

Contents

Introduction	7
1. Basic algebraic properties of integers	9
2. Congruences mod m and basic algebraic properties of the rings \mathbb{Z}_m	16
3. Local method	23
4. Gaussian integers	30
5. Representation of prime numbers as $x^2 + dy^2$	34
6. Legendre symbol and the Quadratic Reciprocity Law	38
7. Applications to cryptography	51
8. Classical problems of number theory	55
9. Prime Number Theorem and its proof	64
10. Integral elements. Trace and norm	70
11. The rings of integers in finite extensions of \mathbb{Q}	76
12. Decomposition of ideals in Dedekind domains	82
13. The rings of integers in quadratic and cyclotomic extensions of \mathbb{Q}	88
14. Splittings of ideals. A new look at QRL	100
15. Hints and solutions to selected problems	108
Bibliography	119
Index	120