EDIN01: Cryptography - Reference Sheet

Karl Hallsby

Last Edited: November 22, 2019

Contents

1 Cryptography Introduction

Defn 1 (Cryptographic Primitive)**.** A *cryptographic primitive* is an algorithm with basic cryptographic properties. These are solutions to different problems where cryptography is required.

Defn 2 (Cryptographic Protocol)**.** A *cryptographic protocol* involves the back-and-forth communication among two or more parties.

Remark 2.1 (Bob and Alice). Typically, the parties are named Bob and Alice. These are arbitrary names, but these are the most commonly used ones.

There are have been several Cryptographic Protocols.

1. *Symmetric-key cryptography* - Methods in which both the sender and receiver share the same key
   (a) Block ciphers
   (b) Stream ciphers
   (c) MAC algorithms
2. *Public-key cryptography*: 2 different, but mathematically related keys are used. A public key and a private key.
   (a) The public key cannot decrypt something that was encrypted with the private key.
   (b) The public key can be shared freely, because the private key cannot be generated from the public key.
3. *Cryptographic hash functions* are a related and important class of cryptographic algorithms.
   (a) This is a keyless Cryptographic Primitive.
   (b) Takes an arbitrary length input and produces a fixed-length output.
   (c) The mapping between the input and output is such that the output cannot generate the input, therefore making it cryptographic.

1.1 Historical Cryptography

Defn 3 (Cryptology)**.** *Cryptology* was the science of secret writing.

Defn 4 (Cryptography)**.** *Cryptography* dealt with the development of systems for secret writing.

Defn 5 (Cryptanalysis)**.** *Cryptanalysis* was the analysis of existing cryptographic systems to break them.

Just to give a super quick background on how we've gotten to where we are today when it comes to cryptography.

1.1.1 Monoalphabetic Ciphers

Defn 6 (Monoalphabetic Cipher)**.** In a *monoalphabetic cipher* a single letter is replaced by the cipher's mapping. Since the cipher can do this to arbitrary letters, this could continue indefinitely for any single letter.

These were some of the first ciphers developed by Man. These include simple substitute ciphers, and letter shifting ciphers. However, these can be broken with *frequency analysis*.

1.1.2 Polyalphabetic Ciphers

Defn 7 (Polyalphabetic Cipher)**.** In a *polyalphabetic cipher* multiple letters are replaced by the cipher's mapping. Additionally, since the cipher can output multiple letters, the ciphered letters could be run through the cipher again.

These were developed in response to Monoalphabetic Ciphers being broken. However, these can also be broken, with *extended frequency analysis*.

Eventually, it was realized that the secrecy of the cipher is not sensible/possible. This leads us to the conclusion that **any cryptographic scheme should remain secure even if the adversary understands the cipher algorithm itself**.

1.1.3 Cryptographic Keys

The use of keys as ciphers is a slightly more modern occurrence.

Defn 8 (Kerckhoff's Principle)**.** *Kerckhoff's Principle* states that the security of the key used should alone be sufficient for a good cipher to maintain confidentiality under an attack. Essentially, the security of the key used should be sufficient such that the cipher can be maintained confidently while under attack.

However, only since the mid-1970s, has public key cryptography has been possible.
Computers can efficiently encrypt, given the following constraints:

Symmetric-Key Cryptography	Public-Key Cryptography
Block ciphers	Public-Key encryption
Stream ciphers	Digital Signature Schemes
Cryptographic Hash Functions	Key exchange protocols
	Electronic Cash/Cryptocurrency
	Interactive Proof Systems

Table 1.1: Uses of Key-Based Cryptography

1. Some modern techniques can only keep the keys secret if certain mathematical problems are Intractable.
   (a) Integer factorization
   (b) Discrete logarithm problems
2. However, there are no absolute proofs that a cryptographic technique is secure.

Defn 9 (Intractable)**.** An *intractable* problem is one in which there are no **efficient** algorithms to solve them.

2 Number Theory

Before we can start with any of the deeper cryptography stuff, we need to start with some basic number theory.

Defn 10 (Number Theory)**.** *Number theory* is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions. Number theorists study prime numbers as well as the properties of objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers).

Defn 11 (Divides)**.** For $a, b \in \mathbb{Z}$, we say that a *divides* b (written $a \,|\, b$) if there exists an integer c such that $b = ac$.

Properties:

(i) $a \,|\, a$
(ii) If $a \,|\, b$ and $b \,|\, c$, then $a \,|\, c$.
(iii) If $a \,|\, b$ and $a \,|\, c$, then $a \,|(bx + cy)$ for any $x, y \in \mathbb{Z}$.
(iv) If $a \,|\, b$ and $b \,|\, a$, then $a = \pm b$.

2.1 Integer Long Division

For $a, b \in \mathbb{Z}$, with $b \geq 1$. Then an ordinary long division of a by b, i.e. $a \div b$ yields two integers q and r such that

$$a = qb + r, \text{where } 0 \leq r < b \tag{2.1}$$

q and r are called the Quotient and Remainder, respectively, and are **unique**.

Defn 12 (Quotient)**.** The *quotient*, q, of a divided by b is denoted $a \operatorname{div} b$.

Defn 13 (Remainder)**.** The *remainder*, r, of a divided by b is denoted $a \bmod b$.

Example 2.1: Integer Long Division.

If $a = 53$ and $b = 9$, what is $a \bmod b$?

$$53 = q9 + r$$
$$q = 5$$
$$r = 8$$

Thus, $53 \bmod 9 = 8$.

2.2 Greatest Common Divisor

Defn 14 (Common Divisor)**.** An integer c is a *common divisor* of a and b if $c \mid a$ and $c \mid b$.

Defn 15 (Greatest Common Divisor)**.** A non-negative integer d is called the *greatest common divisor* (*GCD*) of integers a and b if:

1. d is a Common Divisor of a and b.
2. For every other common divisor c it holds that $c \mid d$.

The greatest common divisor is denoted

$$\gcd(a, b) \tag{2.2}$$

$\gcd(a, b)$ is the **largest positive** integer dividing both a and b (except for $\gcd(0, 0) = 0$).

Remark 15.1. If $a, b \in \mathbb{Z}^+$, then $\text{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$

Example 2.2: Greatest Common Divisor.

What is the $\gcd(18, 24)$?

Common Divisors $= \{\pm 1, \pm 2, \pm 4, \pm 6\}$.
Since we can only allow positive integers,

$$\gcd(18, 24) = +6$$

2.3 Least Common Multiple

Defn 16 (Least Common Multiple)**.** A non-negative integer d is called the *least common multiple* (*LCM*) of integers a and b if:

1. $a \mid d$ and $b \mid d$
2. For every integer c such that $a \mid c$ and $b \mid c$, we have $d \mid c$.

The least common multiple is denoted

$$\text{lcm}(a, b) \tag{2.3}$$

$\text{lcm}(a, b)$ is the **smallest positive** integer divisible by both a and b.

Remark 16.1. If $a, b \in \mathbb{Z}^+$, then $\text{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$

2.4 Primality

Defn 17 (Relatively Prime)**.** a, b are called *relatively prime* if $\gcd(a, b) = 1$.

Defn 18 (Prime)**.** An integer $p \geq 2$ is called *prime* if its only positive divisors are 1 and p. Otherwise, p is called a *Composite*.

Defn 19 (Composite)**.** An integer $p \geq 2$ is called *composite* if it has more positive divisors than just 1 and p. Otherwise, p is called a *Prime*.

2.4.1 Number of Primes

The number of primes $\leq x$ is denoted

$$\pi(x) \tag{2.4}$$

1. There are infinitely many primes
2. $\lim\limits_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$
3. For $x \geq 17$, $\frac{x}{\ln(x)} < \pi(x) < \frac{1.25506x}{\ln(x)}$

2.5 Unique Factorization

Theorem 2.1 (Unique Factorization Theorem)**.** *Every integer $n \geq 2$ can be written as a product of prime powers,*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1, p_2, \ldots p_k$ are distinct primes and $e_1, e_2, \ldots e_k$ are positive integers. Furthermore, the factorization is unique up to rearrangement of the factors.

2.5.1 Greatest Common Divisor and Least Common Multiple with Unique Factors

If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{e_k}$, where $e_i, f_i, i = 1, 2, \ldots k$ are non-negative integers, then

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)} \tag{2.5}$$

and

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)} \tag{2.6}$$

2.6 Euler Phi Function

Defn 20 (Euler Phi Function)**.** For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1, n]$, which are Relatively Prime to n. This function is called the *Euler Phi Function.*

$$\phi(n) = \left(p_1^{e_1} - p_1^{e_1 - 1}\right) \left(p_2^{e_2} - p_2^{e_2 - 1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k - 1}\right) \tag{2.7}$$

Remark 20.1. The Euler Phi Function is closely related to Set Order.

Theorem 2.2 (Euler Phi Function)**.** *There are a few properties of the Euler Phi Function that we will treat as true because of this theorem.*

(i) *If p is a Prime, then $\phi(p) = p - 1$.*

(ii) *If $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.*

(iii) *If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then*

$$\phi(n) = \left(p_1^{e_1} - p_1^{e_1 - 1}\right) \left(p_2^{e_2} - p_2^{e_2 - 1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k - 1}\right)$$

Example 2.3: Euler Phi Function. Exercise 1, Question 1.2a

Find the value of $\phi(36)$?

First, we note that 36 is not a Prime number, thus we need to find a set of primes that are equal to 36. The divisors of 36 are

$$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 9, \pm 12, \pm 18, \pm 36\}$$

And all possible prime numbers present as divisors of 36 are

$$\{2, 3\}$$

So, there must be some combination of $2^x \cdot 3^y$ that yields 36. In fact, $2^2 \cdot 3^2 = 4 \cdot 9 = 36$. Since 36 can be broken up as a product of 2 Prime numbers raised to some power, we can use Property **(iii)** of the Euler Phi Function to simplify this. But first, we need to separate the two values from each other using Property **(ii)** of the Euler Phi Function to apply Property **(iii)**.

We need to check $\gcd\left(2^2, 3^2\right) = 1$.

$$\begin{aligned} \gcd\left(2^2, 3^2\right) &= \gcd(4, 9) \\ 9 &= a4 + b \\ &= 2 \cdot 4 + 1 \\ 4 &= a \cdot 1 + b \\ &= 4 \cdot 1 + 0 \end{aligned}$$

So, $\gcd\left(2^2, 3^2\right) = 1$, so we can use Property **(ii)**.

$$\phi\left(2^2 \cdot 3^2\right) = \phi\left(2^2\right) \phi\left(3^2\right)$$

And now we can apply Property **(iii)** to find our answer.

$$\begin{aligned} \phi\left(2^2\right) \phi\left(3^2\right) &= \left(2^2 - 2^{2-1}\right) \left(3^2 - 3^{2-1}\right) \\ &= (4 - 2)(9 - 3) \\ &= (2)(6) \\ &= 12 \end{aligned}$$

Thus, $\phi(36) = 12$.

