Chapter 2: Divisibility & Primes

2.1 Divisibility

DIVIDES: a divides b, denoted as $a|b$, means $\exists c \in Z$ s.t. $ac = b$. We also say a is *a divisor* of b or b is *divisible* by a

Lemma 2.1.3: Let a, b, c, x, y be integers

i. if $a|b$ and $x|y$, then $ax|by$
ii. if $a|b$ and $b|c$, then $a|c$
iii. if $a|b$ and $b \neq 0$, then $|a| \leq |b|$
iv. if $a|b$ and $a|c$, then $a|(bx + cy)$ (or $a|(b - c)$)

PRIME: for any $p \in \mathbb{N}$ where $p > 1$, p is *prime* if its only positive divisors are 1 and p. Otherwise, p is *composite*

WELL ORDERING PRINCIPLE: every non-empty set of positive (or nonnegative) integers contains a smallest element

DIVISION THEOREM: Given integers $a > 0$ and $b > 0$, there exists a unique q, r such that $a = bq + r$ with $0 \leq r < b$. Here, r is the remainder, q is the quotient

FLOOR: For $x \in \mathbb{R}$, the *floor* of x, $\lfloor x \rfloor$, is the *largest* $z \in \mathbb{Z}$ s.t. $z \leq x$
CEILING: For $x \in \mathbb{R}$, the *ceiling* of x, $\lceil x \rceil$, is the *smallest* $z \in \mathbb{Z}$ s.t. $z \geq x$

Lemma 2.1.11: Let $n, d \in \mathbb{N}$. The number of positive multiples of d that are less than or eqal to n is $\lfloor \frac{n}{d} \rfloor$

Lemma 2..1.13: if $x, y \in \mathbb{R}$ and $n \in \mathbb{Z}$, then:

i. $x - 1 < \lfloor x \rfloor \leq x$
ii. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
iii. $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$

2.2 Primes

Proposition 2.2.1: Every positive integer can be decomposed as a product of prime numbers

Theorem 2.2.2: (Euclid) There are infinitely many prime numbers

Proposition 2.2.3: (Primality Test) A number p is prime iff it is not divisible by any prime q, $1 < q \leq \sqrt{p}$

Chapter 3: Modular Arithmetic

CONGRUENT: if $a, b, m \in \mathbb{Z}$, then a is *congruent* to b modulo m, denoted as $a \equiv b \ mod \ m$, if $m|(a - b)$ (i.e., a and b leave the same remainder when you divide by m). Otherwise, $a \not\equiv b \ mod \ m$

Proposition 3.1.3: *congruence modulo m is an equivalence relation*

i. $a \equiv a \ (mod \ m)$
ii. $a \equiv b \ (mod \ m) \ iff \ b \equiv a \ (mod \ m)$
iii. $((a \equiv b \ (mod \ m)) \wedge (b \equiv c \ (mod \ m))) \Rightarrow a \equiv c \ (mod \ m)$

Proposition 3.1.5: Let $a, b, c, d \in \mathbb{Z}$. Then,

i. $a \equiv a \ (mod \ m) \Rightarrow ac \equiv bc \ (mod \ m)$
ii. $a \equiv b \ (mod \ m) \Rightarrow a \pm c \equiv b \pm c \ (mod \ m)$
iii. $(a \equiv b \ (mod \ m) \wedge c \equiv d \ (mod \ m)) \Rightarrow ac \equiv bd \ (mod \ m)$

Proposition 3.1.7:

i. if $a \equiv b\ (mod\ m) \wedge d|m$, then $a \equiv b\ (mod\ d)$
ii. if $ac \equiv bc\ (mod\ m)$, then $a \equiv b\ (mod\ \frac{m}{(c,m)})$
iii. if $ac \equiv bc\ (mod\ m) \wedge (c,m) = 1$, then $a \equiv b\ (mod\ m)$

Proposition 3.1.10: if $(m,n) = 1$, then $a \equiv b\ (mod\ m)$ and $a \equiv b\ (mod\ m)\ iff\ a \equiv b\ (mod\ mn)$

Complete Residue System mod m: is a set S of integers which contains exactly one member of each equivalence class, i.e., exactly one value congruent to each of $\{0, 1, 2, ..., m-1\}$

INVERSE mod m: a number a' is an *inverse* of a mod m if $aa' \equiv a'q \equiv 1\ (mod\ m)$