Elementary Number Theory Cheat Sheet

Comprehensive Summary for Academic Excellence

1. Divisibility and Primes

Definition (Divisibility): Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say a divides b (denoted $a \mid b$) if there exists $c \in \mathbb{Z}$ such that $b = ac$.

Properties:

- If $a \mid b$ and $b \mid c$, then $a \mid c$.
- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.

Division Algorithm: For any integers a and b with $b > 0$, there exist unique integers q and r such that:

$$a = bq + r, \quad 0 \leq r < b$$

Prime Numbers: An integer $p > 1$ is prime if its only positive divisors are 1 and p.

Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be factored uniquely as a product of primes:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

—

2. Greatest Common Divisor

Definition: The greatest common divisor (GCD) of a and b, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b.

Bézout's Identity: For any nonzero integers a and b, there exist integers x and y such that:

$$\gcd(a, b) = ax + by$$

Euclidean Algorithm: To find $\gcd(a, b)$ where $a > b$:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b \\ b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad r_n = 0 \end{aligned}$$

The last non-zero remainder r_{n-1} is $\gcd(a, b)$.

Least Common Multiple (LCM):

$$\operatorname{lcm}(a, b) = \frac{|ab|}{\gcd(a, b)}$$

—

3. Modular Arithmetic

Congruence Modulo n: Let $n \in \mathbb{Z}^+$ $(n > 1)$. We write $a \equiv b \pmod{n}$ if $n \mid (a - b)$.

Properties:

- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

$$a + c \equiv b + d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

Linear Congruences: The equation $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. If solvable, there are d incongruent solutions modulo n.

Modular Inverse: An integer a has an inverse modulo n if and only if $\gcd(a, n) = 1$. The inverse a^{-1} satisfies:

$$aa^{-1} \equiv 1 \pmod{n}$$

—

4. Classical Theorems

Fermat's Little Theorem: If p is a prime and $\gcd(a, p) = 1$, then:

$$a^{p-1} \equiv 1 \pmod{p}$$

— Equivalently, for any integer a:

$$a^p \equiv a \pmod{p}$$

Euler's Totient Function $\phi(n)$: Counts the positive integers up to n that are relatively prime to n.

- If p is prime, $\phi(p) = p - 1$.
- If $n = p_1^{a_1} \cdots p_k^{a_k}$, then:

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

Euler's Theorem: If $\gcd(a, n) = 1$, then:

$$^{\phi(n)} \equiv 1 \pmod{n}$$

—

5. Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers. Then the system of linear congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

Solution Formula: Let $M_i = M/m_i$ and let $y_i = M_i^{-1} \pmod{m_i}$. The solution is:

$$x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod{M}$$