ p-1)$, and therefore $m^{e \cdot d} \equiv m \ (mod\ p)$.

4. A modification on Fermat's Little Theorem that is useful for RSA is the following.

   Let $p,\ q$ be primes and $n = p \cdot q$. Then for any integer $0 < m < n$,and all integers k:

   $$m^{k \cdot (p-1)(q-1)+1} \equiv m \ (mod\ n).$$

   Pick some $p,\ q,\ k$ such that $k \cdot (p-1)(q-1)$ splits up into $e \cdot d$. You have just generated an RSA public key cryptosystem. You can give the public key (e, n) to a fellow student, so they can send you an encrypted message $c = m^e \ (modn)$. Then you can decrypt it using $c^d \equiv m \ (modn)$.

   Example: If I pick $p = 7$, $q = 5$ and $k = 1$, then $1 \cdot (p-1)(q-1) + 1 = 25$, which splits up into 5 and 5. Then $n = 35$ and I can use $(5, 35)$ as my public key and 5 as my secret key.

   Or I could try to make it harder and pick, say, $p = 7$, $q = 5$ and $k = 3$. Then $3 \cdot (p-1)(q-1) + 1 = 3 \cdot 24 + 1 = 73$. 73 is prime, so it's not gonna work. Let's try $k = 5$. Then $5 \cdot 24 + 1 = 121$. Now I can use $e = 11,\ d = 11,\ n = 35$.