Computational Number Theory I

Math Fundamentals: Group Theory, Algorithmic Number Theory, Abstract Algebra

Why study this?

- This is a crypto (i.e., security) course right? What relevance does pure mathematics have?

- Old math, new uses

- Cryptography relies heavily on pure math:
  - Number theory (Prime number theory)
  - Abstract algebra (Groups, Rings, Fields, Monoids,…)

- So, we take a review of (undergrad?) math, but from an algorithmic perspective

Divisibility

- n|a; n ≠ 0 read as "n divides a"
  - 3|9, 4|16, -5|20, 17|0, …

- Division theorem (a.k.a. Division algorithm)

For any integers $n > 0$, $a \geq 0$, there exist unique integers $q > 0$, $r > 0$ such that

$$a = qn + r, \text{ and}$$

$$0 \leq r < n, \text{ where } q = \lfloor a/n \rfloor$$

q = quotient, r = remainder, a = dividend, n = divisor

Given a, b, we can compute q, r in polynomial time

Primes

- Prime: any positive integer, $p > 1$, with no factors (divisors) other than those in set $\{1,p\}$
- Composite number: any positive integer, $n > 1$, that is not prime
- 1: neither prime nor composite

- Fundamental theorem of arithmetic:

$$N = \prod_i p_i^{e_i}$$

For all $N > 1$, p_i are distinct primes, and $e_i > 1$ for all i

GCD

- $c = \gcd(a,n)$ is the largest integer that divides both a and n; $a,n > 0$
- $\gcd(a,n) = \max[c$, such that $c|a$ and $c|n]$
- E.g., $\gcd(10,15) = 5$, $\gcd(20,30) = 10$
- $\gcd(a,0) = |a|$ (absolute value)
- $\gcd(0,0)$: undefined

- **Co-prime** or **relatively prime** integers:

If a,n such that $a \neq 0$ and $n \neq 0$, and $\gcd(a,n) = 1$, then a, n are co-prime or relatively prime

Modular Arithmetic

- If $n > 0$ and $a \geq 0$, and $a = qn + r$, where $0 \leq r < n$, then

$$a \bmod n = r$$

- n = modulus, r = remainder
- E.g., $5 \bmod 3 = 2$, $16 \bmod 3 = 1$

- Let $a \geq 0$, $b \geq 0$, $n > 0$ be integers. Then:

If ($a \bmod n$) = ($b \bmod n$), a and b are said to be ***congruent modulo n.***

$a \equiv b \pmod{n}$ iff $(a \bmod n) = (b \bmod n)$

Modular Arithmetic Congruence

- E.g., $17 \equiv 5 \pmod{3}$
- Why? Because 17/3 --> r = 2 and 5/3 --> r = 2

- $24 \equiv 9 \pmod{5}$

- Note we used 17/3 and not $3|17$
- Why? Because $r \neq 0$

Modular Arithmetic Properties

1. If $a \equiv 0 \pmod{n}$, then $n|a$, i.e., for a/n, $r = 0$
   - Check: $6 = 0 \pmod{3}$, $6/3 = 0$

2. $a \equiv b \pmod{n}$ iff $n|(a - b)$
   - Check: $17 \equiv 5 \pmod{3}$, and $3|12$

3. $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$ (Symmetric)
   - Check: $17 \equiv 5 \pmod{3}$, and $5 \equiv 17 \pmod{3}$

Modular Arithmetic Properties

4. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ (Transitivity)
    - Check: $17 \equiv 5 \pmod{3}$ and $5 \equiv 14 \pmod{3}$, then $17 \equiv 14 \pmod{3}$

5. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
    - Check: $[(17 \bmod 3) + (11 \bmod 3)] \bmod 3 = 4 \bmod 3 = 1$
    - $(17+11) \bmod 3 = 28 \bmod 3 = 1$

Modular Arithmetic Properties

6. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
   - Check: $[(17 \bmod 3) - (11 \bmod 3)] \bmod 3 = (2-2) \bmod 3 = 0$
   - $(17-11) \bmod 3 = 6 \bmod 3 = 0$

7. $[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$
   - Check: $[(17 \bmod 3) \cdot (11 \bmod 3)] \bmod 3 = 4 \bmod 3 = 1$
   - $(17 \cdot 11) \bmod 3 = 187 \bmod 3 = 1$

Modular Arithmetic Properties

- Congruence modulo division does not respect divison, generally
  - $[(a \bmod n) / (b \bmod n)] \bmod n \neq (a / b) \bmod n$

- Except in groups where multiplicative inverses exist

Modular Arithmetic Tricks

- Find (4*9*9*11*23) mod 5

- One way
  - (36*99*23) mod 5 = 81972 mod 5 = 2

- Better way:
  - (4*9) mod 5 = 1
  - (1*9) mod 5 = 4
  - (4*11) mod 5 = 44 mod 5 = 4
  - (4*23) mod 5 = 92 mod 5 = 2

Modular Arithmetic Tricks

- Let n = 21
- Find 4^{10} mod n

- $4^{10} \bmod 21 = (4^2 \cdot 4^8) \bmod 21 = (16 \cdot 4^8) \bmod 21$
- $\equiv (16 \cdot (4^4 \cdot 4^4) \bmod 21) \bmod 21$
- $\equiv (16 \cdot (256.4^4) \bmod 21) \bmod 21$
- $\equiv (16 \cdot 4 \cdot (4^4) \bmod 21) \bmod 21$
- $\equiv (16 \cdot 4 \cdot 4 \bmod 21) \bmod 21$
- $= 256 \bmod 21$
- $= 4$

GCD Useful Results

- Let $a, b > 0$. There exist integers X, Y, such that:

$$Xa + Yb = \gcd(a,b)$$

- For any $a,b,c > 0$, if $c|ab$ and $\gcd(a,c) = 1$, then $c|b$. If $p > 1$ is a prime, and $p|ab$, then $p|a$ or $p|b$

- For $a,b,N > 0$, if $a|N$, and $b|N$, and $\gcd(a,b) = 1$, then $ab|N$

Set Algebra

- What is a *set*?

- Any attempt to define a set has been very challenging for mathematicians
    - We are referring to an abstract notion of set, not defining specific sets

- We make no attempt to define a set

- We *think* of a set as a *well-defined* collection of some objects

- Collection of all outstanding baseball players – not a set
- Collection of all baseball players who have scored more than 100 home runs – set

Basic Set Notations

- N : set of natural numbers
- N = { 0, 1, 2, 3, …, }

- Z: set of integers
- Z = { -3, -2, -1, 0, 1, 2, 3, … }

- Z^+ : set of positive integers
- Z^+ = {1, 2, 3, …}

- Z^*: set of non-negative integers, {0, 1, 2, 3, …}
- $Z^* = 0 \cup Z^+$

Set Notations Modulo n

- For $n \in Z^*$:

- $Z_n = \{0,1, \ldots, n-1 \}$
  - Set of residues
  - Math: Z/nZ, CS: Z_n; we'll just use Z_n

- $Z_n^* = \{ a \in Z_n \mid \gcd(a,n) = 1\}$
  - Set of integers co-prime with n
  - E.g., n = 15
  - $Z_n = \{0,1, 2, \ldots,14\}$
  - $Z_n^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$