Lemma 2.2.1 (Computing the Greatest Common Divisor)**.** *If a and b are positive integers where $a > b$, then*

$$\gcd(a, b) = \gcd(b, a \bmod b) \tag{2.8}$$

Remark. This can be repeated to efficiently calculate the $\gcd(a, b)$. This is called the Euclidean Algorithm.

Defn 21 (Euclidean Algorithm)**.** The *euclidean algorithm* is a way to efficiently calculate the $\gcd(a, b)$.

1. Set $r_0 \leftarrow a, r_1 \leftarrow b, i \leftarrow 1$.
2. While $r_i \neq 0$ do:
   (a) Set $r_{i+1} \leftarrow r_{i-1} \bmod r_i, i \leftarrow i + 1$
3. Return r_i

Example 2.4: Euclidean Algorithm. Exercise 1, Question 1.1a

Find the Greatest Common Divisor of 222 and 1870?

$$\begin{aligned}
1870 &= a222 + b \\
&= 8 \cdot 222 + 94 \\
222 &= a94 + b \\
&= 2 \cdot 94 + 34 \\
94 &= a34 + b \\
&= 2 \cdot 34 + 26 \\
34 &= a26 + b \\
&= 1 \cdot 26 + 8 \\
26 &= a8 + b \\
&= 3 \cdot 8 + 2 \\
8 &= a2 + b \\
&= 4 \cdot 2 + 0
\end{aligned}$$

Thus, since $4 \cdot 2 = 8$, 2 is the Greatest Common Divisor of 222 and 1870.

Theorem 2.3. *There exist integers x, y such that* $\gcd(a, b)$ *can be written as*

$$\gcd(a, b) = ax + by \tag{2.9}$$

Proof.

$$\begin{aligned}
\gcd(a, b) &= r_i \\
&= r_{i-2} - q_{i-1} r_{i-1} \\
&= r_{i-2} - q_{i-1}(r_{i-3} - q_{i-2} r_{i-2}) \\
&\vdots \\
&= r_0 x + r_1 y \\
&= ax + by
\end{aligned}$$

for some integers $x, y \in \mathbb{Z}$. ■

This means that the Euclidean Algorithm can be extended to return the values of x and y from Equation (2.9).

Defn 22 (Extended Euclidean Algorithm)**.** The *extended euclidean algorithm* is a way to efficiently calculate the linear pair of integers ($x, y \in \mathbb{Z}$) that satisfy Equation (2.9).

$$\gcd(a, b) = ax + by$$

1. If $b = 0$, then return $a, x \leftarrow 1, y \leftarrow 0$.
2. Set $x_2 \leftarrow 1, x_2 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$

3. While $b > 0$ do:
   (a) $q \leftarrow a \operatorname{div} b, r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$
   (b) $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y$.
4. Set $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$ and return d, x, y.

Example 2.5: Extended Euclidean Algorithm. Exercise 1, Question 1.1b

Find the integers x and y such that $\gcd(222, 1870) = 222x + 1870y$?

From Example 2.4, we know $\gcd(222, 1870) = 2$, so we can plug that in. We now know that

$$2 = 222x + 1870y$$

Now, we essentially run the Euclidean Algorithm backwards.

$$\begin{aligned}
2 &= 26 - 3 \cdot 8 \\
&= 26 - 3(34 - 1 \cdot 26) = 26 - 3 \cdot 34 + 3 \cdot 26 \\
&= 4 \cdot 26 - 3 \cdot 34 \\
&= 4(94 - 2 \cdot 34) - 3 \cdot 34 = 4 \cdot 94 - 8 \cdot 34 - 3 \cdot 34 \\
&= 4 \cdot 94 - 11 \cdot 34 \\
&= 4 \cdot 94 - 11(222 - 2 \cdot 94) = 4 \cdot 94 - 11 \cdot 222 + 22 \cdot 94 \\
&= 26 \cdot 94 - 22 \cdot 222 \\
&= 26(1870 - 8 \cdot 222) - 22 \cdot 222 = 26 \cdot 1870 - 208 \cdot 222 - 11 \cdot 222 \\
&= -219 \cdot 222 + 26 \cdot 1870
\end{aligned}$$

Now we need to check the solution we might have found

$$\begin{aligned}
-219 \cdot 222 + 26 \cdot 1870 &= 2 \\
-48618 + 48620 &= 2 \\
2 &= 2
\end{aligned}$$

Thus,

$$\begin{aligned}
x &= -219 \\
y &= 26
\end{aligned}$$

2.7 The Integers modulo n

Let n be a positive integer.

Defn 23 (Congruence)**.** If a and b are integers, then *a is said to be congruent to b modulo n*, which is written as

$$a \equiv b \pmod{n} \tag{2.10}$$

If n divides $(a - b)$, i.e. $n \,|\, (a - b)$, then we call n the *modulus* of the congruence.

Theorem 2.4. *For $a, a_1, b, b_1, c \in \mathbb{Z}$, we have*
(i) $a \equiv b \pmod{n}$ if and only if *a and b leave the same Remainder when divided by n.*
(ii) $a \equiv a \pmod{n}$
(iii) *If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$*
(iv) *If $a \equiv b \pmod{n}$ adn $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$*
(v) *If $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$, then $a + b = a_1 + b_1 \pmod{n}$ and $ab = a_1 b_1 \pmod{n}$.*
*Properties **(ii)** to **(iv)** are called* reflexivity, symmetry*, and* transitivity*, respectively.*

Example 2.6: Integers modulo n. Exercise 1, Question 1.2b

Write all the units (Invertible Element) in $\mathbb{Z}_{36}$?

First, we start by constructing our set of integers modulo n.

$$\mathbb{Z}_{36} = \big\{[0], [1], [2], [3], [4], \ldots, [35]\big\}$$

Since we are only worried about the units of $\mathbb{Z}_{36}$, we need to find the integers that satisfy Equation (4.3). This is done by finding an a value that has a Multiplicative Inverse, which requires that Equation (3.1) be true, namely

$$\gcd(a, n) = 1$$

This leaves us with

$$\mathbb{Z}_{36} = \big\{[1], [5], [7], [11], [13], [17], [19], [23], [25], [29], [31], [35]\big\}$$

which is the solution.

2.8 Equivalence Classes

Defn 24 (Equivalence Class)**.** Congruence modulo n partitions $\mathbb{Z}$ into n sets, called *equivalence class*es, where each integer belongs to exactly one equivalence class.

For example, these are all congruent to each other modulo n:

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\} \tag{2.11a}$$

$$[1] = \{\ldots - 2n + 1, -n + 1, 1, n + 1, 2n + 1 \ldots\} \tag{2.11b}$$

$$[r] = \mathbb{Z}_r = (x \bmod r) + n\,\mathbb{Z} \tag{2.11c}$$

Since all elements in an equivalent class have the same Remainder, r, we use r as a *represenatative* for the equivalence class.

Remark 24.1. In this case, the representatives of the equivalence classes shown in Equations (2.11a) to (2.11b) are 0 and 1, respectively, and consist of all integers that are mod 0 or mod 1, respectively.

3 Number Theory on Sets

While this section is not technically different than Section 2, it is worth it to split these up, since Section 2 does not deal with sets. However, using what we learned in Section 2, Number Theory, it is natural to extend these to sets of numbers.

3.1 $\mathbb{Z}_n$

Defn 25 ($\mathbb{Z}_n$)**.** The Integers modulo n, denoted $\mathbb{Z}_n$, is the set of (Equivalence Classes of) integers $\{[0], [1], \ldots, [n-1]\}$. Addition, subtraction, and multiplication are all performed with modulo n. Examples 3.1 to 3.3 demonstrate this.

Example 3.1: Addition on Integers mod n.

When dealing with the set of integers $\mathbb{Z}_{15}$, what is the sum of 5 and 9?

$$5 \bmod 15 + 9 \bmod 15 = 11 \bmod 15$$

Thus, the answer is 11.

Example 3.2: Subtraction on Integers mod n.

When dealing with the set of integers $\mathbb{Z}_{15}$, what is 5 minus 9?

$$\begin{aligned}5 \bmod 15 - 9 \bmod 15 &= 5 \bmod 15 + (-9 \bmod 15)\\ &= 5 \bmod 15 + \underbrace{-9 \bmod 15}_{-9+15=6}\\ &= 5 \bmod 15 + 6 \bmod 15\\ &= 11 \bmod 15\end{aligned}$$

Thus, the answer is, again, 11.

Example 3.3: Multiplication on Integers mod n.

When dealing with the set of integers $\mathbb{Z}_{15}$, what is the product of 5 and 9?

$$\begin{aligned}5 \bmod 15 \cdot 9 \bmod 15 &= 45 \bmod 15\\ &= 0\end{aligned}$$

Thus, the answer is 0, because $45 = 3 \cdot 15$.

3.2 Inverse in $\mathbb{Z}_n$

Addition, subtraction, and multiplication can be performed trivially in $\mathbb{Z}_n$, as shown in Examples 3.1 to 3.3. However, the concept of division is a little bit more difficult.

Defn 26 (Multiplicative Inverse)**.** Let $a \in \mathbb{Z}_n$. The *multiplicative inverse* of a is an integer $x \in \mathbb{Z}_n$, such that $ax = 1$. If such an integer, x, exists, then a is said to be *invertible* and x is called the inverse of a, denoted as a^{-1}.

Defn 27 (Division in $\mathbb{Z}_n$)**.** *Division* of a by an element $b \in \mathbb{Z}_n$ (written a/b) is defined as ab^{-1}, and is only defined if b has a Multiplicative Inverse.

Defn 28 (Invertible)**.** Let $a \in \mathbb{Z}_n$. Then a is *invertible* if and only iff

$$\gcd(a, n) = 1 \tag{3.1}$$

Proof. Assume that $\gcd(a, n) = 1$. We know that $1 = \gcd(a, n) = xa + yn$ for some $x, y \in \mathbb{Z}$. Since yn is a multiple of n, namely $yn \bmod n = 0$, it is removed from the equation. Then $x \bmod n$ is an inverse to a.

Now assume $\gcd(a, n) > 1$. If a has an inverse x, then $ax = 1 \bmod n$, which means $1 = ax + ny$ for some $x, y \in \mathbb{Z}$, directly contradicting the assumption that $\gcd(a, n) = 1$. ■

The two possible cases of division, i.e. possible and impossible, are shown in Examples 3.4 to 3.5.

Example 3.4: Possible Division on Integers mod n.

