Chapter 1: The Basics

Definition (1.1 Divisibility). If $a, b \in \mathbb{Z}$ with $a \neq 0$ and there exists a $c \in \mathbb{Z}$ such that $b = ac$, then **a divides b** and we write $\mathbf{a|b}$.

Definition (1.2 Prime/Composite). Let $p \in \mathbb{Z}$. If $p \geq 2$ whose only positive divisors are 1 and itself, then p is a **prime**. If $p > 1$ and p is not prime, then p is **composite**.

Definition (1.10 Positional Notation). For any $a \in \mathbb{N}$ and any integer $b > 1$, we can write a as $\mathbf{a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0}$, where $n \geq 0$ and $0 \leq c_i < b$ for all $o \leq i \leq n$. This is denoted $\mathbf{a_{10} = (c_n c_{n-1} \cdots c_1 c_0)_b}$ and is the **positional notation of a in base b**.

Theorem (1.9 Division Algorithm). For any $b \in \mathbb{N}$ and any $a \in \mathbb{Z}$, $\exists! q, r \in \mathbb{Z}$ such that $\mathbf{a = bq + r}$, where $0 \leq r < b$. (e.g. $2021 = 21 \cdot 96 + 5$)

Chapter 2: Divisibility

Definition (2.1 GCD). If d is the largest common divisor of a and b, where a, b are not both equal to 0, then d is the **greatest common divisor** of a and b, denoted $\mathbf{d = (a, b)}$.

Definition (2.1 LCM). If m is the smallest common multiple of a and b, where a, b are not equal to 0, then m is the **least common multiple** of a and b, denoted $\mathbf{m = [a, b]}$.

Definition (Pythagorean Triples). If the lengths of a Pythagorean triangle are all integers, we say (a, b, c) is a **Pythagorean Triple**. If $\gcd(a, b, c) = 1$, then (a, b, c) is a **Primitive Pythagorean Triple**.

Definition (Greatest Integer Function). If $\alpha \in \mathbb{R}$, then $[\alpha]$ (or $\lfloor \alpha \rfloor$) is the **greatest integer** that is $\leq \alpha$.

Definition (2.5 Exact Order of Division). Let $m, n \in \mathbb{N}$ where $m \geq 2$ and $n \geq 1$. $\mathbf{m^f}$ **exactly divides n** if $m^f | n$ and $m^{f+1} \nmid n$. f is the **exact order of division** of n by m, denoted $\mathbf{m^f \| n}$.

Theorem (2.1). If $a \neq 0$, then $a|0$ and $a|a$.
$1|b \; \forall b$.
If $a|b$, then $a|bc$.
If $a|b$ and $b|c$, then $a|c$.

Theorem (2.2). If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

Corollary (2.3). If $a|b$ and $b|a \; \forall a, b \in \mathbb{Z}$, then $a = b$.

Theorem (2.4). If $a, b \neq 0$ and $d = (a, b)$, then d is the least element in the set of all positive integers of the form $ax + by$.

Theorem (2.5). $d = (a, b)$ if and only if $d > 0$, $d|a$, $d|b$, and for any f such that $f|a$ and $f|b$, we have $f|d$.

Theorem (2.8). If $a|bc$ and $(a, b) = 1$, then $a|c$.

Theorem (2.9). If p is prime and $p|bc$, then $p|b$ or $p|c$.

Theorem (2.12). If $(a, b_i) = 1$ for $1 \leq i \leq n$, then $(a, b_1 b_2 \cdots b_n) = 1$.

Theorem (2.13). If $a|c$, $b|c$ and $(a, b) = 1$, then $ab|c$.

Theorem (2.18). For $a, b \in \mathbb{N}$, $[a, b] = m$ if and only if $m > 0$, $a|m$, $b|m$, and $m|n$ for any n such that $a|n$ and $b|n$.

Theorem (2.19). For $a, b \in \mathbb{N}$, $(a, b)[a, b] = ab$.

Theorem (2.22 FTA). Every integer $a \geq 2$ is either prime or a product of primes, and the product is unique up to different orders of prime divisors of a. $\mathbf{a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}}$, where $p_1 < p_2 < \cdots < p_n$ are prime divisors of n and $e_1 \geq 1, e_2 \geq 1, \cdots, e_n \geq 1$ is the **canonical representation of a**

Theorem (2.24). If $a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ is the canonical representation of a, then $\tau(\mathbf{a}) = \mathbf{(e_1 + 1)(e_2 + 1) \cdots (e_n + 1)}$ and $\sigma(\mathbf{a}) = \mathbf{\frac{p_1^{e_1+1} - 1}{p_1 - 1} \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_n^{e_n+1} - 1}{p_n - 1}}$.

