Intermediate Number Theory

Brandon Kong

18 December 2025

Introduction

This lecture is intended for students preparing for AMC 10/12 and AIME. We focus on understanding **number theory deeply**, including the following topics:

- Modular arithmetic and congruences
- Prime numbers and factorization
- Euler's totient function and Euler's theorem
- Fermat's little theorem
- Wilson's theorem
- Factorials and prime powers
- Exponent patterns and cycles
- Multi-step challenge problems

Each topic contains **step-by-step worked examples**, **practice problems with hints**, and **detailed explanations**.

—

1 1. Modular Arithmetic

Definition and Properties

For integers a, b, m with $m > 0$, we say:

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

This means that a and b leave the same remainder when divided by m.

Properties:

1. $(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$
2. $(a \cdot b) \mod m = ((a \mod m) \cdot (b \mod m)) \mod m$
3. $(a^k) \mod m = ((a \mod m)^k) \mod m$

Example 1: Simple Congruence

Solve $3x \equiv 4 \mod 7$.

Step by Step: 1. List multiples of 3 modulo 7: $3 \cdot 0 \equiv 0$, $3 \cdot 1 \equiv 3$, $3 \cdot 2 \equiv 6$, $3 \cdot 3 \equiv 2$, $3 \cdot 4 \equiv 5$, $3 \cdot 5 \equiv 1$, $3 \cdot 6 \equiv 4$ 2. Match remainder 4: occurs at $x = 6$

Answer: $x \equiv 6 \mod 7$

Example 2: Powers Modulo

Find the remainder of 7^{100} divided by 13.

Step by Step: 1. Compute small powers modulo 13: $7^1 \equiv 7$, $7^2 \equiv 10$, $7^3 \equiv 5$, $7^4 \equiv 9$, $7^5 \equiv 11$, $7^6 \equiv 12$, $7^7 \equiv 6$, $7^8 \equiv 3$, $7^9 \equiv 8$, $7^{10} \equiv 4$, $7^{11} \equiv 2$, $7^{12} \equiv 1$ 2. Observe cycle repeats every 12 powers. 3. $100 \mod 12 = 4$, so $7^{100} \equiv 7^4 \equiv 9$

Answer: 9

Practice Problems

1. Solve $5x \equiv 3 \mod 11$ *Hint: Try multiples of 5 modulo 11*
2. Find last digit of 5^{2025} *Hint: Consider the cycle of last digits for 5*
3. Compute $13^{100} \mod 9$ *Hint: Use digit sum trick for modulo 9*

—

2 2. Prime Numbers and Factorization

Definition and Fundamental Theorem of Arithmetic

- Prime numbers: integers greater than 1 divisible only by 1 and itself. - Composite numbers: integers greater than 1 that are not prime. - **Fundamental Theorem of Arithmetic:** Every integer greater than 1 can be uniquely factored as a product of primes.

Example 1: Factorization

Factor 360 step by step:

1. Divide by 2: $360/2 = 180 \implies 2$ is a factor 2. Divide by 2: $180/2 = 90 \implies 2^2$ 3. Divide by 2: $90/2 = 45 \implies 2^3$ 4. Divide by 3: $45/3 = 15 \implies 3$ 5. Divide by 3: $15/3 = 5 \implies 3^2$ 6. Remaining number 5 is prime

Prime factorization: $360 = 2^3 \cdot 3^2 \cdot 5$

Divisors

- Number of divisors formula: $d(n) = (a_1 + 1)(a_2 + 1) \dots (a_k + 1)$ - For $360 = 2^3 \cdot 3^2 \cdot 5^1$: $d(360) = (3 + 1)(2 + 1)(1 + 1) = 24$

Practice Problems

1. Factor 252 and 198, find number of divisors
2. Find sum of exponents in $(2^3 \cdot 3^2 \cdot 5)^2$

—

3 3. Euler's Totient Function and Euler's Theorem

Definitions

- $\phi(n)$ counts integers $1 \leq k \leq n$ coprime to n. - If $n = p_1^{a_1} \dots p_k^{a_k}$ then:

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Euler's Theorem

If $\gcd(a, n) = 1$, then:

$$a^{\phi(n)} \equiv 1 \mod n$$

Example 1: Step by Step

Find $3^{40} \mod 100$

1. Factor $100 = 2^2 \cdot 5^2$ 2. Compute $\phi(100) = 100 \cdot (1 - 1/2) \cdot (1 - 1/5) = 40$ 3. Check $\gcd(3, 100) = 1 \rightarrow$ Euler's theorem applies 4. Thus $3^{40} \equiv 1 \mod 100$

Practice Problems

1. Compute $\phi(360)$
2. Find $7^{100} \mod 40$

—

4 4. Fermat's Little Theorem

- Special case of Euler's theorem: if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$

Example: Step by Step

Find remainder of $7^{100} \mod 13$

1. $p = 13$, $7^{12} \equiv 1 \mod 13$ 2. $100 = 12 \cdot 8 + 4 \rightarrow 7^{100} = (7^{12})^8 \cdot 7^4 \equiv 1^8 \cdot 7^4 \equiv 7^4$ 3. $7^2 = 10$, $7^4 = (7^2)^2 = 10^2 = 100 \equiv 9 \mod 13$

Answer: 9

Practice Problems

1. Compute $5^{100} \mod 13$
2. Find last digit of 9^{123}

—

5 5. Wilson's Theorem

- Prime $p > 1$ iff $(p-1)! \equiv -1 \mod p$

Example: Step by Step

Check if $p = 7$ is prime:

1. $(7-1)! = 6! = 720$ 2. $720 \mod 7 = 720 - 7 \cdot 102 = 720 - 714 = 6$ 3. $6 \equiv -1 \mod 7 \rightarrow$ confirms 7 is prime

Practice Problems

1. Verify Wilson's theorem for $p = 11$

—

6 6. Factorials and Prime Powers

Definition

- $n! = 1 \cdot 2 \cdot \cdots \cdot n$ - Highest power of prime p in $n!$:

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Example: Step by Step

Highest power of 2 in 100!:

1. Compute $\lfloor 100/2 \rfloor = 50$, $\lfloor 100/4 \rfloor = 25$, $\lfloor 100/8 \rfloor = 12$, $\lfloor 100/16 \rfloor = 6$, $\lfloor 100/32 \rfloor = 3$, $\lfloor 100/64 \rfloor = 1$ 2. Sum: $50 + 25 + 12 + 6 + 3 + 1 = 97$ 3. So 2^{97} divides 100! exactly

Practice Problems

1. Highest power of 3 dividing 50!
2. Highest power of 5 dividing 100!

—

7 7. Exponent Patterns and Cycles

Concepts

- Units digits of powers repeat in cycles - Find cycle length and reduce exponent modulo cycle length

Example

Find units digit of 7^{2025}:

1. Cycle of 7: $7, 9, 3, 1$ (length 4) 2. $2025 \mod 4 = 1$ 3. Units digit = 7

Practice Problems

1. Last digit of 3^{1234}
2. Last two digits of 13^{100}

—

8 8. Multi-Step Challenge Problems

1. Solve $2^a \cdot 3^b \cdot 5^c = 180$ **Solution:** Factor $180 = 2^2 \cdot 3^2 \cdot 5 \implies (a, b, c) = (2, 2, 1)$
2. Compute remainder of 123456^{789} divided by 10 **Solution:** Units digit of 6 always $\rightarrow$ remainder 6
3. Find all n such that $n^2 + n + 1$ divisible by 7, sum all $n < 50$ **Solution:** Solve $n^2 + n + 1 \equiv 0 \mod 7 \implies n \equiv 2, 4 \mod 7$ List all $n < 50$: 2,4,9,11,... sum = 196