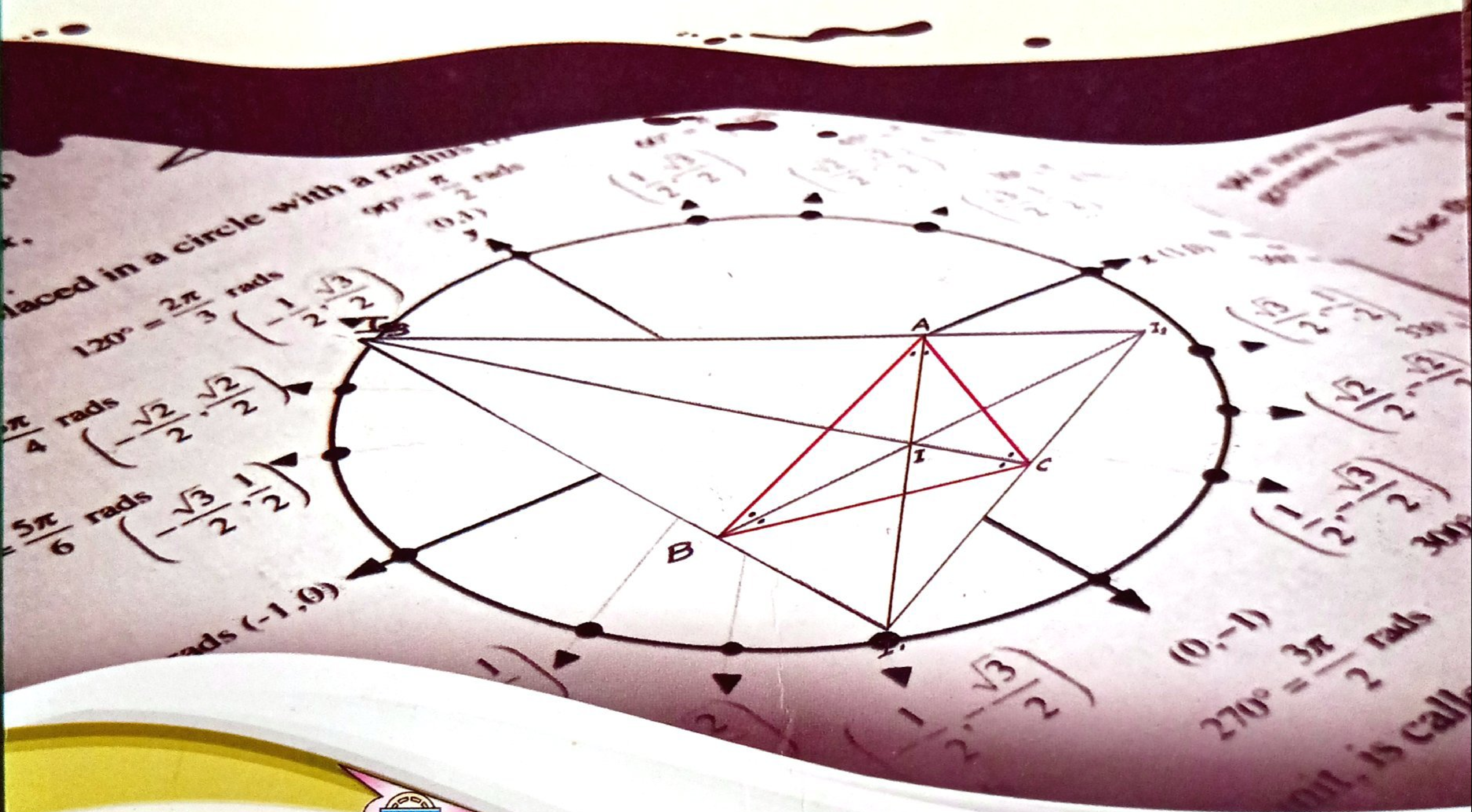


Pundir • Pundir



THEORY OF NUMBERS



A Pragati Edition

CONTENTS

| | |
|--------------------------------------------------------------------------------------------|--------------|
| 1. INTRODUCTION | 1-22 |
| 1.1 Introduction | 1 |
| 1.2 Number System | 1 |
| 1.3 Basic Binary Operations on the Set of Integers | 2 |
| 1.4 Ordering of the Integers | 3 |
| 1.5 Well Ordering Principle | 4 |
| 1.6 Mathematical Induction | 4 |
| 1.7 Basic Representation Theorem | 18 |
| <i>Summary</i> | 22 |
| | |
| 2. DIVISIBILITY THEORY | 23-58 |
| 2.1. Introduction | 23 |
| 2.2. Division Algorithm | 23 |
| 2.3. Greatest Common Divisor | 31 |
| 2.4. Relatively Prime Integers | 37 |
| 2.5. Algorithm to Find G.C.D. :Investigation of the Set of Integers $\{bx + cy\}$ | 40 |
| 2.6. Greatest Common Divisor of More Than Two Integers | 44 |
| 2.7. Least Common Multiple | 45 |
| 2.8. Least Common Multiple of n Integers | 47 |
| 2.9. Fibonacci Sequence | 49 |
| <i>Summary</i> | 58 |
| | |
| 3. LINEAR DIOPHANTINE EQUATIONS | 59-80 |
| 3.1. Introduction | 59 |
| 3.2. Linear Diophantine Equations | 59 |
| 3.3. The Equation $ax + by = c$ | 59 |
| 3.4. Diophantine Equation in Three or More Unknowns | 68 |
| 3.5. Diophantine Equation of the Second Degree | 71 |
| 3.6. General Integer Solution of the Equation $x^2 + y^2 + z^2 = w^2, (x, y, z, w) = 1$ | 73 |
| 3.7. Equation $x^2 + y^2 = z^2$ | 75 |
| <i>Summary</i> | 79 |
| | |
| 4. PRIMES AND THEIR DISTRIBUTIONS | 81-98 |
| 4.1. Introduction | 81 |
| 4.2. Prime Number | 81 |
| 4.3. The Sieve of Eratosthenes | 85 |
| 4.4. Positive Divisors of a Positive Integer | 91 |
| 4.5. The Goldbach Conjecture | 93 |
| <i>Summary</i> | 97 |

5. CONGRUENCES

- 5.1 Introduction 99
- 5.2 Congruence 99
- 5.3 Properties of Congruences 99
- 5.4 Least and Minimal Residue 103
- 5.5 Complete and Reduced Residue Systems 106
- 5.6 Special Divisibility Tests 109
- 5.7 Linear Congruence 111
- 5.8 Chinese Remainder Theorem 113
- 5.9 Congruences of Higher Degree 120
- Summary* 122

6. FERMET'S THEOREM AND ITS APPLICATIONS

23-142

- 6.1 Introduction 123
- 6.2 Fermat's Factorization Method 123
- 6.3 Fermat's Little Theorem 124
- 6.4 Fermat's Last Theorem 128
- 6.5 Wilson's Theorem 131
- 6.6 Euler's Factorization Method 134