Theorem (2.26). $x, y, z \in \mathbb{N}$ where x is even form a primitive Pythagorean triple if and only if $\exists s, t$ such that $s < t$, $(s, t) = 1$, one of s and t is odd and the other is even, $x = 2st$, $y = t^2 - s^2$, $z = t^2 + s^2$.

Theorem (2.29). If $a > 0$ and p is prime, then $p^e \| a!$, where $e = \lfloor \frac{a}{p} \rfloor + \lfloor \frac{a}{p^2} \rfloor + \cdots + \lfloor \frac{a}{p^r} \rfloor$, and r satisfies $p^r \leq a < p^{r+1}$

Chapter 3: Primes

Definition (Mersenne)**.** Primes of the form $\mathbf{2^n - 1}$ are called **Mersenne primes**.

Definition (Fermat)**.** Primes of the form $\mathbf{2^{2^n} + 1}$ are called **Fermat primes** $\mathcal{F}(n)$

Definition (3.1 Perfect)**.** If $\sigma(\mathbf{a}) = \mathbf{2a}$, then a is a **perfect number**.

Theorem (3.2)**.** If $(a, d) = 1$ where $a > 0, d > 0$, then there are infinitely many primes of the form $ax + d$.

Theorem (3.8)**.** Let $\pi(x)$ be the number of primes $\leq x$. Then $\pi(\mathbf{x}) \approx \frac{\mathbf{x}}{\ln(\mathbf{x})}$.

Theorem (3.11)**.** If $2^n - 1$ is a Mersenne prime, then $a = 2^{n-1}(2^n - 1)$ is perfect. Also, every even perfect number is of the form $2^{n-1}(2^n - 1)$, where $2^n - 1$ is a Mersenne prime.

Chapter 4: Congruence

Definition (4.1 Congruence)**.** If $m > 0$ and $m|(a - b)$, then **a is congruent to b**$(\text{mod}\mathbf{m})$ and $\mathbf{a} \equiv \mathbf{b}(\text{mod}\mathbf{m})$.

Definition (4.2 Least Residue)**.** If $a = mq + r$, where $0 \leq r \leq m - 1$, then $a \equiv r(\text{mod} m)$ and r is the **least residue of** $\mathbf{a}(\text{mod}\mathbf{m})$.

Definition (4.4 LR Systems)**.** The set of integers $\{0, 1, \ldots, m - 1\}$ is a **least residue system** $(\text{mod}\mathbf{m})$. Any set of m integers, no two of which are congruent mod m, is called a **complete modulo system modulo m**

Definition (Pseudoprime)**.** If a composite number passes Fermat's test to base 2, then it's a **pseudoprime** to base 2.

Definition (Strong Pseudoprime)**.** If n passes the base a Miller's test and n is composite, then n is a **strong pseudoprime** to base a.

Theorem (4.3)**.** If $a_i \equiv b_i(\text{mod} m)$, where $i = 1, 2, \ldots, n$, then $\sum_{i=1}^n a_i \equiv \sum_{i=1}^n b_i(\text{mod} m)$ and $\prod_{i=1}^n a_i \equiv \prod_{i=1}^n b_i(\text{mod} m)$

Theorem (4.6)**.** If $ac \equiv bc(\text{mod} m)$, then $a \equiv b(\text{mod} \frac{m}{d})$, where $d = (c, m)$.

Corollary (4.7)**.** If $(c, m) = 1$ and $ac \equiv bc(\text{mod} m)$, then $a \equiv b(\text{mod} m)$.

Theorem (4.8)**.** If $c \neq 0$ and $ac \equiv bc(\text{mod} mc)$, then $a \equiv b(\text{mod} m)$.

Theorem (4.9)**.** If $a \equiv b(\text{mod} m)$, $a \equiv b(\text{mod} n)$, and $(m, n) = 1$, then $a \equiv b(\text{mod} mn)$.

Corollary (4.10)**.** If $a \equiv b(\text{mod} m_i)$, $1 \leq i \leq n$, and $m_1, m_2, \cdots, m_n$ are pairwise relatively prime, then $a \equiv b(\text{mod} m_1 m_2 \cdots m_n)$.

Theorem (4.14)**.** If $n \in \mathbb{Z}_+$, then $\phi(1) = 1$, and for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \geq 2$ the canonical representation of n, we have $\phi(n) = n \prod_{i=1}^r (1 - \frac{1}{p_i})$.

Theorem (Fermat's Lil Thm)**.** If p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1(\text{mod} p)$. This implies that if p is prime, then $a^p \equiv a(\text{mod} p)$.

Theorem (4.17 Euler-Fermat)**.** If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1(\text{mod} m)$, where $\phi(m)$ is the number of integers from 0 to $m - 1$ that are relatively prime to m.

Chapter 5: Congruence Equations

Definition (5.1)**.** For an odd prime p and $c \in \mathbb{Z}$ such that $(c, p) = 1$, if $\mathbf{x}^2 \equiv \mathbf{c}(\text{mod}\mathbf{p})$ is solvable, then c is a **quadratic residue modp**.