When dealing with the set of integers $\mathbb{Z}_{15}$, what is the result from the division of 5 by 11?

$$5 \bmod 15 \div 11 \bmod 15 = 5 \cdot 11^{-1}$$

Now we need to find the Multiplicative Inverse of 1.

$$11^{-1} = \gcd(11, 15)$$

We can compute the Greatest Common Divisor efficiently with the Euclidean Algorithm.

$$\begin{aligned}15 &= 1 \cdot 11 + 4\\ 11 &= 2 \cdot 4 + 3\\ 4 &= 1 \cdot 3 + 1\\ 3 &= 3 \cdot 1 + 0\end{aligned}$$

Thus, the Euclidean Algorithm gives us $\gcd(11, 15) = 1$. Since $\gcd(11, 15) = 1 = 1$, 11 **does** have a Multiplicative Inverse, making the division possible. Now we need to run through the Extended Euclidean Algorithm, to find the values $x, y \in \mathbb{Z}$.

$$\begin{aligned}
1 &= 4 - 1 \cdot 3 \\
&= 4 - 1 \cdot (11 - 2 \cdot 4) = 3 \cdot 4 - 1 \cdot 11 \\
&= 3(15 - 1 \cdot 11) - 1 \cdot 11 \\
&= 3 \cdot 15 - 3 \cdot 11 - 1 \cdot 11 \\
&= 3 \cdot 15 - 4 \cdot 11
\end{aligned}$$

Thus,

$$\begin{aligned}
x &= -4 \\
y &= 3
\end{aligned}$$

Now we know

$$(11 \bmod 15)^{-1} = -4 \bmod 15$$

Since -4 is not part of $\mathbb{Z}_{15}$, we need to find the additive inverse. $-4 + 15 = 11$. Thus,

$$(11 \bmod 15)^{-1} = 11 \bmod 15$$

Now, we perform a simple substitution.

$$\begin{aligned}
5 \bmod 15/11 \bmod 15 &= 5 \bmod 15 \cdot (11 \bmod 15)^{-1} \\
&= 5 \bmod 15 \cdot 11 \bmod 15 \\
&= 55 \bmod 15 \\
&= 10
\end{aligned}$$

So, the result of the division of 5 by 11 is 10.

Example 3.5: Impossible Division on Integers mod n.

When dealing with the set of integers $\mathbb{Z}_{15}$, what is the result from the division of 5 by 9?

$$5 \bmod 15 \div 9 \bmod 15 = 5 \cdot 9^{-1}$$

Now we need to find the Multiplicative Inverse of 9.

$$9^{-1} = \gcd(9, 15)$$

We can compute the Greatest Common Divisor efficiently with the Euclidean Algorithm.

$$\begin{aligned}
15 &= 1 \cdot 9 + 6 \\
9 &= 1 \cdot 6 + 3 \\
3 &= 1 \cdot 3 + 0
\end{aligned}$$

Thus, the Euclidean Algorithm gives us $\gcd(9, 15) = 3$. Since $\gcd(9, 15) = 3 \neq 1$, 9 does **not** have a Multiplicative Inverse, making the division impossible.

3.3 Chinese Remainder Theorem

Theorem 3.1 (Chinese Remainder Theorem)**.** *Let the integers $n_1, n_2, \ldots, n_k$ be pairwise Relatively Prime. Then the system of Congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution modulo $n = n_1 n_2 \cdots n_k$.

Defn 29 (Gauss's Algorithm)**.** The solution x to the system of Congruences promised by the Chinese Remainder Theorem can be calculated as

$$x = \left(\sum_{i=1}^{k} a_i N_i M_i \right) \bmod n \tag{3.2}$$

where $N_i = \frac{n}{n_i}$ and $M_i = N_i^{-1} = \left(\frac{n}{n_i}\right)^{-1} \bmod n_i$ (M_i is the Multiplicative Inverse of $N_i \bmod n_i$).

This simplifies to

$$x = \sum_{i=1}^{k} a_i \frac{n}{n_i} \left(\frac{n_i}{n} \bmod n \right) \tag{3.3}$$

Defn 30 (Chinese Remainder Theorem)**.** The *Chinese Remainder Theorem* allows us to change the way we represent elements of our set, $\mathbb{Z}_n$.

The integers modulo n, $\mathbb{Z}_n$, where $n = n_1 n_2$ and $\gcd(n_1, n_2) = 1$. An element $a \in \mathbb{Z}_n$ has a unique representation: $(a \bmod n_1, a \bmod n_2)$. We can denote this mapping by $\gamma : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$.

(i) $\gamma(a) = \gamma(b)$ if and only if $a = b$.
(ii) For all $(a_1, a_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, there exists an a such that $\gamma(a) = (a_1, a_2)$.
(iii) $\gamma(a + b) = \gamma(a) + \gamma(b)$
(iv) $\gamma(ab) = \gamma(a)\gamma(b)$

These properties (Properties **(i)** to **(iv)**) make γ an *Isomorphism.*

Remark 30.1. In the case of large integers for cryptography, knowing just one part of the number can ehlp get the other part. However, if the number is very large, 2048 bits for instance, these calculations start becoming Intractable.

Example 3.6: Chinese Remainder Theorem Mapping.

Find the mapping of 7 when in $\mathbb{Z}_{15}$?

We need to find a prime factorization for 15.

$$15 = 3^1 \cdot 5^1$$

So, the 2 modulos we will use are 3 and 5. Additionally, since 7 is an element in $\mathbb{Z}_{15}$ we can simply say,

$$7 \Leftrightarrow (7 \bmod 3,\ 7 \bmod 5) = (1, 2)$$

3.4 Multiplicative Groups, $\mathbb{Z}_n^*$

Defn 31 (Multiplicative Group, $\mathbb{Z}_n^*$)**.** Define the *multiplicative group* of $\mathbb{Z}_n$, denoted $\mathbb{Z}_n^*$ as the set of all elements in $\mathbb{Z}_n$ with Multiplicative Inverses.

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \,|\, \gcd(a, b) = 1\} \tag{3.4}$$

Defn 32 (Set Order)**.** The *order a set*, for example, $\mathbb{Z}_n^*$, is the number of elements in $\mathbb{Z}_n^*$ ($|\mathbb{Z}_n^*|$). From the definition of the Euler Phi Function

$$|\mathbb{Z}_n^*| = \phi(n) \tag{3.5}$$

Remark 32.1 (Closed Under Multiplication). Since the produce of two elements with Multiplicative Inverses is another element with a Multiplicative Inverse, we say that $|\mathbb{Z}_n^*|$ is *closed under multiplication.*

Defn 33 (Element Order)**.** The *order of an element* $a \in \mathbb{Z}_n^*$, denoted $\mathrm{ord}(a)$ is defined as the least positive integer t ($t \in \mathbb{Z}$) such that

$$a^t \bmod n = 1 \tag{3.6}$$

Lemma 3.1.1 (Element Order)**.** *Let $a \in \mathbb{Z}_n^*$. If a^s for some s, then $ord(a) \mid s$. In particular, $ord(a) \mid \phi(n)$ must be true.*

Example 3.7: Element Order. Exercise 1, Problem 1.6b

Find the ord(5) in $\mathbb{Z}_8^*$?

We need to solve

$$a^t \bmod n = 1$$

where $a = 5$ and $n = 8$.

$$5^t \bmod 8 = 1$$

Now we test values for t until we satisfy the equation.

$$t = 1 \rightarrow 5^1 \bmod 8 = 5 \bmod 8 = 5 \neq 1$$
$$t = 2 \rightarrow 5^2 \bmod 8 = 25 \bmod 8 = 1 = 1$$

Since $t = 2$ satisfies our equation, the $\text{ord}(5) = 2$.

Element Order. Let $t = \text{ord}(a)$. By long division, $s = qt + r$, where $r < t$. Then $a^s = a^{qt+r} = a^{qt}a^r$ and since $a^t = 1$, from Equation (3.6), we have $a^s = a^r$ and $a^r = 1$. This reduction is shown below:

$$\begin{aligned} a^s &= a^{qt+r} \\ &= a^{qt}a^r \\ &= \left(a^t\right)^q a^r \\ &= (1)^q a^r \\ &= 1^q a^r \\ &= 1a^r \\ &= a^r \end{aligned}$$

But, $r < t$, so we must have $r = 0$, and so $\text{ord}(a) \mid s$. ∎

3.5 Euler's Theorem

Theorem 3.2 (Euler's Theorem)**.** *If $a \in \mathbb{Z}_n^*$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{3.7}$$

Euler's Theorem. Let $\mathbb{Z}_n^* = \{a_1, a_2, \ldots, a_{\phi(n)}\}$. Looking at the set of elements $A = \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$, it is easy to see that $A = a\,\mathbb{Z}_n^*$. So we have 2 ways of writing the product of all of the elements, i.e.

$$\prod_{i=1}^{\phi(n)} aa_i = \prod_{i=1}^{\phi(n)} a_i$$

This leads to

$$\prod_{i=1}^{\phi(n)} a = a^{\phi(n)} = 1$$

which is the same as what we said in Equation (3.7). ∎

3.6 Fermat's Little Theorem

Theorem 3.3 (Fermat's Little Theorem)**.** *Let p be a Prime number. If $\gcd(a, p) = 1$, then*

$$a^{p-1} \equiv 1 \pmod{p} \tag{3.8}$$

Remark. This ties in with Euler's Theorem, because working in $\mathbb{Z}_n$, all exponents can be reduced by modulo $\phi(n)$.

3.7 Generators

Defn 34 (Generator)**.** Let $a \in \mathbb{Z}_n^*$. If the Element Order of a is equal to the Euler Phi Function, i.e. $\operatorname{ord}(a) = \phi(n)$, then a is said to be a *generator* (or a *primitive element*) of $\mathbb{Z}_n^*$.

$$\operatorname{ord}(a) = \phi(n) \tag{3.9a}$$

$$\operatorname{ord}(a) = |\mathbb{Z}_n^*| \tag{3.9b}$$

Furthermore, if $\mathbb{Z}_n^*$ has a generator, then $\mathbb{Z}_n^*$ is said to be*Cyclic*.

Remark 34.1. It is clear that if $a \in \mathbb{Z}_n^*$ is a Generator, then every element in $\mathbb{Z}_n^*$ can be expressed as a^i for some integer i ($i \in \mathbb{Z}$). So, we can write

$$\mathbb{Z}_n^* = \{a^i | 0 \leq i \leq \phi(n) - 1\} \tag{3.10}$$

Example 3.8: Cyclic Group. Exercise 1, Problem 1.6c

Is $\mathbb{Z}_8^*$ a Cyclic Group?

