Due date : June 30, 2016

1) Compute the remainder when 3^{47} is divided by 23.

2) What is the remainder when $22 \times 21 \times 20 \times \cdots 5 \times 4 \times 3$ (note the missing 2) is divided by 23?

3) Using Fermat's little theorem, find the remainder when 3^{40} is divided by 43.

4) Let $n = pq$ where p, q are prime numbers. Consider the list of numbers from 1 to n denoted by $A = \{1, 2, \cdots, n-1, n\}$.

   (i) How many elements in A are divisible by p?

   (ii) How many elements in A are divisible by q?

   (iii) How many elements in A are co-prime to n *i.e.* have no common factors with n? (Hint: Count the number of elements that are neither divisible by p nor by q. These are precisely the elements that are co-prime to pq.)

5) (i) For an RSA cipher, if $p = 3, q = 5$ and $e = 7$, what are n and d.

   (ii) Devise an RSA cipher (with the encoding and decoding powers) starting with the primes $p = 11, q = 13$. Encrypt the value 10 and decrypt it to verify that you recover 10.