Definition (5.2)**.** The **Legendre symbol** is defined as $(\frac{a}{p})$. Its value is 1 if a is a quadratic residue mod$p$, 0 if $p|a$, or -1 if a is a quadratic non-residue mod$p$, where p is an odd prime.

Theorem (5.1)**.** $ax \equiv b(\text{mod} m)$ is solvable if and only if $d|b$, where $d = (a, m)$. In the case that $d|b$, the congruence equation has precisely d incongruent solutions mod m (e.g. $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \cdots, x_0 + (d - 1)\frac{m}{d}$), where x_0 can be found via Euclid's algorithm.

Theorem (5.5 Chinese Remainder Theorem)**.** Suppose m_1, m_2, m_s are pairwise relatively prime and $(a_i, m_i) = 1$ for $1 \le i \le s$. Then the system $a_1 x \equiv b_1 (\text{mod} m_1)$, $a_2 x \equiv b_2 (\text{mod} m_2), \cdots, a_s x \equiv b_s (\text{mod} m_s)$ has a unique solution mod$M$, where $M = \prod_{i=1}^{s} m_i$.

Theorem (5.15 Gauss Quadratic Reciprocity)**.** If p and q are distinct odd primes, then $(\frac{p}{q}) = (\frac{q}{p})$ if $p \equiv 1(\text{mod} 4)$ or $q \equiv 1(\text{mod} 4)$, or $-(\frac{q}{p})$ if $p \equiv q \equiv 3(\text{mod} 4)$.

Theorem (5.16)**.** For an odd prime p, we have $(\frac{2}{p}) = 1$ if $p \equiv 1$ or $7(\text{mod} 8)$, and -1 if $p \equiv 3$ or $5(\text{mod} 8)$.

Chapter 6: Cryptography

Definition (Caesar Cipher)**.** Take $m = 26$ and let $A, B, C, \ldots, Z$ be represented by the 26 least residues.
Key: $(\mathbf{r}, \mathbf{s})$ where r is a multiplier and s is a shift such that $1 \le r \le 25$ and $(r, 26) = 1$, $0 \le s \le 25$, and $(r, s) \ne (1, 0)$.
Encryption: $\mathbf{C} \equiv \mathbf{rP} + \mathbf{s}(\text{mod}\mathbf{26})$**, where** $0 \le C \le 25$.
Decryption: First find r^{-1} such that $rr^{-1} \equiv (\text{mod} 26)$ via Euclid. Then $\mathbf{P} \equiv \mathbf{r}^{-1}(\mathbf{C} - \mathbf{s})(\text{mod}\mathbf{26})$.

Definition (Exponentiation Cipher)**.** First change the plaintext to groups of letters and use numbers to represent them (e.g. $A = 00, B = 01, \ldots, Z = 25$). Choose p such that each group of numbers with $2m$ digits.
Key: $(\mathbf{k}, \mathbf{p} - \mathbf{1}) = \mathbf{1}$.
Encryption: Compute the least residue of $T^k(\text{mod} p)$, which is the ciphertext C.
Decryption: Compute deciphering key q which satisfies $kq \equiv 1(\text{mod} p - 1)$ via Euclid. Then compute the least residue of $C^q(\text{mod} p)$, which is the plaintext T.

Definition (Diffie-Hellman Key Exchange)**.** A method which makes it possible to share a common secret without meeting in person.
First Alice and Bob pick a prime p and $r \in \mathbb{Z}$ such that $(r, p) = 1$ and $(r, p - 1) = 1$.
Then Alice picks a k_1, computes $x_1 \equiv r^{k-1}(\text{mod} p)$, and send it to Bob. Bob also picks a k_2 and computes $x - 2 \equiv r^{k_2}(\text{mod} p)$ and sends it to Alice.
Now Alice computes $k \equiv x_2^{k_1}(\text{mod} p)$ and Bob computes $k \equiv x_1^{k-2}(\text{mod} p)$.

Definition (RSA Cryptosystem)**.** An asymmetric cryptosystem where Alice and Bob have different keys.
Key: Pick 2 large primes p and q, compute $n = pq$ and $\alpha(n) = pq(1 - \frac{1}{p})(1 - \frac{1}{q})$. Pick a number e that is relatively prime to n and $\alpha(n)$. Publish $(\mathbf{n}, \mathbf{e})$, keep $\alpha(n)$ secret.
Encryption: Compute $\mathbf{C} \equiv \mathbf{m}^{\mathbf{e}}(\text{mod}\mathbf{n})$. Send C.
Decryption: Compute d such that $ed \equiv 1(\text{mod}()p - 1)(q - 1)$. The pair (n, d) is the private key. Compute $m \equiv C^d(\text{mod} n)$.