We need to find an a that satisfies $\operatorname{ord}(a) = \phi(n)$. In this case $n = 8$. First, we will calculate $\phi(n)$.

$$\phi(n) = \phi(8)$$

We need to find a Prime factorization of 8.

$$\begin{aligned}\phi(8) &= \phi\left(2^3\right) \\ &= \left(2^3 - 2^{3-1}\right) \\ &= \left(2^3 - 2^2\right) \\ &= (8 - 4) \\ &= 4\end{aligned}$$

So, $\phi(8) = 4$.
Now we need to solve

$$\operatorname{ord}(a) = 4$$

All of the terms in $\mathbb{Z}_8^*$ must be Invertible, so they **must** satisfy $\gcd(z, 8) = 1$, $z \in \mathbb{Z}_8$. All of the terms in $\mathbb{Z}_8$ are:

$$\mathbb{Z}_8 = \Big\{[0], [1], [2], [3], [4], [5], [6], [7]\Big\}$$

Now we check the Greatest Common Divisors for $z \in \mathbb{Z}_8$.

$$\begin{aligned}\gcd(0, 8) &= 8 & \gcd(4, 8) &= 2 \\ \gcd(1, 8) &= 1 & \gcd(5, 8) &= 1 \\ \gcd(2, 8) &= 2 & \gcd(6, 8) &= 2 \\ \gcd(3, 8) &= 1 & \gcd(7, 8) &= 1\end{aligned}$$

So,

$$\mathbb{Z}_8^* = \Big\{[1], [3], [5], [7]\Big\}$$

Now we test $\operatorname{ord} a = 4$, $a \in \mathbb{Z}_8^*$.

$$\begin{aligned}&\operatorname{ord}(1) = 1 \\ \operatorname{ord}(3) = 3^t \bmod 8 = 1 \to t = 2 \to &\operatorname{ord}(3) = 2 \\ &\operatorname{ord}(5) = 2 \\ \operatorname{ord}(7) = 7^t \bmod 8 = 1 \to t = 2 \to &\operatorname{ord}(7) = 2\end{aligned}$$

Since no element from $\operatorname{ord}(\mathbb{Z}_8^*) = \phi(8) = 4$, $\mathbb{Z}_8^*$ is **NOT** Cyclic.

3.8 Quadratic Residues

Defn 35 (Quadratic Residue)**.** An element $a \in \mathbb{Z}_n^*$ is said to be a *quadratic residue* modulo n (or a *square*) if there exists an $x \in \mathbb{Z}_n^*$ such that $x^2 = a$.

$$a \in \mathbb{Z}_n \, \exists x \in \mathbb{Z}_n^* \;\; x^2 = a \pmod{n} \tag{3.11a}$$

$$a \in \mathbb{Z}_n \, \exists x \in \mathbb{Z}_n^* \;\; a \equiv x^2 \pmod{n} \tag{3.11b}$$

Remark 35.1 (Square Root)*.* If $x^2 = a$, then x is called the *square root* of a mod n.

Otherwise, a is called a *Quadratic Non-Residue modulo n*.

Defn 36 (Quadratic Non-Residue)**.** An element $a \in \mathbb{Z}_n^*$ is said to be a *quadratic non-residue* modulo n if there does not exist an $x \in \mathbb{Z}_n^*$ such that $x^2 = a$.

$$a \in \mathbb{Z}_n \, \nexists x \in \mathbb{Z}_n^* \;\; x^2 = a \pmod{n}$$

Otherwise, a is called a *Quadratic Residue modulo n*.

4 Abstract Algebra

In the beginning of this course, we covered some basic abstract algebra. These include:

- Aspects covering integers and calculus modulo n
- Covering a few examples of algebraic structures
- Some basic concepts from abstract algebra, which provide a more general treatement of algebraic structures
- In cryptography, we are generally interested in *finite* sets

4.1 Groups

Defn 37 (Binary Operation)**.** A *binary operation*, denoted $*$ on a set S, is a mapping from $S * S$ to S.

Remark 37.1. Note that $*$ is **NOT** multiplication nor any kind of convolution. It is just a placeholder for some Binary Operation that can be done.

Defn 38 (Group)**.** A *group* is a set G and a Binary Operation, $*$, on G denoted as $(G, *)$, which satisfies the following properties:

(i) $a * (b * c) = (a * b) * c$ for all $a, b, c, \in G$ (Associativity)..

(ii) There is a special element $1 \in G$ such that $a * 1 = 1 * a = a$ for all $a \in G$ (Identity).

$$\exists 1 \in G \forall a \in G \; (a * 1 = 1 * a = a)$$

(iii) For each $a \in G$ there is an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$ (Inverse).

We call 1 the *identity element* as defined in Property **(ii)**, and call a^{-1} the *inverse* of a. Furthermore,

(iv) If $a * b = b * a$ for all $a, b \in G$ (Abelian/Commutativity).

$$\forall a, b \in G \; (a * b = b * a)$$

Example 4.1: Show Set Is Group. Exercise 1, Problem 1.8a

Let S be the set of binary triples, $S = \{(s_0, s_1, s_2) \, | s_i \in \mathbb{Z}_2\}$. Let the operation be bitwise addition.

Remark. In this case, "bitwise addition" means element-wise addition, i.e. each element of each triple gets added together. Additionally, all additions are done in modulo 2.

I will define the bitwise addition Binary Operation with the symbol .+, like how MATLAB or GNU Octave define it. We will need to prove that Properties **(i)** to **(ii)** are true. Property **(iv)** is *not* necessary to show that a set is a Group. Property **(iv)** only shows that the Group is Abelian
First, the elements present in the set S:

$$S = \Big\{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\Big\}$$

To prove that S is a group with an element-wise addition Binary Operation, I will arbitrarily select

$$
\begin{aligned}
a &= (0,1,0) \\
b &= (0,1,1) \\
c &= (1,1,0)
\end{aligned}
$$

Starting with Property **(i)**:

$$
\begin{aligned}
a \,.+ (b \,.+ c) &= (a \,.+ b) \,.+ c \\
(0,1,0) \,.+ \big((0,1,1) \,.+ (1,1,0)\big) &= \big((0,1,0) \,.+ (0,1,1)\big) \,.+ (1,1,0) \\
(0,1,0) \,.+ \big((1,0,1)\big) &= \big((0,0,1)\big) \,.+ (1,1,0) \\
(1,1,1) &= (1,1,1)
\end{aligned}
$$

Thus, Property **(i)** is satisfied.
Now, Property **(ii)**

$$
\begin{aligned}
a \,.+ 1 &= a \\
(0,1,0) \,.+ 1 &= (0,1,0) \\
1 &= (0,1,0) \,.+ \Big(-(0,1,0)\Big)
\end{aligned}
$$

It is important to remamber that these additions are done in the modulo 2 domain, so addition and subtraction yield the same results, making negatives irrelevant.

$$
\begin{aligned}
1 &= (0,1,0) \,.+ (0,1,0) \\
1 &= (0,0,0)
\end{aligned}
$$

Thus, Property **(ii)** is satisfied, and $1 = (0,0,0)$.
Lastly, we need to prove Property **(iii)**.

$$
\begin{aligned}
a \,.+ a^{-1} &= 1 \\
(0,1,0) \,.+ a^{-1} &= (0,0,0) \\
a^{-1} &= (0,0,0) \,.+ \Big(-(0,1,0)\Big)
\end{aligned}
$$

Like before, addition and subtraction are irrelevant here.

$$
\begin{aligned}
a^{-1} &= (0,0,0) \,.+ (0,1,0) \\
a^{-1} &= (0,1,0)
\end{aligned}
$$

Thus, Property **(iii)** is satisfied, where each element a is its own inverse.
Since Properties **(i)** to **(iii)** are satisfied, S **is** a Group with the bitwise addition Binary Operation.

Defn 39 (Abelian)**.** An *abelian* group, also called a *commutative Group*, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written. That is, these are the groups that obey the axiom of commutativity.

4.1.1 Examples of Groups

- $\mathbb{Z}$ with the addition Binary Operation, denoted $(\mathbb{Z}, +)$ is a Group.
- Finite Groups are $(\mathbb{Z}_n\,, +)$ and $(\mathbb{Z}_n^*\,, \cdot)$, where $\cdot$ denotes multiplication modulo n
- **NOTE:** $(\mathbb{Z}_n\,, \cdot)$ is **NOT** a Group, nor is $(\mathbb{Z}, \cdot)$.

4.1.2 Definitions for Groups

Defn 40 (Subgroup)**.** A non-empty subset H of a Group G is called a *subgroup* of G, if H itself is a Group with respect to the operation of G.

Example 4.2: Find Subgroups. Exercise 1, Problem 1.10

Find all Subgroups in the multiplicative group $\mathbb{Z}_{19}^*$ (under the multiplication Binary Operation)?

The goal here is to find a Generator that can be raised to some set of exponents that can generate Subgroups of $\mathbb{Z}_{19}^*$. The first thing to note is that 19 is a Prime, so

$$|\mathbb{Z}_{19}^*| = 18 = \phi(n)$$

We can also apply Lagrange's Theorem to restrict the number of Subgroups possible. Because $\mathbb{Z}_{19}^*$ is a finite Group, and we are considering G to be a Subgroup of $\mathbb{Z}_{19}^*$, we apply Lagrange's Theorem. This means $|G| \, ||\mathbb{Z}_{19}^*|$ must be true. Thus,

$$|G| = \{1, 2, 3, 6, 9, 18\}$$

Now, we can find a Generator for the Group $\mathbb{Z}_{19}^*$. This means, we need to find some element a that raised to some power t, modulo 19 will yield 1. We know that t **must** equal 18, because $\phi(n) = 18$, and we want to find a Generator. So, we solve for a.

$$a^{18} \bmod 18 = 1$$

In this case, $a = 2$, making 2 a Generator of $\mathbb{Z}_{19}^*$, or $< 2 >$.
Now, all possible Subgroups of $\mathbb{Z}_{19}^*$ are:

$$\begin{aligned}
G_1 &= \left\{ \left[2^{18}\right] \right\} \\
G_2 &= \left\{ \left[2^{9}\right], \left[2^{18}\right] \right\} \\
G_3 &= \left\{ \left[2^{6}\right], \left[2^{12}\right], \left[2^{18}\right] \right\} \\
G_6 &= \left\{ \left[2^{3}\right], \left[2^{6}\right], \left[2^{9}\right], \left[2^{12}\right], \left[2^{15}\right], \left[2^{18}\right] \right\} \\
G_9 &= \left\{ \left[2^{2}\right], \left[2^{4}\right], \left[2^{6}\right], \left[2^{8}\right], \left[2^{10}\right], \left[2^{12}\right], \left[2^{14}\right], \left[2^{16}\right], \left[2^{18}\right] \right\} \\
G_{18} &= \left\{ \left[2^{0}\right], \left[2^{1}\right], \ldots, \left[2^{18}\right] \right\}
\end{aligned}$$

Defn 41 (Cyclic)**.** G is *cyclic* if there is an element $a \in G$ such that each $b \in G$ can be written as a^i for some integer i. The element a is called a *Generator* of G.

Example 4.3: Cyclic.

Find a, the Cyclic term in the Group $\mathbb{Z}_{15}$?

$$\begin{aligned}
\mathbb{Z}_{15} &= \{3, 6, 9, 12, 0, \ldots\} \\
&= \{3, 3+3, 3+3+3, 3+3+3+3, 5 \cdot 3, \ldots\}
\end{aligned}$$

Thus, $< a >= 3 \rightarrow < 3 >$.

Defn 42 (Element Order)**.** The *order of an element a*, denoted ord(a) is defined as the least positive integer t ($t \in \mathbb{Z}$) such that

$$a^t = 1 \tag{4.1}$$

If such an integer t does not exist, then the order of a is defined to be ∞.

Remark 42.1. **NOTE:**

- The a^t part does not mean exponentiation, but rather repeated uses of the Binary Operation used to create the Group.
- The 1 is not a value 1, but the Identity of the Group, as defined by Property **(ii)**.

