DM Cheatsheet - Number Theory - Shivram Sambhus (Group K, HS25)

1 Introduction: The Integers and Their Secrets

Number theory is the study of the integers ($\mathbb{Z}$). This chapter explores the fundamental properties of divisibility, prime numbers, and modular arithmetic, culminating in powerful applications like modern cryptography.

1.1 TOC

2 Part I: Divisibility and Core Algorithms

The concept of one integer dividing another is the bedrock of number theory. From this simple idea, we can derive powerful algorithms for finding common divisors and solving linear equations.

2.1 Divisibility and Remainders

Core Concepts

- **Divisibility:** For integers a, b, we say $\boldsymbol{a}$ **divides** $\boldsymbol{b}$, written $a \mid b$, if there exists an integer c such that $b = ac$. Here, a is a **divisor** of b, and b is a **multiple** of a.
- **Division Theorem (Euclid):** For any integers a and $d \neq 0$, there exist **unique** integers q (quotient) and r (remainder) such that: $a = qd + r \quad \text{and} \quad 0 \leq r < |d|$ The remainder r is often denoted $a \bmod d$.

2.2 Greatest Common Divisor (GCD)

Definition

The **greatest common divisor** of a and b (not both zero), denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b.

- **Relatively Prime:** Two integers a, b are **relatively prime** (or coprime) if $\gcd(a, b) = 1$.

Euclidean Algorithm

A fast, recursive algorithm to compute the GCD. It's based on the identity: $\gcd(a, b) = \gcd(b, a \bmod b)$

Approach: Calculating GCD with the Euclidean Algorithm To find $\gcd(a, b)$ for $a > b$:

1. Let $(x, y) = (a, b)$.
2. While $y \neq 0$:
   - Calculate the remainder $r = x \bmod y$.
   - Update the pair: $(x, y) = (y, r)$.
3. The GCD is the last non-zero value of y (which will be in the x position).

Example: $\gcd(48, 18)$

- $\gcd(48, 18) = \gcd(18, 48 \bmod 18) = \gcd(18, 12)$
- $\gcd(18, 12) = \gcd(12, 18 \bmod 12) = \gcd(12, 6)$
- $\gcd(12, 6) = \gcd(6, 12 \bmod 6) = \gcd(6, 0)$
- The last non-zero remainder is 6. So, $\gcd(48, 18) = 6$.

2.3 Extended Euclidean Algorithm

Bézout's Identity

For any integers a, b (not both zero), there exist integers u, v such that: $ua + vb = \gcd(a, b)$ The integers u, v are called **Bézout coefficients**. The Extended Euclidean Algorithm finds them.

Approach: Finding Bézout Coefficients This algorithm works by running the Euclidean algorithm forward and then substituting backwards.

1. **Forward Pass:** Find the GCD using the division algorithm, keeping track of each equation.
   - $48 = 2 * 18 + 12$
   - $18 = 1 * 12 + 6$
   - $12 = 2 * 6 + 0$
2. **Backward Pass:** Start from the last non-zero remainder equation and solve for the GCD (which is 6).
   - $6 = 18 - 1 * 12$
3. Substitute the previous remainder (12) upwards.
   - $6 = 18 - 1 * (48 - 2 * 18)$
4. Group terms by a and b.
   - $6 = 18 - 1 * 48 + 2 * 18$
   - $6 = 3 * 18 - 1 * 48$

So, $u = -1$ and $v = 3$.

Application: This is crucial for finding multiplicative inverses in modular arithmetic.

3 Part II: Prime Numbers & Factorization

Prime numbers are the "atoms" of the integers. The Fundamental Theorem of Arithmetic is one of the most important results in all of mathematics.

3.1 Fundamental Theorem of Arithmetic

Core Concepts

- **Prime:** A positive integer $p > 1$ whose only positive divisors are 1 and p.
- **Composite:** An integer greater than 1 that is not prime.
- **Fundamental Theorem:** Every integer $n > 1$ can be written as a product of primes, and this factorization is **unique** up to the order of the factors. $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$

Euclid's Lemma

A key step in proving uniqueness: If a prime p divides a product ab, then p must divide a or p must divide b ($p|ab \rightarrow p|a \lor p|b$).

GCD & LCM via Prime Factorization

If $a = \prod p_i^{a_i}$ and $b = \prod p_i^{b_i}$:

- $\gcd(a, b) = \prod p_i^{\min(a_i, b_i)}$
- $\operatorname{lcm}(a, b) = \prod p_i^{\max(a_i, b_i)}$
- A useful identity: $a * b = \gcd(a, b) * \operatorname{lcm}(a, b)$.

3.2 Primality Testing & Distribution

Trial Division

To check if an integer n is prime, it is sufficient to test for divisibility by all primes up to $\sqrt{n}$.

- **Lemma:** Every composite integer n has a prime divisor $p \leq \sqrt{n}$.
- **Proof Idea:** If $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, otherwise $ab > n$. This divisor either is prime or has a smaller prime factor.

Infinitude of Primes

Theorem (Euclid): There are infinitely many prime numbers.

Proof by Contradiction:

1. Assume there is a finite list of all primes: $p_1, p_2, \ldots, p_n$.
2. Construct the number $N = (p_1 * p_2 * \ldots * p_n) + 1$.
3. N is not divisible by any prime on our "complete" list (it always leaves a remainder of 1).
4. This means N must either be prime itself, or be divisible by a new prime not on our list.
5. This contradicts the assumption that our list was complete.

