**Number theory and Cryptography**

**Module-2**

1. Define Euler totient function.
2. Find the value of the following:
3. (ii) (iii)
4. State and prove Euler’s theorem.
5. State and prove Fermat’s little theorem.
6. Write the statement of Wilson’s theorem.
7. Find the last digit of .
8. Find the last digit of .
9. Use Euler’s theorem find the last digit of .
10. Use Euler’s theorem find the last two digit of .
11. Use Euler’s theorem find the last two digit of .
12. Define Fermat’s number and prove that is divisible by
13. Define a Field with respect to binary operations addition and multiplication.
14. Show that are finite fields w.r.t addition and multiplication modulo 2, 3, 5, and respectively.
15. Show that are not fields w.r.t addition and multiplication modulo and respectively.

**Module-3**

1. Define order of a modulo n. Give an example

2. Find the order of the integers 2, 3 and 5 (a) modulo 17 (b) modulo 19

(c) modulo 23

3. Let the integer have order modulo . Then prove that if and only if ; In particular .

4. Let be an integer have the order modulo and . Prove that has order module .

5. Define Primirtive root. Show that has no primitive root by calculating the orders of and modulo

6. If has a primitive root, then it has exactly of them.

7. Verify that each of the congruences

(i)

(ii)

(iii)

Has four incongruent solutions

8. Verify that 2 is a primitive root of but not of

9. Show that has no primitive root by calculating the orders of and modulo

10. Find two primitive roots of 9 and 10.

**Theory of indices**

**For the following problems (1-3) assume 2 is a primitive root of 13**

1. Use the theory of indices to solve the congruence .

2. Use the theory of indices to solve the congruence .

3. Use the theory of indices to solve the congruence .

4. Use the theory of indices to find the remainder when is divide by by considering 3 is primitive root

.

**Quadratic residues and reciprocity law**

1.Solve the following quadratic congruences:

(i)

(ii)

(iii)

(iv)

2. State and prove Euler’s criterion for quadratic reciprocity.

3. Define Legendre symbol

4. Evaluate the following:

(i) (iii)

(ii) (iv)