Example 4.4: Order of Element in Group. Exercise 1, Problem 1.8c

Given the element $(1,1,1,)$ from the group of bit triples, $S = \{(s_0, s_1, s_2)\,|s_i \in \mathbb{Z}_2\}$, using an bitwise addition Binary Operation, what is the Element Order of $(1,1,1)$? The identity element of this Group is $1 = (0,0,0)$.

It is important to remember the note in Remark 42.1, especially for this problem.
Since the given Binary Operation was "bitwise", i.e. element-wise, I will define the operation to be $.+$. In this case, the Element Order of any element in this Group will be the number of element-wise additions that must occur to get the identity element, 1.
For this problem, since we are working in the modulo 2 domain, we have some basic facts:

$$\begin{aligned}(0+0) \bmod 2 &= 0\\(1+0) \bmod 2 &= 1\\(0+1) \bmod 2 &= 1\\(1+1) \bmod 2 &= 0\end{aligned}$$

And for subtraction:

$$\begin{aligned}&(0-0) \bmod 2 = 0\\&(1-0) \bmod 2 = 1\\&(0-1) \bmod 2 = -1 \bmod 2 = 1\\&(1-1) \bmod 2 = 0\end{aligned}$$

We start by constructing the equation needed to solve this problem.

$$(1,1,1). + a = (0,0,0)$$

Now we can move the $(1,1,1)$ term over to the left, and since we are working in the modulo 2 domain, the "negative" that would be introduced by normal subtraction (negative addition) is irrelevant. Thus, we end up with

$$\begin{aligned}a &= (0,0,0). + (1,1,1)\\&= (1,1,1)\end{aligned}$$

This means that if t from Equation (4.1) is 2, we get the identity element 1. So, our answer is $t = 2$, thus $\operatorname{ord}\big[(1,1,1)\big] = 2$.

Lemma 4.0.1. *Let $a \in G$ be an element of finite Element Order t. Then the set of all powers of a forms a Cyclic Subgroup of G, denoted by $< a >$. Furthermore, the Element Order of $< a >$ is t.*

Defn 43 (Left Coset)**.** Let H be a Subgroup in G and pick an element $a \in G$. A set of elements of the form

$$aH = \{ah|h \in H\} \tag{4.2}$$

is called the *left coset* of H. If G is commutative, it is simply called a *coset*.

The set consisting of all such left cosets is written G/H. Note that H itself is a left coset. Furthermore, every left coset contains the same number of elements (the order of H) and every element is contained in exactly one left coset.

So, the elements of G are partitioned into $|G|/|H|$ different cosets, each containing $|H|$ elements.

4.2 Properties of Groups

(i) Suppose $a^n = 1$ for some $n > 0$. We must have $ElementOrder(a)\,|\,n$.

1. Write $n = k \cdot \operatorname{ord}(a) + r$, where $0 \leq r \leq \operatorname{ord}(a)$.
2. Then, $1 = a^n = a^{k \cdot \operatorname{ord}(a) + r} = a^r$ and $r = 0$.

(ii) There is a k such that $a^k = 1$ for all $a \in G$.

1. If G is a finite Group, all elements must have finite Element Order.
2. Choose k as the product of the Element Order of all different elements in G.
3. Then, $a^k = 1$ for all $a \in G$

4.2.1 Lagrange's Theorem

Theorem 4.1 (Lagrange's Theorem)**.** *If G is a finite group and H is a Subgroup of G, then $|H|$ divides $|G|$. In particular if $a \in G$, then the order of a divides $|G|$.*

Remark. If $|G|$ is a Prime number, then the order of an element a is either 1 or $|G|$. In particular, if $|G|$ is a Prime number, then G must be Cyclic.

4.3 Rings

Defn 44 (Ring)**.** A *ring* (with unity) consists of a set R with two Binary Operations. A ring is denoted as $(R, +, *)$., where $+$ and $*$ are **not** addition and multiplication respectively, but placeholders for the two Binary Operations. A ring must also satisfy the following conditions:

(i) $(R, +)$ is an Abelian Group with an identity element denoted 0.

(ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$ (Associativity).

$$\forall a, b, c \in R \, a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) There is a multiplicative identity, denoted 1, with the multiplicative identity not being equal to the identity element of the underlying Abelian Group $(1 \neq 0)$, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$ (Multiplicative Identity).

(iv) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$ (Distributive).

$$\forall a, b, c \in R \, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$\forall a, b, c \in R \, (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

A *commutative ring* is a ring where additionally

(v) $a \cdot b = b \cdot a$ for all $a, b \in R$ (Commutativity)

$$\forall a, b \in R \, a \cdot b = b \cdot a$$

Remark 44.1 (Ring Multiplicative Inverses)*.* Note that we haven't said anything about multiplicative inverses yet.

Defn 45 (Invertible Element)**.** An element $a \in R$ is called an *invertible element* or a *unit* if there is an element $b \in R$ such that

$$a \cdot b = b \cdot a = 1 \tag{4.3}$$

Remark 45.1. The set of Invertible Elements in a Ring R forms a Group under multiplication. For example, the Group of Invertible Elements of the Ring $\mathbb{Z}_n$ is $\mathbb{Z}_n^*$.

Remark 45.2 (Multiplicative Inverse). The Multiplicative Inverse of an element $a \in R$ is denoted by a^{-1}, assuming it exists. The division expression a/b should then be interpreted as $a \cdot b^{-1}$.

4.3.1 Examples of Rings

- A commutative ring is $(\mathbb{Z}, +, \cdot)$, where $+$ and $\cdot$ are the susual operations of addition and multiplication.
- Finite Ring: $\mathbb{Z}_n$ with addition and multiplication modulo n
  - The additive inverse of $a \in R$ is denoted $-a$. So the subtraction expression $a - b$ should be interpreted as $a + (-b)$.
  - The multiplication of $a \cdot b$ is equivalently written ab.
  - Similarly $a^2 = aa = a \cdot a$.

4.4 Fields

Defn 46 (Field)**.** A *field* is a commutative Ring where all nonzero elements from the underlying set have Multiplicative Inverses.

Example 4.5: Prove Set is Not Field. Exercise 1, Problem 1.11

Prove that $\mathbb{Z}_4$ is not a Field?

We begin by checking that all elements from the underlying set, $\mathbb{Z}_4$, have Multiplicative Inverses, for all the **non-zero** elements.

$$\mathbb{Z}_4 = \Big\{[0], [1], [2], [3]\Big\}$$

First, we check 1.

$$1^{-1} = \gcd(1, 4) = 1a + 4b$$

$$
\begin{aligned}
\gcd(1,4) \Rightarrow 4 &= q1 + r \\
&= 4 \cdot 1 + 0 \\
\gcd(1,4) &= 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1(-3) + 4(1) \\
a &= -3 \\
b &= 1
\end{aligned}
$$

Since $a = -3$, we need to find the additive inverse:

$$
\begin{aligned}
-3 \bmod 4 &= (-3 + 4) \bmod 4 \\
&= 1 \bmod 4 \\
&= 1
\end{aligned}
$$

So, 1 has a Multiplicative Inverse.
Now we check 2.

$$2^{-1} = \gcd(2,4) = 2a + 4b$$

$$
\begin{aligned}
\gcd(2,4) \Rightarrow 4 &= q2 + r \\
&= 2 \cdot 2 + 0 \\
\gcd(2,4) &= 2
\end{aligned}
$$

Since $\gcd(2,4) \neq 0$, 2 is **not** invertible, meaning it has no Multiplicative Inverses.
$\mathbb{Z}_4$ is NOT a Field because 2 is **not** invertible.

Defn 47 (Characteristic)**.** The *characteristic* of a field is the smallest integer $m > 0$ such that

$$\overbrace{1 + 1 + \cdots + 1}^{m} = 0 \tag{4.4}$$

If no such integer m exists, the characteristic is defined to be 0.

Defn 48 (Finite Field)**.** A Field is *finite* only if Theorem 4.2 is satisfied.

Theorem 4.2 (Finite Field)**.** *$\mathbb{Z}_n$ is a Field if and only if n is a Prime number. If n is a Prime, the Characteristic of $\mathbb{Z}_n$ is n.*

Defn 49 (Subfield)**.** A subset F of a Field E is called a *subfield* of E if F is itself a Field with respect to the operations of E.

Remark 49.1 (Extension Field)*.* Likewise, we say E is an *extension field* of F.

Defn 50 (Isomorphism)**.** Two Fields are *isomorphic* if they are structurally the same, but elements hvae a different representation. For example, for a Prime, p, $\mathbb{Z}_p$ is a Field or Set Order p. So we associate the Finite Field $\mathbb{F}_{p^w}$ith $\mathbb{Z}_p$ and its representation.

4.4.1 Examples of Fields

- The rational Numbers: $\mathbb{Q}$
- The Real Numbers: $\mathbb{R}$
- The Complex Numbers: $\mathbb{C}$
- Finite Field:
  - $\mathbb{Z}_p$, where p is Prime

4.5 Polynomial Rings

Polynomial Rings are getting their own subsection separate from other Rings, because they are actually a more general case of what we have learned already.

Defn 51 (Polynomial)**.** A *polynomial* in the indeterminate x over the Ring R is an expression of the form

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \tag{4.5}$$

where each $a_i \in R$, $a_n \neq 0$, and $n \geq 0$.

Remark 51.1. **Remember that even integers can be polynomials!** This means that everything we have learned about Rings already is actually a special case of Polynomial Rings.

$$1 = 0x^m + 0x^{m-1} + \cdots + 0x + 1$$

Defn 52 (Degree)**.** We say that $f(x)$ has *degree* n, denoted

$$\deg f(x) = n \tag{4.6}$$

Remark 52.1. We also allow $f(x)$ to be the Polynomial with all coefficients being zero, in which case, the Degree is defined to be $-\infty$.

Defn 53 (Monic)**.** A Polynomial is said to be *monic* if the leading coefficient is equal to 1.

$$a_n = 1 \tag{4.7}$$

Defn 54 (Polynomial Ring)**.** Let R be a commutative Ring (i.e. Property **(v)** is fulfilled). Then the *polynomial ring*, denoted by $R[x]$ is the ring formed by the set of all Polynomials in the indeterminate x having coefficients from R. The operations are addition and multiplication of Polynomials, with the coefficient arithmetic performed in R.

Example 4.6: Polynomial Ring. Lecture 2

Find the Polynomial Ring formed when the underlying Ring is $\mathbb{Z}_2$?

$$\mathbb{Z}_2 \underset{R[x]}{\Longrightarrow} \mathbb{Z}_2[x] = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x, x^2+x+1, \ldots\}$$

If you consider the $F[x]$, where F denotes an arbitrary Field. $F[x]$ has many properties in common with integers.

Defn 55 (Irreducible)**.** A polynomial $f(x) \in F[x]$, of Degree $d \geq 1$ is *irreducible* if $f(x)$ cannot be written as a product of 2 polynomials, $g(x), h(x) \in F[x]$, where the $\deg g(x)$ and $\deg h(x)$ are both less than d.

