SCR3443 – Sem I 2012/13
Tutorial 2: Mathematics for Cryptography

1. Find the results of the following operations.
   a. 22 mod 7
   b. 140 mod 10
   c. -78 mod 13
   d. 0 mod 15

2. Perform the following operations using reduction first.
   a. (273 + 147) mod 10
   b. (4223 + 17323) mod 10
   c. (148 + 14432) mod 12
   d. (2467 + 461) mod 12

3. Perform the following operations using reduction first.
   a. (125 × 45) mod 10
   b. (424 × 32) mod 10
   c. (144 × 34) mod 12
   d. (221 × 23) mod 22

4. Let us assign numeric value to the uppercase alphabet (A = 0, B = 1, . . . Z = 25). We can now do modular arithmetic on the system using modulo 26.
   a. What is (A + N) mod 26 in this system?
   b. What is (A + 6) mod 26 in this system?
   c. What is (Y - 5) mod 26 in this system?
   d. What is (C - 10) mod 26 in this system?

5. Using the Euclidean algorithm, find the greatest common divisor of the following pairs of integers.
   a. 88 and 220
   b. 300 and 42
   c. 24 and 320
   d. 401 and 700

6. Using extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.
   a. 4 and 7
   b. 291 and 42
   c. 84 and 320
   d. 400 and 60

7. Find the value of $\phi(29)$, $\phi(32)$, $\phi(80)$, $\phi(100)$, $\phi(101)$.

8. Find the results of the following, using Fermat's little theorem:
   a. 5^{15} mod 13
   b. 15^{18} mod 17
   c. 456^{17} mod 17
   d. 145^{102} mod 101

9. Find the results of the following, using Fermat's little theorem:
   a. $5^{-1} \bmod 13$
   b. $15^{-1} \bmod 17$
   c. $27^{-1} \bmod 41$
   d. $70^{-1} \bmod 101$

   Note that all moduli are primes.

10. Find the results of the following, using Euler's theorem:
   a. $12^{-1} \bmod 77$
   b. $16^{-1} \bmod 323$
   c. $20^{-1} \bmod 403$
   d. $44^{-1} \bmod 667$

   Note that $77 = 7 \times 11$, $323 = 17 \times 19$, $403 = 31 \times 13$, and $667 = 23 \times 29$.

11. Find the results of the following using the square-and-multiply method.
   a. $21^{24} \bmod 8$
   b. $320^{23} \bmod 461$
   c. $1736^{41} \bmod 2134$
   d. $2001^{35} \bmod 2000$