MC40N
AIME Basic Number Theory

Chapter 1: Number Bases

- Non-decimal bases
- Legendre's formula

Sample Problem:
(Folklore) What is the 200^{th} smallest positive integer that can be written as the sum of distinct powers of 3?

Chapter 2: Primes & Prime Factorization

- Definitions of primes and Euclid's Lemma
- Fundamental Theorem of Arithmetic

Sample Problem:
(AIME-2006-I-4) Let N be the number of consecutive 0's at the right end of the decimal representation of the product $1!2!3!4!\ldots 99!100!$. Find the remainder when N is divided by 1000.

Chapter 3: Divisibility Rules

- Divisibility rules
- p-adic valuation

- Lifting the exponent

Sample Problem:
(Brian Shimanuki) Construct the smallest positive integer divisible by 18 using only the digits 3 and 4.

Chapter 4: Multiplicative Functions

- Problems involving multiplicative functions, such as Divisor function, Sigma function, Totient function
- Properties of φ function

Sample Problem:
(BMT-2012-Tournament-Round7-P3) Let φ be the Euler totient function, and let $S = \{x \mid \frac{x}{\varphi(x)} = 3\}$. What is $\sum_{x \in S} \frac{1}{x}$?

Chapter 5: Factoring Techniques

- Difference of squares and arbitrary powers, sum of cubes and odd powers
- Simon's Favorite Factoring Trick
- Sophie Germain identity

Sample Problem:
(HMMT Nov-2008-Guts-31) Find the sum of all primes p for which there exists a prime q such that $p^2 + pq + q^2$ is a square.

Chapter 6: GCD & LCM

- Greatest common divisor, least common multiple
- Euclidean algorithm and its applications
- Bezout's identity

Sample Problem:
(Hong Kong MC-2006-18) For any positive integer n, let $f(n) = 70 + n^2$ and $g(n)$ be the H.C.F. of $f(n)$ and $f(n+1)$. Find the greatest possible value of $g(n)$.

Chapter 7: Modular Arithmetic

- Properties of modulo
- Modular inverses
- Using binomial theorem to find remainders
- Solving AIME level problems using modular arithmetic

Sample Problem:
(AMC12-2014-B23) The number 2017 is prime. Let $S = \sum_{k=0}^{62} \binom{2014}{k}$. What is the remainder when S is divided by 2017?

(A) 32 **(B)** 684 **(C)** 1024 **(D)** 1576 **(E)** 2016

Chapter 8: Fermat's Little Theorem & Euler Theorem

- Fermat's little theorem
- Euler's totient theorem
- Wilson's theorem

Sample Problem:
(ARML-2002-Individual-6) Let a be the integer such that $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{22}+\frac{1}{23} = \frac{a}{23!}$. Compute the remainder when a is divided by 13.

Chapter 9: Chinese Remainder Theorem

- Chinese remainder theorem (CRT)
- Computing solutions to CRT, using CRT backwards

Sample Problem:
(PUMaC-2008-Number Theory-5) If $f(x) = x^{x^{x^x}}$, find the last two digits of $f(17) + f(18) + f(19) + f(20)$.

Chapter 10: Degree

- Definition and properties of order modulo m

Sample Problem:
(CHMMC-2014-Individual-7) A robot is shuffling a 9 card deck. Being very well machined, it does every shuffle in exactly the same way: it splits the deck into two piles, one containing the 5 cards from the bottom of the deck and the other with the 4 cards from the top. It then interleaves the cards from the two piles, starting with a card from the bottom of the larger pile at the bottom of the new deck, and then alternating cards from the two piles while maintaining the relative order of each pile. The top card of the new deck will be the top card of the bottom pile.
The robot repeats this shuffling procedure a total of n times, and notices that the cards are in the same order as they were when it started shuffling. What is the smallest possible value of n?

Chapter 11: Primitive Roots

- Definition of primitive roots
- Primitive root theorem
- Finding number of equations of modular equations using primitive roots

Sample Problem:
(Kevin Li) How many primitive roots does 1458 have?

Chapter 12: Diophantine Equations

- General strategies for solving AIME level diophantine equations
- Chicken McNugget Theorem
- Computing Pythagorean triples
- Fermat's Last Theorem (optional)

Sample Problem:
(PUMaC-2014-Number Theory-5) Find the number of pairs of integer solutions (x, y) that satisfies the equation

$$(x-y+2)(x-y-2)=-(x-2)(y-2).$$