Number Theory Reference Sheet

Definitions

Let $\mathbb{Z}$ be the set of integers: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Let $\mathbb{Z}^+$ be the set of positive integers: $\{1, 2, 3, \ldots\}$.

Let $\mathbb{N}$ be the set of nonnegative integers: $\{0, 1, 2, \ldots\}$.

Definition: $a \mid b$ **("a *divides* b")**

For $a, b \in \mathbb{Z}$:

$$a \mid b \text{ iff } \exists(k \in \mathbb{Z})\ b = ka$$

Definition: $a \equiv b \pmod{n}$ **("a *is congruent to* b *modulo* n)"**

For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$:

$$a \equiv b \ (\text{mod } m) \text{ iff } m \mid (b - a)$$

Definition: prime

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

Definition: composite

An integer $p > 1$ is composite if it has a positive divisor other than 1 and itself.

Definition: gcd **("greatest common divisor")**

gcd(a, b) is the largest integer c such that $c \mid a$ and $c \mid b$.

Definition: "least common multiple"

lcm(a, b) is the smallest positive integer c such that $a \mid c$ and $b \mid c$.

Theorems

Theorem: Division Theorem

If $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, then there exist unique $q, r \in \mathbb{Z}$, where $0 \leq r < d$ such that $a = dq + r$.

We call q "the quotient" and $r = a\%d$ the "remainder".

Theorem: Relation Between Mod and Congruences

Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$
$a \equiv b \pmod{n} \leftrightarrow a\%n = b\%n$.

Theorem: Adding Congruences

Suppose $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$:
$(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \rightarrow a + c \equiv b + d \pmod{n}$.

Theorem: Multiplying Congruences

Suppose $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$
$(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \rightarrow ac \equiv bd \pmod{n}$.

Theorem: Additivity of mod

If $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, then $(a + b)\%n = ((a\%n) + (b\%n))\%n$

Theorem: Multiplicativity of mod

If $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, then $(a \cdot b)\%n = ((a\%n) \cdot (b\%n))\%n$

Theorem: Subtraction of modulus

If $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, then $a\%n = (a - n)\%n$

Theorem: Base b Representation of Integers

Suppose n is a positive integer (in base b) with exactly m digits.

Then, $n = \sum_{i=0}^{m-1} d_i b^i$, where d_i is a constant representing the i-th digit of n.

Theorem: Raising Congruences To A Power

If $a, b \in \mathbb{Z}$, $i \in \mathbb{N}$, and $n \in \mathbb{Z}^+$, then $a \equiv b \pmod{n} \to a^i \equiv b^i \pmod{n}$.

Theorem: GCD Facts

Let $a, b \in \mathbb{Z}^+$

$$\text{gcd}(a, b) = \text{gcd}(b, a\%b)$$

$$\text{gcd}(a, 0) = a$$

Theorem: Bézout's Theorem

If $a, b \in \mathbb{Z}^+$, then there exists integers s, t such that:

$$\text{gcd}(a, b) = sa + tb$$

Theorem: Fundamental Theorem of Arithmetic

If $q \in \mathbb{Z}^+$ then q has a unique prime factorization.