4 Part III: Modular Arithmetic

Modular arithmetic deals with remainders. Instead of the infinite set of integers, we work with a finite set of "congruence classes," which simplifies many problems.

4.1 Congruence Relations

Definition

Two integers a, b are **congruent modulo m** (where $m \geq 1$) if they have the same remainder when divided by m. $a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a - b)$

- This is an **equivalence relation**: it is reflexive, symmetric, and transitive.
- The equivalence classes are the sets of integers with the same remainder. For modulo m, there are m classes: $[0]_m, [1]_m, \ldots, [m-1]_m$.
- The set of these classes is denoted $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$.

Modular Arithmetic Rules

Congruence is compatible with addition and multiplication. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$:

- $a + c \equiv b + d \pmod{m}$
- $a * c \equiv b * d \pmod{m}$

Intuition: You can reduce intermediate results modulo m at any point in a calculation without changing the final result's remainder.

Example: Compute $7^{100} \bmod 24$. $7^2 = 49 \equiv 1 \pmod{24}$. $7^{100} = (7^2)^{50} \equiv 1^{50} \equiv 1 \pmod{24}$.

4.2 Multiplicative Inverses & Groups

Definition & Existence

The **multiplicative inverse** of an integer a modulo m is an integer x such that: $ax \equiv 1 \pmod{m}$ This inverse is often denoted a^{-1}.

Theorem: A multiplicative inverse of a modulo m exists **if and only if** $\gcd(a, m) = 1$. If it exists, it is unique in $\mathbb{Z}_m$.

Approach: Finding the Inverse Use the Extended Euclidean Algorithm to find u, v such that $ua + vm = \gcd(a, m)$.

1. If $\gcd(a, m) = 1$, then we have: $ua + vm = 1$
2. Taking this equation modulo m: $ua + vm \equiv 1 \pmod{m}$ $ua + 0 \equiv 1 \pmod{m}$ $ua \equiv 1 \pmod{m}$
3. The Bézout coefficient u is the inverse of a. If u is negative, add m to get the equivalent inverse in $\mathbb{Z}_m$.

The Group of Units $\mathbb{Z}_m^\star$

- The set of all integers in $\mathbb{Z}_m$ that are relatively prime to m is denoted $\mathbb{Z}_m^\star$.
- $\mathbb{Z}_m^\star$ forms a **multiplicative group**. This means it's closed under multiplication, has an identity (1), and every element has an inverse within the set.

4.3 Key Theorems

Euler's Totient Function

Euler's totient function, $\varphi(m)$, counts the number of positive integers up to m that are relatively prime to m.

- In other words, $\varphi(m) = |\mathbb{Z}_m^\star|$.
- If p is prime, $\varphi(p) = p - 1$.
- If p, q are distinct primes, $\varphi(pq) = (p - 1)(q - 1)$.
- If $m = p_1^{k_1} ... p_r^{k_r}$, then $\varphi(m) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

Euler's Theorem

If $\gcd(a, m) = 1$, then: $a^{\varphi(m)} \equiv 1 \pmod{m}$

Intuition: This is a deep result from group theory (Lagrange's Theorem) applied to $\mathbb{Z}_m^\star$. It provides a powerful way to reduce large exponents.

Fermat's Little Theorem

A special case of Euler's Theorem. If p is a prime and a is not a multiple of p: $a^{p-1} \equiv 1 \pmod{p}$ An alternative form is $a^p \equiv a \pmod{p}$ for any integer a.

4.4 Chinese Remainder Theorem (CRT)

The Theorem

Let $m_1, m_2, ..., m_r$ be pairwise relatively prime integers. Then for any integers $a_1, ..., a_r$, the system of simultaneous congruences: $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$ ... $x \equiv a_r \pmod{m_r}$ has a **unique solution** for x modulo $M = m_1 * m_2 * ... * m_r$.

Approach: Constructive Solution

1. For each i, calculate $M_i = \frac{M}{m_i}$.
2. For each i, find the modular inverse of M_i modulo m_i. Let's call it N_i. $M_i N_i \equiv 1 \pmod{m_i}$. (Use Extended Euclidean Alg.)
3. The solution x is the sum of these parts: $x = \sum_{i=1}^{r} a_i M_i N_i$
4. The final unique solution is $x \bmod M$.

Intuition: Each term $a_i M_i N_i$ is constructed to be congruent to a_i modulo m_i and congruent to 0 modulo all other m_j (since $m_j \mid M_i$ for $j \neq i$). Summing them up satisfies all congruences simultaneously.

5 Part IV: Cryptographic Applications

Number theory, once considered pure mathematics, is now the foundation of modern digital security.

5.1 Diffie-Hellman Key Exchange

The Problem & The Protocol

How can Alice and Bob agree on a shared secret key over a public channel?

1. **Public Parameters:** Large prime p and a generator g in $\mathbb{Z}_p^\star$.
2. **Alice:** Chooses secret x_A, sends public $y_A = g^{x_A} \bmod p$.
3. **Bob:** Chooses secret x_B, sends public $y_B = g^{x_B} \bmod p$.
4. **Shared Secret:** Alice computes $(y_B)^{x_A}$. Bob computes $(y_A)^{x_B}$. Both get $g^{x_A x_B} \bmod p$.

Security

Based on the **Discrete Logarithm Problem**: given g, p, and y, it is computationally hard to find the exponent x such that $y = g^x \bmod p$.