Remark 55.1 (Sum to Zero). It seems that Irreducible Polynomials, $f(x)$, where $f(x) \in \mathbb{F}_{p^q}$ must sum to a non-zero value for all values of x from the underlying set of integers, $\mathbb{Z}_p$.

Remark 55.2 (Relation Between Irreducible Polynomials and Prime Numbers). Irreducible polynomials are the Polynomial Ring counterpart of Prime numbers.

Example 4.7: Irreducible Polynomial. Exercise 1, Problem 1.14a

Is $f(x) = x^4 + x + 1$ in $\mathbb{Z}_2$ an Irreducible Polynomial and/or a Primitive Element?

We start by checking the Sum to Zero conditions.

$$f(0) = 0^4 + 0 + 1 = 1$$
$$f(1) = 1^4 + 1 + 1 = 1$$

The Sum to Zero conditions for this Polynomial.
Because our Polynomial is of Degree 4, we can factor it 2 ways:

1.
$$\left(x^2 + y\right)\left(x^2 + z\right) = x^4 + yx^2 + zx^2 + yz$$
$$x^4 + yx^2 + zx^2 + yz = x^4 + x + 1$$

   This cannot work, because there are no x^2 terms in the potential factorization.

2.
$$(x + y)\left(x^3 + z\right) = x^4 + yx^3 + zx + yz$$
$$x^4 + yx^3 + zx + yz = x^4 + x + 1$$

This also cannot work, because the coefficient's terms do not line up ($y \neq 0$ because $yz = 1$).

Thus, $f(x)$ is an Irreducible.
Now we need to check if $f(x)$ is a Primitive Element.

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 \\
\alpha^4 &= \alpha + 1 \\
\alpha^5 &= \alpha^2 + \alpha \\
\alpha^6 &= \alpha^3 + \alpha^2 \\
\alpha^7 &= \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1
\end{aligned}$$

$$\begin{aligned}
\alpha^8 &= \alpha^4 + \alpha^2 + \alpha = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1 \\
\alpha^9 &= \alpha^3 + \alpha \\
\alpha^{10} &= \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1 \\
\alpha^{11} &= \alpha^3 + \alpha^2 + \alpha \\
\alpha^{12} &= \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^{13} &= \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha + 1 = \alpha^3 + \alpha^2 + 1 \\
\alpha^{14} &= \alpha^4 + \alpha^3 + \alpha = \alpha + 1 + \alpha^3 + \alpha = \alpha^3 + 1 \\
\alpha^{15} &= \alpha^4 + \alpha = \alpha + 1 + \alpha = 1
\end{aligned}$$

Because $\alpha^4 = \alpha + 1$ can generate all Polynomials in $\mathbb{F}_{2^4}$, $f(x)$ is also Primitive Element.
Thus, the Polynomial, $f(x)$ is both Irreducible and a Primitive Element.

Example 4.8: Reducible Polynomial. Exercise 1, Problem 1.14c

Is $f(x) = x^4 + x + 1$ in $\mathbb{Z}_2$ an Irreducible Polynomial and/or a Primitive Element?

Just by inspection, Sum to Zero holds up.
Now we have to check if the Polynomial is reducible. I will arbitrarily choose to start with a factorization of

$$\begin{aligned}
\left(x^2 + c\right)\left(x^2 + c\right) &= x^4 + 2cx^2 + c^2 \\
x^4 + 2cx^2 + c^2 &= x^4 + x^2 + 1 \\
x^4 + c^2 &= x^4 + x^2 + 1 \\
c^2 &= x^2 + 0x + 1
\end{aligned}$$

Because of the modulo addition we are doing here, 2 mod 2 = 0, eases the factorization.

$$\begin{aligned}
c^2 &= x^2 + 2x + 1 \\
c^2 &= (x + 1)(x + 1) \\
c &= x + 1
\end{aligned}$$

So, $f(x)$ is reducible.
We can check if $f(x)$ is a Irreducible, though we don't have to.

$$\alpha^4 = \alpha^2 + 1$$

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 \\
\alpha^4 &= \alpha^2 + 1 \\
\alpha^5 &= \alpha^3 + \alpha \\
\alpha^6 &= \alpha^4 + \alpha^2 + \alpha^2 + 1 + \alpha^2 = 1
\end{aligned}$$

Thus, $f(x)$ is reducible and NOT a Primitive Element.

Example 4.9: Reducible Polynomial By Sum. Exercise 1, Problem 1.14d

Is $f(x) = x^4 + x + 1$ in $\mathbb{Z}_3$ an Irreducible Polynomial and/or a Primitive Element?

We can start by looking at Remark 55.1.

$$f(x=0) = 0^4 + 0 + 1 = 1 \bmod 3 = 1$$
$$f(x=1) = 1^4 + 1 + 1 = 3 \bmod 3 = 0$$
$$f(x=2) = 2^4 + 2 + 1 = 19 \bmod 3 = 1$$

Since there is a case where $f(x) = 0$ in the set $\mathbb{Z}_3$, $f(x)$ is reducible. We can make the table of α:

$$\alpha^4 = \alpha + 1$$

$$\begin{aligned}
\alpha^0 &= 1 & \alpha^8 &= \alpha^4 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1 \\
\alpha^1 &= \alpha & \alpha^9 &= \alpha^3 + \alpha \\
\alpha^2 &= \alpha^2 & \alpha^{10} &= \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1 \\
\alpha^3 &= \alpha^3 & \alpha^{11} &= \alpha^3 + \alpha^2 + \alpha \\
\alpha^4 &= \alpha + 1 & \alpha^{12} &= \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^5 &= \alpha^2 + \alpha & \alpha^{13} &= \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha + \alpha + \alpha^3 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + 1 \\
\alpha^6 &= \alpha^3 + \alpha^2 & \alpha^{14} &= \alpha^4 + \alpha^3 + \alpha = \alpha + 1 + \alpha^3 + \alpha = \alpha^3 + 1 \\
\alpha^7 &= \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1 & \alpha^{15} &= \alpha^4 + \alpha = \alpha + 1 + \alpha = 1
\end{aligned}$$

Thus, $f(x)$ is reducible and MAY be a Primitive Element.

4.5.1 Long Division of Polynomials

Similarly as for integers (Section 2.1), we have a division algorithm for polynomials.

Defn 56 (Polynomial Long Division)**.** If $a(x), b(x) \in F[x]$, with $b(x) \neq 0$, then there are polynomials $q(x), r(x) \in F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \tag{4.8}$$

where

- $\deg r(x) < \deg b(x)$.
- $q(x)$ and $r(x)$ are unique.
- $q(x)$ is referred to as the Polynomial Quotient
- $r(x)$ is referred to as the Polynomial Remainder

Defn 57 (Polynomial Quotient)**.** The *Polynomial quotient*, $q(x)$, of $a(x)$ divided by $b(x)$ ($a(x) \div b(x)$, $a(x)/b(x)$) is denoted $a(x) \operatorname{div} b(x)$.

Defn 58 (Polynomial Remainder)**.** The *Polynomial remainder*, $r(x)$, of $a(x)$ divided by $b(x)$ ($a(x) \div b(x)$, $a(x)/b(x)$) is denoted $a(x) \bmod b(x)$.

Example 4.10: Long Division of Polynomials. Lecture 3

Calculate $\left(x^3 + 11x^2 + x + 7\right) \bmod \left(x^2 + x + 3\right)$ while working in the Field $Z_{13}[x]$?

First thing to note is that $Z_{13}[x]$ is a Finite Field because 13 is a Prime. Now, we perform long division:

$$
\begin{array}{r}
x+10 \\
x^2+x+3 \overline{\smash{\big)}\ x^3+11x^2 \quad +x \quad +7} \\
-x^3 \quad -x^2 \quad -3x \qquad \\
\hline
10x^2 \quad -2x \quad +7 \\
-10x^2-10x-30 \\
\hline
-12x-23
\end{array}
$$

Since our Polynomial Remainder is $(-12x-23) \bmod 13$, we perform some reduction. Thus, the Polynomial Remainder is:

$$
\begin{aligned}
-12x \bmod 13 &= 1x \bmod 13 \\
-23 \bmod 13 = -10 \bmod 13 &= 3 \bmod 13
\end{aligned}
$$

So, the reduced Polynomial Quotient and Polynomial Remainder are:

$$
\begin{aligned}
q(x) &= x+10 \\
r(x) &= x+3
\end{aligned}
$$

4.5.2 Properties of Polynomial Rings

Defn 59 (Divide)**.** If $g(x), h(x) \in F[x]$, then $h(x)$ is said to *divide* $g(x)$, written

$$h(x) \mid g(x)\text{if } g(x) \bmod h(x) = 0 \tag{4.9}$$

Defn 60 (Congruent)**.** Let $g(x), h(x) \in F[x]$. Then, $g(x)$ is said to be *congruent* to $h(x)$ mod $f(x)$ if $f(x) \,|\big(g(x) - h(x)\big)$. We denote this

$$g(x) \equiv h(x) \pmod{f(x)} \tag{4.10}$$

(i) $g(x) \equiv h(x) \pmod{f(x)}$ if and only if $g(x)$ and $h(x)$ leave the same remainder when divided by $f(x)$.
(ii) $g(x) \equiv g(x) \pmod{f(x)}$.
(iii) If $g(x) \equiv h(x) \pmod{f(x)}$, the $h(x) \equiv g(x) \pmod{f(x)}$.
(iv) If $g(x) \equiv h(x) \pmod{f(x)}$ and $h(x) \equiv s(x) \pmod{f(x)}$, then $g(x) \equiv s(x) \pmod{f(x)}$.
(v) If $g(x) \equiv g_1(x) \pmod{f(x)}$ and $h(x) \equiv h_1(x) \pmod{f(x)}$, then:

- $g(x) + h(x) \equiv g_1(x) + h_1(x) \pmod{f(x)}$
- $g(x)h(x) \equiv g_1(x)h_1(x) \pmod{f(x)}$

We can divide $F[x]$ into sets called Equivalence Class, where each Equivalence Class contains all Polynomials that leaves a certain Polynomial Remainder when divided by $f(x)$.

Defn 61 (Equivalence Class)**.** By $F[x]/f(x)$, we denote the set of *equivalence class*es of Polynomials in $F[x]$ of degree less than $\deg f(x0$. The addition and multiplication operations are performed $\bmod f(x)$.

Defn 62 (Representative)**.** Since the Polynomial Remainder, $r(x)$ itself is a Polynomial in the Equivalence Class we use it as a *representative* of the Equivalence Class.

Defn 63 (Commutative Ring)**.** A commutative Ring for Polynomials is defined as

$$F[x]/f(x) \tag{4.11}$$

Remark 63.1. Note that this is the inverse condition of when a Polynomial Ring is a Field.

Defn 64 (Field)**.** If $f(x) \in F[x]$ is Irreducible, then $F[x]/f(x)$ is a Field.

Remark 64.1. Note that this is the inverse condition of when a Polynomial Ring is a Commutative Ring

Defn 65 (Finite Field)**.** A *finite Field* is a Field which contains a finite number of elements, i.e. the Set Order of the Field is not ∞.

