1.2 Contents Structure

Contents in this book are organized in such a way that naturally fits the typical learning curve.

Chapter 2 Modular Arithmetic Basics introduces the basic concepts and operations which are the fundamentals. One must thoroughly understand these before being able to apply modular arithmetic.

Chapter 3 Evaluate Modular Expression focuses on various computation techniques. Just like learning regular arithmetic, being proficient in carrying out actual computation is a necessary prerequisite for problem solving.

Chapter 4 Typical Problems and Techniques explores frequently seen problems and well-known techniques. Familiarity with these can help students avoid re-inventing wheels during tests and thus improve performance in a meaningful way.

Chapter 5 Important Theorems begins exploring more advanced topics. Among others, Euler's theorem and multiplicative orders are two powerful tools for solving many challenging number theory problems.

Chapter 6 Modular Equation discusses modular equations. While solving high degree modular equations is beyond the scope of high school competition, simpler ones and special cases are not uncommon in intermediate and advanced level competitions.

1.3 Learning Guidance

For beginners, the focus should be set as getting familiar with the concept of residues and becoming comfortable with modular operations. Upon having achieved these, one should be proficient

in solving problems such as finding the ending digits and so on.

Intermediate level students should aim to master various well-known techniques such as the divide-by-nine method and φ function. They are frequently used to solve related AMC10/12 and AIME problems.

Advanced level students should target to become skillful in applying modular arithmetic to solve a wide range of problems, such as indeterminate equations. Such problems can be very hard, if not entirely impossible, to tackle without employing modular arithmetic.

1.4 Conventions

The following conventions are used in this book, unless specifically described otherwise.

- An alphabet letter, e.g. n, m, k, etc, represents an integer.
- $gcd(n, m)$ or, simply, (n, m) means the greatest common divisor of integers n and m.
- $a \mid b$ means a divides b, or equivalent b is a multiple of a.