CHEAT SHEETS HERO

Number Theory Cheatsheet

A concise reference for key concepts, theorems, and formulas in Number Theory, covering divisibility, congruences, prime numbers, and classical theorems.

Divisibility and Primes

Basic Divisibility

Divisibility Notation	`a | b` means 'a divides b', i.e., there exists an integer k such that `b = ak`.
Divisor Properties	If `a | b` and `a | c`, then `a | (bx + cy)` for any integers x, y.
Transitivity of Divisibility	If `a | b` and `b | c`, then `a | c`.
Divisibility by a Product	If `a | c`, `b | c` and `gcd(a, b) = 1`, then `ab | c`.
Euclidean Algorithm	Efficiently computes the greatest common divisor (GCD) of two integers.
GCD Definition	`gcd(a, b)` is the largest positive integer that divides both a and b.

Prime Numbers

Prime Number Definition	A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself.
Fundamental Theorem of Arithmetic	Every integer greater than 1 can be uniquely represented as a product of prime numbers, up to the order of the factors.
Prime Factorization	Expressing a number as a product of its prime factors (e.g., `12 = 2^2 * 3`).
Infinitude of Primes	There are infinitely many prime numbers.
Mersenne Primes	Primes of the form `2^p - 1`, where p is also prime.
Twin Primes	Pairs of primes that differ by 2 (e.g., 3 and 5, 5 and 7).

Congruences

Modular Arithmetic

Congruence Notation	`a ≡ b (mod m)` means 'a is congruent to b modulo m', i.e., `m | (a - b)`.
Properties of Congruences	If `a ≡ b (mod m)` and `c ≡ d (mod m)`, then: • `a + c ≡ b + d (mod m)` • `a - c ≡ b - d (mod m)` • `ac ≡ bd (mod m)`
Cancellation	If `ac ≡ bc (mod m)` and `gcd(c, m) = 1`, then `a ≡ b (mod m)`.
Linear Congruences	An equation of the form `ax ≡ b (mod m)`.
Solving Linear Congruences	A solution exists if and only if `gcd(a, m) | b`. If a solution exists, there are `gcd(a, m)` solutions modulo m.
Modular Inverse	If `ax ≡ 1 (mod m)`, then x is the modular inverse of a modulo m. Exists if and only if `gcd(a, m) = 1`.

Important Theorems

Fermat's Little Theorem	If p is prime and `gcd(a, p) = 1`, then `a^(p-1) ≡ 1 (mod p)`.
Euler's Theorem	If `gcd(a, m) = 1`, then `a^φ(m) ≡ 1 (mod m)`, where φ(m) is Euler's totient function.
Euler's Totient Function	φ(m) counts the number of integers between 1 and m that are relatively prime to m.
Calculating Euler's Totient	If `m = p1^k1 * p2^k2 * ... * pn^kn`, then `φ(m) = m * (1 - 1/p1) * (1 - 1/p2) * ... * (1 - 1/pn)`.
Chinese Remainder Theorem (CRT)	Given a system of congruences `x ≡ a1 (mod m1), x ≡ a2 (mod m2), ..., x ≡ an (mod mn)`, where `gcd(mi, mj) = 1` for all `i ≠ j`, there exists a unique solution modulo `M = m1 * m2 * ... * mn`.
Applying CRT	The CRT provides a method to reconstruct a number from its remainders modulo pairwise coprime moduli.

Diophantine Equations

Linear Diophantine Equations

General Form	`ax + by = c`, where a, b, c are integers, and we seek integer solutions for x and y.
Solvability Condition	A solution exists if and only if `gcd(a, b) | c`.
Finding Solutions	Use the Extended Euclidean Algorithm to find integers x0, y0 such that `ax0 + by0 = gcd(a, b)`. If `gcd(a, b) | c`, then `x = x0 * (c / gcd(a, b))` and `y = y0 * (c / gcd(a, b))` is a particular solution.

General Solution	If (x0, y0) is a particular solution, then the general solution is given by:
	`x = x0 + (b / gcd(a, b)) * t`
	`y = y0 - (a / gcd(a, b)) * t`
	where t is any integer.

Example	Solve `3x + 6y = 9`. Since `gcd(3, 6) = 3` and `3 | 9`, a solution exists. From `3x + 6y = 3*3`, we simplify to `x + 2y = 3`. A particular solution is `x=3`, `y=0`. General solution: `x = 3 + 2t`, `y = -t`.

Pythagorean Triples

Definition	A Pythagorean triple consists of three positive integers a, b, and c, such that `a^2 + b^2 = c^2`.
Primitive Pythagorean Triple	A Pythagorean triple (a, b, c) is primitive if `gcd(a, b, c) = 1`.

Generating Pythagorean Triples	If m and n are positive integers with `m > n`, `gcd(m, n) = 1`, and one of m and n is even, then:
	`a = m^2 - n^2`
	`b = 2mn`
	`c = m^2 + n^2`
	forms a primitive Pythagorean triple.

Example	Let `m = 2` and `n = 1`. Then:
	`a = 2^2 - 1^2 = 3`
	`b = 2 * 2 * 1 = 4`
	`c = 2^2 + 1^2 = 5`
	Thus, (3, 4, 5) is a Pythagorean triple.

Arithmetic Functions

Common Arithmetic Functions

Divisor Function (σ(n))	σ(n) is the sum of all positive divisors of n, including 1 and n itself. `σ(n) = ∑_{d|n} d`
Number of Divisors (τ(n) or d(n))	τ(n) is the number of positive divisors of n. `τ(n) = ∑_{d|n} 1`
Euler's Totient Function (φ(n))	φ(n) is the number of integers between 1 and n that are relatively prime to n. `φ(n) = |{k : 1 ≤ k ≤ n, gcd(n, k) = 1}|`
Möbius Function (μ(n))	μ(n) is defined as: • 0 if n has one or more repeated prime factors. • 1 if n = 1. • (-1)^k if n is a product of k distinct primes.
Example: σ(12)	The divisors of 12 are 1, 2, 3, 4, 6, and 12. Thus, `σ(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28`.
Example: τ(12)	The number of divisors of 12 is 6. Thus, `τ(12) = 6`.

Multiplicativity

Definition	An arithmetic function f(n) is multiplicative if `f(mn) = f(m)f(n)` whenever `gcd(m, n) = 1`. It is completely multiplicative if this holds for all m and n.
Examples of Multiplicative Functions	Euler's totient function φ(n), the divisor function σ(n), and the number of divisors function τ(n) are multiplicative.
Möbius function	The Möbius function μ(n) is also multiplicative.
Implications of Multiplicativity	If f(n) is multiplicative and `n = p1^k1 * p2^k2 * ... * pr^kr`, then `f(n) = f(p1^k1) * f(p2^k2) * ... * f(pr^kr)`.