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. $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$
iv. if n is positive, then $\lfloor \frac{x}{n} \rfloor = \lfloor \frac{\lfloor x \rfloor}{n} \rfloor$

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, $1 < q \leq \sqrt{p}$

$\pi(x)$: The number of primes less than or equal to x

Property 2.2.9: There are arbitrarily large gaps in the sequence of prime numbers (eg: gap of $k - 1$: $k! + 2, k! + 3, ..., k! + k$)

Mersenne Prime: Prime number of the form $2^p - 1$
Twin Primes: A pair of primes which differ by 2. (eg. 11, 13)

2.3 Unique Factorization

The factoring of any positive integer n into primes is unique apart from the order of the primes

Lemma 2.3.1: Let $a = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$. A positive integer b divides a iff $b = p_1^{b_1}p_2^{b_2}...p_k^{b_k}$ where $0 \leq b_i \leq a_i$ for $i = 1, ..., k$

$v(n)$: Let n be a positive integer with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$. $v(n)$ is the number of positive divisors of n (incuding 1 and n). $v(n) = (e_1 + 1) \cdots (e_k + 1)$

Proposition 2.3.2: Let n be a positive integer with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$. The number of positive divisors of n is $v(n) = (e_1 + 1) \cdots (e_k + 1)$

Proposition 2.3.4: Let a, b be integers. If p is prime such that $p|ab$, then $p|a$ or $p|b$

Proposition 2.3.5: The number $\sqrt{2}$ is irrational

Proposition 2.3.8: if $p \leq n$, the exponent of p in the factorization of $n!$ is $\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + ...$

2.4 GCD and LCM

GCD: The *greatest common divisor* of two numbers a, b, not both zero, is the largest integer dividing both a and b, denoted as $gcd(a, b)$ or (a, b)
Remark: every positive integer divides 0; hence $(0, 0)$ is undefined

COPRIME: Two integers a, b are *relatively prime* or *coprime* if $(a, b) = 1$

Lemma 2.5.4: GCD of two numbers satisfies the following:

i. $(a, b) = (-a, b)$
ii. $(a, b) = (a - b, b)$
iii. If $(a, b) = d$, then $(\frac{a}{d}, \frac{b}{d}) = 1$

Theorem 2.5.6: For any two integers a, b there exists m, n such that $ma + nb = (a, b)$

LCM: The *least common multiple* (denoted $[a, b]$) of two integers a, b is the smallest positive integer disvisble by both a and b

Proposition 2.5.10: Suppose $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = p_1^{b_1} \cdots p_k^{b_k}$ with $a_i, b_i \geq 0$. Then:

i. $(a, b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \cdots p_k^{min(a_k,b_k)}$
ii. $[a, b] = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \cdots p_k^{max(a_k,b_k)}$

Corollary 2.5.12: $(a, b)[a, b] = |ab|$
Corollary 2.5.13: If $a|bc$ and $(a, c) = 1$, then $a|b$

Proposition 2.5.15: Given two integers a, b, if $a = bq + r$ and $0 \leq r < b$ then $(a, b) = (b, r)$

Chapter 3: Modular Arithmetic

3.1 Conguences

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. $(a \equiv b \ (mod \ m) \wedge c \equiv d \ (mod \ m)) \Rightarrow ac \equiv bd \ (mod \ m)$
iv. $a \equiv b \ (mod \ m)$ implies $a^k \equiv b^k \ (mod \ m)$ for all positive integers k

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 $\{0, 1, 2, ..., m-1\}$

3.2 Inverses Modulo m and Linear Congruences

INVERSE mod m: a number a' is an *inverse* of a mod m if $aa' \equiv 1 \ (mod \ m)$. We say a is *invertible modulo m*

Proposition 3.2.3: An integer a is invertible modulo m iff $(a, m) = 1$. If a has an inverse then it is unique modulo m

Proposition 3.2.7: The linear congruence $ax = b \ (mod \ m)$ has exactly $d = (a, m)$ solutions if $d \mid b$, and no solutions if $d \nmid b$.
If $d \mid b$ and x_0 is a solution, then the d distinct solutions modulo m are $x_0 + (\frac{m}{d})i \ (mod \ m)$ for $i = 0, 1, ..., d-1$

3.3 Chinese Remainder Theorem

Chinese Remainder Theorem: Let $m_1, m_2, ..., m_r$ be pairwise relatively prime integers. Then the simultaneous congruence

$$x \equiv a_1 \ (mod \ m_1)$$
$$x \equiv a_2 \ (mod \ m_2)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_r \ (mod \ m_r)$$

has a unique solution modulo the product $m_1 m_2 \cdots m_r$

Steps:

1. Check if $m_1, m_2, ..., m_r$ are pairwise prime
2. Compute $M = m_1 m_2 \cdots m_r$
3. Compute $M_i = \frac{M}{m_i}$
4. Solve $M_i x \equiv 1 \ (mod \ m_i)$

5. Compute $x = a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r \ (mod\ M)$

Theorem 3.3.4: Let $m_1, ..., m_r$ be integers; then the system of congruences $x \equiv a_i (mod\ m_i), i = 1, ..., r$ has a solution iff for al $i \neq j, (m_i, m_j) | a_i - a_j$. The solution is unique modulo $[m_1, ..., m_r]$