Modular Arithmetic and Its Applications

Based on Sections 4.1 to 4.6

Divisibility

- Definition: $b \mid a \Leftrightarrow \exists\, k \in \mathbb{Z}$ such that $a = bk$
- Properties:
- • If $a \mid b$ and $b \mid c$, then $a \mid c$
- • If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- Example: $15 = 5 \times 3 \Rightarrow 5 \mid 15$

Division Algorithm

- For integers a and b ($b > 0$): $a = bq + r$ where $0 \leq r < b$
- Example: $17 \div 5 = 3$ remainder 2
- $\Rightarrow 17 = 5 \times 3 + 2$

Modular Arithmetic

- $a \equiv b \pmod{m} \Leftrightarrow$ a and b leave same remainder mod m
- Example: $17 \equiv 2 \pmod{5}$
- Properties:
- • $(a + c) \equiv (b + d) \bmod m$
- • $(a - c) \equiv (b - d) \bmod m$
- • $(a \times c) \equiv (b \times d) \bmod m$

Binary Representation

- Any positive integer = sum of powers of 2
- Convert by repeated division by 2
- Example: 13 → 1101

Euclidean Algorithm

- Used to find GCD of two numbers
- Steps:
- • Divide larger number by smaller
- • Replace larger with smaller, smaller with remainder
- • Repeat until remainder is 0
- Example: GCD(48, 18) = 6

Prime Numbers

- Prime: Only divisible by 1 and itself
- Composite: More than two divisors
- Examples:
- • Prime: 2, 3, 5, 7, 11
- • Composite: 4, 6, 8, 9

Fundamental Theorem of Arithmetic

- Every integer >1 is either a prime or product of primes
- Example: $60 = 2^2 \times 3 \times 5$

GCD and LCM

- GCD: Largest number dividing both integers
- LCM: Smallest number divisible by both
- Relationship: GCD(a, b) × LCM(a, b) = a × b

Solving Linear Congruences

- Equation: $ax \equiv b \pmod{m}$
- Solution exists if $\gcd(a, m)$ divides b
- Example: $3x \equiv 6 \pmod{9} \rightarrow x \equiv 2 \pmod{3}$

Chinese Remainder Theorem

- If moduli are pairwise coprime, system has unique solution mod product
- Example:
- • $x \equiv 2 \pmod{3}$
- • $x \equiv 3 \pmod{5}$
- • $x \equiv 2 \pmod{7}$
- $\Rightarrow x \equiv 23 \pmod{105}$

Applications of Congruences

- Check Digits: Used in ISBN, credit cards
- • ISBN-10: $(1 \times d_1 + \dots + 10 \times d_{10}) \equiv 0 \pmod{11}$
- Hash Functions: sum of ASCII values mod table size
- Pseudorandom Number Generators:
- • Linear congruential: $x_{⍰+1} = (ax_{⍰} + c) \bmod m$

Classical Cryptography

- Caesar Cipher: Shift letters by fixed number
- Example: HELLO → KHOOR
- Affine Cipher: $E(x) = (ax + b) \bmod 26$

RSA Algorithm

- Choose primes p and q, compute $n = pq$, $\phi(n) = (p - 1)(q - 1)$
- Choose e: $\gcd(e, \phi(n)) = 1$, find d: $ed \equiv 1 \bmod \phi(n)$
- Public key: (e, n), Private key: (d, n)
- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$
- Example: $p = 3$, $q = 11$ → $M = 4$ → $C = 31$ → $M = 4$