(i) If F is a Finite Field, then the Set Order of F is p^m for some Prime p and integer $m \geq 1$.
(ii) For every Prime power order p^m, there is a unique (up to Isomorphism) Finite Field of Set Order p^m. This Field is denoted by $\mathbb{F}_{p^m}$ or $GF\left(p^m\right)$.
(iii) If $\mathbb{F}_q$ is a Finite Field of Set Order $q = p^m$, i.e. $\mathbb{F}_{p^m}$, the the *Characteristic* of $\mathbb{F}_q$ is p. Furthermore, $F[q]$ contains a copy of $\mathbb{Z}_p$ as a *Subfield*.

(iv) Let $\mathbb{F}_q$ be a Finite Field of Set Order $q = p^m$, i.e. $\mathbb{F}_{p^m}$. Then every Subfield of $\mathbb{F}_q$ has Set Order p^n for some positive integer n where $n \mid m$. Conversely, if $n \mid m$, then there is exactly one Subfield of $\mathbb{F}_q$ of Set Order p^n.

(v) An element $a \in \mathbb{F}_q$ is in the Subfield $\mathbb{F}_{p^n}$ if and only if $a^{p^n-1} = 1$.

Defn 66 (Multiplicative Group)**.** The non-zero elements of $\mathbb{F}_{q^a}$ll have inverses and thus, they form a Group under multiplication. This Group is called the *multiplicative group* of $\mathbb{F}_{q^a}$nd denoted by $\mathbb{F}_q^*$. It can be shown that $\mathbb{F}_q^*$ is a Cyclic Group (of Set Order $q-1$). Especially, this means that $a^{q-1} = 1$ for all $a \in \mathbb{F}_q$.

Defn 67 (Primitive Element)**.** A Generator of the Cyclic Group $\mathbb{F}_q^*$ is called a *primitive element*.

4.5.3 Extension of Greatest Common Divisor, Euclidean Algorithm, and Extended Euclidean Algorithm

Defn 68 (Greatest Common Divisor)**.** Let $g(x), h(x) \in \mathbb{Z}_p[x]$, where not both are zero. Then the *greatest common divisor, GCD*, of $g(x)$ and $h(x)$, denoted $\gcd\big(g(x), h(x)\big)$, is the Monic of greatest Degree in $Z_p[x]$ which Divides both $g(x)$ and $h(x)$.

Remark 68.1. By definition $\gcd(0, 0) = 0$.

Theorem 4.3 (Unique Factorization of Polynomials)**.** *Every non-zero polynomial $f(x) \in \mathbb{Z}_p[x]$ has a factorization*

$$f(x) = af_1(x)^{e_1} f_2(x)^{e_2} \cdots f_k(x)^{e_k} \tag{4.12}$$

where each $f_i(x)$ is a distinct Monic Irreducible Polynomial in $Z_p[x]$, the e_i are positive integers, and $a \in \mathbb{Z}_p$, where p is for Primes. The factorization is unique up to the rearrangement of factors.

Defn 69 (Polynomial Euclidean Algorithm)**.** Takes 2 non-negative Polynomials $a(x), b(x) \in \mathbb{F}_q[x]$. Returns the $\gcd\big(a(x), b(x)\big)$

1. Set $r_0(x) \leftarrow a(x)$, $r_1(x) \leftarrow b(x)$, $i \leftarrow 1$.
2. While $r_i(x) \neq 0$ do:
   (a) Set $r_{i+1}(x) \leftarrow r_{i-1}(x) \bmod r_i(x)$, $i \leftarrow i + 1$
3. Return the value $r_i(x)$.

This is demonstrated in Example 4.11

Example 4.11: Polynomial Euclidean Algorithm. Lecture 3

Given $f(x) = x^3 + x$, where $f(x) \in Z_2[x]$, find the Greatest Common Divisor of $f(x)$ given that $f(x)g(x) = 1 \bmod \big(x^4 + x + 1\big)$. Assume $f(x)g(x)$ is Irreducible.

Considering that $Z_2[x]/f(x)$ where $f(x) \in Z_2[x]$ and $f(x)$ is Irreducible, this is a Polynomial Ring. Since the order of the Polynomial Ring is a Prime power, this is a Finite Field. Because this is a Finite Field, $\mathbb{F}_{2^4}[] = 2^4 = 16$ elements. Now, we calculate the Polynomial Euclidean Algorithm.

$$\gcd\Big(\big(x^4 + x + 1\big), \big(x^3 + x\big) \Big)$$
$$x^4 + x + 1 = q(x)\big(x^3 + x\big) + r(x)$$

We can perform Polynomial Long Division to find $q(x)$ and $r(x)$ for this iteration.

$$\begin{array}{r} x \\ x^3 + x \big) \overline{\; x^4 \qquad + x + 1} \\ \underline{- x^4 - x^2 } \\ - x^2 + x + 1 \end{array}$$

So,

$$q(x) = x$$
$$r(x) = \big(-x^2 + x + 1\big) \bmod 2$$

We need to correct the coefficients in $r(x)$ with modulo 2 (where the coefficients come from in the first place).

$$\begin{aligned} r(x) &= \big(-x^2 + x + 1\big) \bmod 2 \\ &= x^2 + x + 1 \end{aligned}$$
$$x^4 + x + 1 = x\big(x^3 + x\big) + \big(x^2 + x + 1\big)$$

Now, the next iteration of Polynomial Euclidean Algorithm.

$$x^3 + x = q(x)\left(x^2 + x + 1\right) + r(x)$$

$$\begin{array}{r}
x - 1 \\
x^2 + x + 1 \overline{\big) \; x^3 \qquad + x} \\
\underline{- x^3 - x^2 - x} \\
- x^2 \qquad \\
\underline{x^2 + x + 1} \\
x + 1
\end{array}$$

$$\begin{aligned}
q(x) &= x - 1 \\
r(x) &= x + 1 \\
x^3 + x &= (x - 1)\left(x^2 + x + 1\right) + (x + 1)
\end{aligned}$$

Another iteration:

$$x^2 + x + 1 = q(x)(x + 1) + r(x)$$

$$\begin{array}{r}
x \\
x + 1 \overline{\big) \; x^2 + x + 1} \\
\underline{- x^2 - x} \qquad \\
1
\end{array}$$

$$\begin{aligned}
q(x) &= x \\
r(x) &= 1 \\
x^2 + x + 1 &= x(x + 1) + 1
\end{aligned}$$

Another iteration (the last):

$$x + 1 = q(x) \cdot 1 + r(x)$$

$$\begin{aligned}
q(x) &= x + 1 \\
r(x) &= 0 \\
x + 1 &= (x + 1) \cdot 1 + 0
\end{aligned}$$

Thus, the $\gcd\Big(x^4 + x + 1, x^3 + x\Big) = 1$.

Defn 70 (Extended Euclidean Algorithm)**.** let $a(x)$ and $b(x)$ be two non-negative polynomials in $F_q[x]$. Then, there exists polynomials $s(x), t(x)$ such that $\gcd\big(a(x), b(x)\big)$ can be written as

$$\gcd\big(a(x), b(x)\big) = a(x)s(x) + b(x)t(x) \tag{4.13}$$

This is demonstrated in Example 4.12

Example 4.12: Polynomial Extended Euclidean Algorithm. Lecture 3

Given $f(x) = x^3 + x$, where $f(x) \in Z_2[x]$, find $g(x)$ of $f(x)$ given that $f(x)g(x) = 1 \bmod \left(x^4 + x + 1\right)$. Assume $f(x)g(x)$ is Irreducible.

Since we know that the $\gcd\left(x^4 + x + 1, x^3 + x\right) = 1$, from Example 4.11, we can solve Equation (4.13).

$$
\begin{aligned}
1 &= \left(x^2+x+1\right) - x(x+1) \\
&= \left(x^2+x+1\right) - x\Big(\left(x^3+x\right) - (x-1)\left(x^2+x+1\right)\Big) = \left(x^2+x+1\right) - x\left(x^3+x\right) - x(x-1)\left(x^2+x+1\right) \\
&= \big(1 - x(x-1)\big)\left(x^2+x+1\right) - x\left(x^3+x\right) \\
&= \big(1 - x(x-1)\big)\Big(\left(x^4+x+1\right) - x\left(x^3+x\right)\Big) - x\left(x^3+x\right) \\
&= \big(1 - x(x-1)\big)\left(x^4+x+1\right) - x\big(1 - x(x-1)\big)\left(x^3+x\right) - x\left(x^3+x\right) \\
&= \big[1 - x(x-1)\big]\left(x^4+x+1\right) - \Big[x\big(1 - x(x-1)\big) - x\Big]\left(x^3+x\right)
\end{aligned}
$$

$$
\begin{aligned}
s(x) &= 1 - x(x-1) = -x^2 - x - 1 \\
t(x) &= x\big(1 - x(x-1)\big) - x = -x^3 + x^2
\end{aligned}
$$

Now, we reduce the coefficients with respect to modulo 2.

$$
\begin{aligned}
s(x) &= x^2 + x + 1 \\
t(x) &= x^3 + x^2
\end{aligned}
$$

So, we end up with:

$$
\begin{aligned}
1 \bmod \left(x^4+x+1\right) &= \left(x^2+x+1\right)\left(x^4+x+1\right) + \left(x^3+x^2\right)\left(x^3+x\right) \\
&= \Big(\left(x^2+x+1\right)\left(x^4+x+1\right) + \left(x^3+x^2\right)\left(x^3+x\right)\Big) \bmod \left(x^4+x+1\right) \\
&= 0 + \left(x^3+x^2\right)\left(x^3+x\right) \\
f(x) &= \left(x^3+x\right) \\
&= \left(x^3+x^2\right) f(x)
\end{aligned}
$$

Thus, $g(x) = x^3 + x^2$.

Defn 71 (Polynomial Basis Representation)**.** The most common representation of element of a Finite Field $\mathbb{F}_q$, where $q = p^m$, p is a Prime, and is a *polynomial basis representation.*

Theorem 4.4. *Let $f(x) \in \mathbb{Z}_p[x]$ be an Irreducible of Degree m. Then $\mathbb{Z}_p[x]/f(x)$ is a Finite Field of Set Order p^m. The elements are all Polynomials of Degree less than m. Addition and multiplication of elements is performed modulo $f(x)$.*

Lemma 4.4.1. *For each $m \geq 1$, there exists a Monic that is also an Irreducible of Degree m over $\mathbb{Z}_p$.*

5 Classical Cryptography

Defn 72 (Cryptosystem)**.** A *cryptosystem* five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where the following conditions are satisfied:

1. $\mathcal{P}$ is a finite set of possible *Plaintext*, producing a message, $\mathbf{m}$.
2. $\mathcal{C}$ is a finite set of possible *Ciphertext*
3. $\mathcal{K}$, the *Keyspace*, is a finite set of all possible keys
4. For each $K \in \mathcal{K}$, there is an *Encryption Rule* $e_K \in \mathcal{E}$ and a corresponding *Decryption Rule* $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that $d_K\left(e_K(x)\right) = x$ for every Plaintext element $x \in \mathcal{P}$.

