



## Basic Number Theory

### SWAYAM Prabha Course Code - S3

<b>PROFESSOR'S NAME</b>	Prof. Shripad Garge
<b>DEPARTMENT</b>	Mathematics
<b>INSTITUTE</b>	Indian Institute of Technology, Bombay
<b>COURSE OUTLINE</b>	This is a basic course in number theory. We begin with integers, prime factorization and develop the contents to study the quadratic reciprocity laws and continued fractions. This course does not require any advanced mathematical training. Some familiarity with group theory will be useful but it is not necessary to understand the course. This is normally offered at the masters level, so some mathematical maturity is expected.

#### COURSE DETAILS

S. No	Module ID/ Lecture ID	Lecture Title/Topic
1	L1	Integers
2	L2	Divisibility and primes
3	L3	Infinitude of primes
4	L4	Division algorithm and the GCD
5	L5	Computing the GCD and Euclid's lemma
6	L6	Fundamental theorem of arithmetic
7	L7	Stories around primes
8	L8	Winding up on 'Primes' and introducing 'Congruences'
9	L9	Basic results in congruences
10	L10	Residue classes modulo $n$

11	L11	Arithmetic modulo $n$ , theory and examples
12	L12	Arithmetic modulo $n$ , more examples
13	L13	Solving Linear Polynomials modulo $n$ – I
14	L14	Solving Linear Polynomials modulo $n$ – II
15	L15	Solving Linear Polynomials modulo $n$ – III
16	L16	Solving Linear Polynomials modulo $n$ – IV
17	L17	Chinese remainder theorem, the initial cases
18	L18	Chinese remainder theorem, the general case and examples
19	L19	Chinese remainder theorem, more examples
20	L20	Using the CRT, square roots of 1 in $Z_n$
21	L21	Wilson's Theorem
22	L22	Roots of polynomials over $Z_p$
23	L23	Euler $\phi$ -function - I
24	L24	Euler $\phi$ -function - II
25	L25	Primitive Roots - I
26	L26	Primitive Roots - II
27	L27	Primitive Roots - III
28	L28	Primitive Roots - IV
29	L29	Structure of $U_n$ - I
30	L30	Structure of $U_n$ - II
31	L31	Quadratic residues
32	L32	The Legendre symbol
33	L33	Quadratic reciprocity law - I

34	L34	Quadratic reciprocity law - II
35	L35	Quadratic reciprocity law - III

**References if Any:**