- 6.7 Mersenne's Factorization Method 135
- Summary* 142

7. NUMBER THEORETIC FUNCTIONS

143-190

- 7.1 Introduction 143
- 7.2 The Function τ and σ 143
- 7.3 Some Important Theorems 145
- 7.4 Multiplicative Function 152
- 7.5 Mobius Function 154
- 7.6 Euler's Function 162
- 7.7 Some Other Important Number Theoretic Functions 170
- 7.8 Application to Cryptography 181
- 7.9 Data Encryption Standard (DES) 187
- 7.10 Asymmetric Key Cryptography 188
- Summary* 190

8. PRIMITIVE ROOTS AND INDICES

191-214

- 8.1 Introduction 191
- 8.2 General Theorems of Primitive Roots 192
- 8.3 The Necessary and Sufficient Condition for the Existence of Primitive Roots 195
- 8.4 Primitive Roots of Primes 195

- 8.5 Composite Numbers Having Primitive Roots 198
- 8.6 Construction of Reduced Residue System 206
- 8.7 The Theory of Indices 208
- 8.8 Rules of Indices with the Base a modulo p 208
- Summary 214

9. QUADRATIC RESIDUES AND CONGRUENCES OF SECOND DEGREE

215-248

- 9.1 Introduction 215
- 9.2 Quadratic Residues 215
- 9.3 Elementary Properties 216
- 9.4 Legendre Symbols 221
- 9.5 Characterization of Primes that have 2 as Quadratic Residue 226
- 9.6 Quadratic Reciprocity Law 226
- 9.7 Jacobi Symbol 231
- 9.8 Quadratic Congruence with Prime Modulus 237
- 9.9 Quadratic Congruence with Composite Modulus 240
- Summary 248

10. PERFECT NUMBERS

249-264

- 10.1 Introduction 249
- 10.2. Perfect Numbers 249
- 10.3. Necessary and Sufficient Condition for a Positive Integer to be an Even Perfect Number 250
- 10.4 Mersenne Numbers 251
- 10.5 Fermat Number 255
- Summary 263

11. SUM OF SQUARES OF INTEGERS

265-282

- 11.1 Introduction 265
- 11.2 Sum of Two Squares 265
- 11.3 Method for Expression of a prime $p = 4n + 1$ as Sum of Two Squares 272
- 11.4 Difference of Two Squares 274
- 11.5 Sum of More than Two Squares 275
- 11.6 Waring Problem 279
- 11.7 Polygonal Numbers 280
- Summary 282

12. SELECTED TOPICS

283-296

- 12.1 Introduction 283
- 12.2 Types of Number Theories 283

12.3 Some Important Functions 284
12.4 Prime Number Theorem 289
12.5 Dirichlet Theorem 290
12.6 Goldbach's Problem 290
12.7 The Twin Prime Problem 290
12.8 Partition 290
12.9 Graphical Representation of Partitions : Ferrers Graphs 292
12.10 Generating Function 293
 Summary 295

GLOSSARY

297-302

BIBLIOGRAPHY

303

APPENDIX

304-314

INDEX

315-316