Contents

1 Introduction **1**

1.1 A Big Topic in Number Theory 1

1.2 Contents Structure 2

1.3 Learning Guidance 2

1.4 Conventions 3

2 Modular Arithmetic Basics **5**

2.1 Basic Concepts 5

2.1.1 Remainder v.s. Residue 5

2.1.2 Residue, Modulo and Notation 6

2.1.3 Residue Class and Residue System 8

2.2 Basic Operations 9

2.2.1 Addition and Subtraction 10

2.2.2 Multiplication and Exponentiation 10

2.2.3 Division 12

2.3 Examples 13

2.4 Practice 14

3 Evaluate Modular Expression **19**

3.1 Power of Negative One 19

3.2 Continuous Simplification 21

3.3 Binomial Expansion 22

3.4 Euler's Totient Function 23

3.5 Positive One via Euler's Theorem 26

3.6 Modular Inverse 28

3.7 Factorial by Wilson's Theorem 30

3.8 Practice 31

4 Typical Problems and Techniques **33**

4.1 Ending Digits 33

4.2 "Divide by Nine" Technique 36

4.3 Sum of Digits 37

4.4 Missing Digit 38

4.5 Square Numbers 39

4.6 System of MOD Equations (Simple) 41
4.7 Pigeonhole Principle 41
4.8 Indeterminate Equation 43
4.9 Practice 45

5 Important Theorems 49
5.1 Euler's Theorem 49
5.2 Fermat's Little Theorem 53
5.3 Multiplicative Order 54
5.4 Practice 56

6 Modular Equation 61
6.1 Modular Equation Fundamentals 61
6.2 Solving Modular Equation 64
6.3 Solving Equation $ax \equiv b \pmod{m}$ 66
6.4 Solving System of Equations 69
6.5 Chinese Remainder Theorem Again 72
6.6 Practice 73

Appendices 77

A Solutions 79
A.1 Introduction 79
A.2 Modular Arithmetic Basics 80
A.3 Evaluate Modular Expression 86
A.4 Typical Problems and Techniques 93
A.5 Important Theorems 104
A.6 Modular Equation 114