CS 435	**Homework 3**	Prof. David Nassimi
Data Structures & Algorithms	Number Theory and Cryptography	

1. (a) List all prime numbers between 2 and 100. Use the fact that a composite integer n must have a prime factor $\leq \sqrt{n}$ to limit the search. Thus, a number < 100 is prime if and only if it is not a factor of $\{2, 3, 5, 7\}$. Other useful facts:
   - An integer is divisible by 3 if and only if sum of its digits are divisible by 3.
   - An integer is divisible by 5 if and only if it ends with a 5.

   (b) How many prime numbers are there in your list in the range 2 to 100?

2. (a) Find the Greatest-Common-Divisor (GCD) of the following pair of numbers by finding their prime factorizations: $a = 7623,\ b = 7425$.
   (b) Use Euclid's algorithm to find GCD of the above integers a, b. Use the iterative algorithm. Also show the computation of integers (s, t) so that $\gcd(a, b) = sa + tb$.

3. (a) Find inverse of integers 1 to 10 mod 11. Tabulate the results. You may find the values by inspection.
   (b) Find inverse of integers 1 to 13 mod 14, if they exist. Tabulate the results.

4. Use the iterative GCD algorithm to compute the inverse of 37 mod 121.

5. Use exponentiation method to find each inverse. Recall $x^{-1} mod\ n = x^{\phi(n)-1} mod\ n$.
   (a) Inverse of 5 mod 17
   (b) Inverse of 5 mod 21

6. Let $n = 14 = 2 * 7$.
   (a) Compute and tabulate $5i\ mod\ n$ for $i = 1, 2, \cdots,\ n - 1$. Observe the result is a permutation of $(1, 2, \cdots, n - 1)$, as proved by Lemma 6.

   (b) Compute and tabulate $6i\ mod\ n$ for $i = 1, 2, \cdots,\ n - 1$. Explain why the result is not a permutation of $(1, 2, \cdots, n - 1)$.

   (c) Let Z_{14}^{*} be set of positive integers smaller than 14 and prime relative to 14.
   For each $x \in Z_{14}^{*}$, compute and tabulate a row $xi\ mod\ 14, i \in Z_{14}^{*}$.
   Observe that every row is a permutation of Z_{14}^{*}, as proved by Lemma 8.

7. Let $p = 7$. For each $x = 2,\ 3, \cdots, p - 1$ compute and tabulate a row $(x^{i} \bmod p)$ for $i = 1, 2, \cdots, p - 1$.
   (a) Relate the results to Fermat's Little Theorem.
   (b) Which column gives the inverse, $x^{-1} \bmod p$? Explain.
8. Let $n = 10 = 2 * 5$. Thus, $\phi(10) = (2 - 1)(5 - 1) = 4,\ \ Z_{10}^{*} = \{1, 3, 7, 9\}$.

For each $x \in Z_{10}^*$ compute and tabulate a row $(x^i \bmod n)$ for $i = 1, 2, 3, 4, 5$.
(a) Which column relates to Euler's Theorem? Explain
(b) Which Column relates to Corollary 1? Explain
(c) Which column gives the inverse, $x^{-1} \bmod n$? Explain.

9. Let $n = 10 = 2 * 5$. So, $\phi(n) = (2-1)(5-1) = 4$. For each positive integer $x < n$, compute and tabulate a row $(x^i \bmod n\ )$ for $i = 1$ to 5.
(a) Explain how the results in column 5 relate to Theorem 6.
(b) Explain how the values in column 4 relate to Euler's Theorem.
(c) Explain why the value in column 4 cannot be 1 for any $x \notin Z_n^*$.

10. (RSA Public Key Cryptosystem) Let us pick two prime numbers $p = 41, q = 67$. Then,

$$n = pq = 41 * 67 = 2747$$
$$\phi(n) = (p-1)(q-1) = 40 * 66 = 2640$$

We pick a small prime number s, with $\gcd(s, \phi(n)) = 1$.

$$s = 13.$$

Then,

$$t = s^{-1}\, mod\ \phi(n) = 13^{-1}\, mod\ 2640 = 2437.$$

(This inverse is computed by Euclid's algorithm.)

The public keys are (s, n) and the private key (t, n).

(a) Suppose a sender wants to send a number $x = 2169$. Compute the encrypted message y. Make sure you perform a mod operation after each multiplication so the intermediate results does not become too large. Use the recursive algorithm Power to compute the exponentiation. (You may use an Excel sheet to generate the data.) Show the computation.

(b) Compute the decrypted message z and verify that $z = x$. Show the computation.