HOMEWORK 7

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (3.1) Solve the following congruences.
  (a) $x^{19} = 36 \mod 97$
  (b) $x^{137} = 428 \mod 541$
  (c) $x^{73} = 614 \mod 1159$
  (d) $x^{751} = 677 \mod 8023$
  (e) $x^{38993} = 328047 \mod 401227$ (Hint: $402117 = 608 \cdot 661$)

(2) (3.4) Recall from Sect. 1.3 that *Euler's phi function* $\phi(N)$ is defined by

$$\phi(N) = \#\{0 \leq k < N \mid \gcd(k, N) = 1\}$$

In other words, $\phi(N)$ is the number of integers between 0 and $N-1$ that are relatively prime to N, or equivariantly, the number of elements of $\mathbb{Z}/N\mathbb{Z}$ that have inverses modulo N.
  (a) Compute the values of $\phi(6), \phi(9), \phi(15)$, and $\phi(17)$.
  (b) If p is prime, what is the value of $\phi(p)$?
  (c) Prove *Euler's formula* for all a satisfying $\gcd(a, N) = 1$

$$a^{\phi(N)} = 1 \mod N$$

(Hint: Mimic the proof of Fermat's little theorem (Theorem 1.24), but instead of looking at all the multiples of a as was done in (1.8), just take the multiples ka of a for values of k satisfying $\gcd(k, N) = 1$).

(3) (3.7) Alice publishes her RSA public key: modulus $N = 2038667$ and exponent $e = 103$.
  (a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?
  (b) Alice knows that her modulus factors into the produce of primes, one of which is $p = 1301$. Find a decryption exponent d for Alice.
  (c) Alice receives the ciphertext 317730 from Bob. Decrypt the message.

(4) (3.9) For each of the given values of $N = pq$ and $(p-1)(q-1)$, use the method described in Remark 3.11 to determine p and q.
  (a) $N = pq = 325717$ and $(p-1)(q-1) = 351520$.
  (b) $N = pq = 77083921$ and $(p-1)(q-1) = 77066212$.
  (c) $N = pq = 109404161$ and $(p-1)(q-1) = 109380612$.
  (d) $N = pq = 172205490419$ and $(p-1)(q-1) = 172204660344$.

(5) (3.15) Use the Miller-Rabin test on each of the following numbers. In each case, either provide a Miller-Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 10 numbers that not Miller-Rabin witnesses for n.
  (a) $n = 1105$
  (b) $n = 294409$
  (c) $n = 294439$
  (d) $n = 118901509$

(e) $n = 118901521$
(f) $n = 118901527$
(g) $n = 118915387$