This can be illustrated with the Shannon Model for Symmetric Encryption.

Figure 5.1: Shannon Model for Symmetric Encryption

A convention is to give the various parties in play names:

- Alice
- Bob

- Caesar
- Eve (The enemy)

Defn 73 (Plaintext)**.** *Plaintext* is the information that Alice wants to send to Bob, and is denoted $\mathcal{P}$ This information can be in any arbitrary format, we do not care, however the elements in the message are drawn from the Alphabet. However, Alice does not want Eve to be able to understand what she sends to Bob.

The message to be sent is:

$$\mathbf{m} \in \mathcal{P} = (m_1, m_2, \ldots, m_n)\, \forall m \in \mathcal{A} \tag{5.1}$$

Defn 74 (Alphabet)**.** Let $\mathcal{A}$ be a finite set, which is called the *alphabet*. We often use the English letters as the alphabet, we number them $\mathtt{a} = 0, \mathtt{b} = 1, \ldots, \mathtt{z} = 25$. This given $\mathcal{A} = \mathbb{Z}_{26}$ and $|\mathcal{A}| = 26$.

a	0.0804	j	0.0016	s	0.0654
b	0.0154	k	0.0067	t	0.0925
c	0.0306	l	0.0414	u	0.0271
d	0.0399	m	0.0253	v	0.0099
e	**0.1251**	n	0.0709	w	0.0192
f	0.0230	0	0.0760	x	0.0019
g	0.0196	p	0.0200	y	0.0173
h	0.0549	q	0.0011	z	0.0009
i	0.0726	r	0.0612		

Table 5.1: Frequency of Letters in the English Alphabet

Defn 75 (Ciphertext)**.** A *ciphertext* is a piece of Plaintext information that has been run through an element of Encryption Rule set.

A message that has been transformed with an Encryption Rule is a cipher message.

$$\mathbf{c} = e_K(\mathbf{m}) \tag{5.2}$$

Defn 76 (Keyspace)**.** *Keyspace*, denoted $\mathcal{K}$. Each *key* in the keyspace describes a certain function

$$e_K : \mathcal{P}^n \to \mathcal{C}^{n'} \tag{5.3}$$

TODO

Defn 77 (Encryption Rule)**.** The *encryption rule* is an element e_K from the set of all encryption rules, $\mathcal{E}$.

$$e_K : \mathcal{P} \to \mathcal{C} \text{ where } e_K \in \mathcal{E} \tag{5.4}$$

Namely, the encryption rule element is used to map the Plaintext pieces of information that Alice wants to send to a corresponding Ciphertext that she can send to Bob.

Remark 77.1 (Invertible)*.* Each Encryption Rule **must** be *invertible*, thus allowing decryption of the ciphertext.

Defn 78 (Decryption Rule)**.** The *decryption rule* is an element d_K from the set of all decryption rules, $\mathcal{D}$.

$$d_K : \mathcal{C} \to \mathcal{P} \text{ where } d_K \in \mathcal{D} \tag{5.5}$$

Namely, the decryption rule element is used to map the Ciphertext pieces of information that Alice sent to a corresponding Plaintext that Bob can use.

Remark 78.1.

$$pd_K(e_K(\mathbf{m})) = \mathbf{m}\ \forall\, \mathbf{m} \in \mathcal{P} \tag{5.6}$$

5.1 Types of Attacks

There are 2 main types of attacks:

1. Ciphertext-only: A ciphertext-only attack is an attack in which the enemy has access to the ciphertext $\mathcal{C}$ and tries to recover the plaintext $\mathcal{P}$ or the key K.
2. Known Plaintext: A known-plaintext attack is an attack in which the enemy has access to not only the ciphertext, $\mathcal{C}$, but may also have some or all of the $\mathcal{P}$, and is trying to recover the key K.

5.2 The Caesar Cipher

The Caesar Cipher is a Monoalphabetic Cipher in which each letter is shifted 3 steps.

This can be generalized to shift not just 3, but K positions, where $K \in \{0, 1, \ldots, 25\}$ is the secret key. In this case, the Keyspace, $\mathcal{K}$, is the set of shifts in position possible.

$$K \in \mathcal{K}, \;\; \mathcal{K} = \{0, 1, \ldots, 25\}$$

To encrypt a message, each individual character is encrypted according to Equation (5.7).

$$e_K(m) = m + k \bmod 26 \tag{5.7}$$

The Decryption Rule for The Caesar Cipher is used to decrypt a message encrypted according to Equation (5.7).

$$d_K(c) = c - k \tag{5.8}$$

5.2.1 Cryptanalysis of The Caesar Cipher

The Caesar Cipher can be broken with an *exhaustive key search*.

Example 5.1: Cryptanalysis of The Caesar Cipher. Lecture 4

Given the input string `wklvlvdphvvdjhwrbrx`, decrypt and find the message. The message was encrypted using The Caesar Cipher

K	Plaintext Equivalent
0	`wklvlvdphvvdjhwrbrx`
1	`vjkukucoguucigvqaqw`
2	`uijtjtbnfttbhfupzpv`
3	`thisisamessagetoyou`
4	`sghrhrzldrrzfdsnxnt`
5	`rfgqgqykcqqyecrmwms`
$\vdots$	$\vdots$
25	`xlmwmweqiwwekixscsy`

So, the key used in this Caesar Cipher was $K = 3$, and the message was `thisisamessagetoyou`.

5.3 The Simple Substitution Cipher

The Simple Substitution Cipher operates on the individual characters in $\mathcal{P}$. However, the key, K is now an arbitrary permutation of the characters.

The set of all permutations on $\mathbb{Z}_{26}$ is written as

$$\mathcal{E} = \{\pi_1, \pi_2, \ldots, \pi_{|\mathcal{K}|}\}$$

The keyspace, $\mathcal{K}$ for this cipher is:

$$\mathcal{K} = \{0, 1, 2, \ldots, 26! - 1\}$$
$$|\mathcal{K}| = 26!$$

The Encryption Rule for this cipher is:

$$e_K(m) = \pi_K(m) \tag{5.9}$$

The Decryption Rule for this cipher's output is:

$$d_K(c) = \pi_k^{-1}(c) \tag{5.10}$$

5.3.1 Cryptanalysis of The Simple Substitution Cipher

We could attemp to perform an exhaustive key search, but because the keyspace is all integers from 0 to $26! - 1$, which is incredibly large, it makes more sense to exploit the statistical nature of the plaintext source.

We could try matching the most common letters present in the Ciphertext against the most common letter in the Plaintext Alphabet, using Table 5.1. However, these 1-grams are only good for the most common letters in the English Alphabet.

If we take use n-grams we will have better luck, because there is a dependence between consecutive letters.

5.4 Polyalphabetic Ciphers

Polyalphabetic ciphers operate differently on different portions of the Plaintext.

The simplist Polyalphabetic Cipher is a number of Monoalphabetic Ciphers with different keys are used sequentially, the cyclically repeated. The Vigenére Cipher is one example of this kind of cipher.

5.4.1 The Vigenére Cipher

Cyclically uses t Caesar ciphers, where t is the period of the cipher.

The Encryption Rule maps the Plaintext message $\mathbf{m} = m_1, m_2, \ldots$ to the Ciphertext $\mathbf{c} = c_1, c_2, \ldots$ through

$$\mathbf{c} = e_{\mathbf{K}}(m_1, m_2, \ldots, m_t), e_{\mathbf{K}}(m_{t+1}, m_{t+2}, \ldots, m_{t+t}), \ldots \tag{5.11}$$

where

$$e_{\mathbf{K}}(m_1, m_2, \ldots, m_t) = (m_1 + k_1, m_2 + k_2, \ldots, m_t + k_t)$$

and $\mathbf{K}$ consists of t characters $\mathbf{K} = (k_1, k_2, \ldots, k_t)$.

Remark. The key, $\mathbf{K}$ is often chosen to be a word, called a keyword.

Example 5.2: Encryption Using The Vigenere Cipher. Lecture 4

The Plaintext `youmustvisitmetonight` is to be encrypted using a Vigenére Cipher, with a period 4, where $\mathbf{K}$ = `lucy`.

y	o	u	m	u	s	t	v	i	s	i	t	m	e	t	o	⋯
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	⋯
l	u	c	y	l	u	c	y	l	u	c	y	l	u	c	y	⋯
j	i	w	k	f	m	v	t	t	m	k	r	x	y	v	m	⋯

The resulting Ciphertext is `jiwkfmvttmkrxyvm`.

5.4.1.1 Cryptanalysis of The Vigenére Cipher

There are 2 steps to breaking The Vigenére Cipher:

1. Determine the period of the cipher, t. Generally, Kasiski's Method is used.
2. Reconstruct the t different The Simple Substitution Cipher Alphabets used.

Defn 79 (Kasiski's Method)**.** *Kasiski's Method* relies on the observation that repeated portions of Plaintext input will yield a repeating Ciphertext output, with some cyclic distance, t between each occurrence. This distance will be a multiple of the keyword length.

To solve this, you calculate the Greatest Common Divisor of these distances.

Now we move onto the second part of breaking The Vigenére Cipher. There are 2 main ways to do this.

1. Split the Ciphertext characters into t different multisets, where each character should have been shifted according to a Simple Substitution Cipher. The key of each Monoalphabetic Cipher can be determined with the statistics in Table 5.1 and some trial-and-error.
2. Measure of Roughness and Index of Coincidence

Defn 80 (Measure of Roughness)**.**

$$\begin{aligned} \mathrm{MR} &= \sum_{i=a\Rightarrow 1}^{z\Rightarrow 26} \left(p_i - \frac{1}{26}\right)^2 \\ &= \sum_{i=a\Rightarrow 1}^{z\Rightarrow 26} (p_i)^2 - \frac{1}{26} \end{aligned} \tag{5.12}$$

Defn 81 (Index of Coincidence)**.** The *index of coincidence* uses values found in the Measure of Roughness.

$$\mathrm{IC} = \frac{\sum_{i=a\Rightarrow 1}^{z\Rightarrow 26} f_i\,(f_1 - 1)}{n(n-1)} \tag{5.13}$$

However, it does *not* return the period of The Vigenére Cipher.

5.4.2 The Vernam Cipher (One-Time Pad)

This is a special case of the The Vigenére Cipher, where the period of the key, **K** is chosen to be the same length as the output ciphertext, **C**. More concretely, for a ciphertext, **C** of length n, pick a Vigenére Cipher key with a period t. Where,

$$n = t$$

5.4.2.1 Cryptanalysis of The Vernam Cipher (One-Time Pad) The Vernam Cipher (One-Time Pad) is an example of Perfect Secrecy (unbreakable) if the the elements of the key **K** are chosen uniformly at random among all possible $\mathbb{Z}_{26}^{n}$ possible values.

5.4.3 Transposition Cipher (Permutation Cipher)

This cipher reorders all the letters in a block of length t. The Encryption Rule's key, K that permutes all the characters in a word block. Equation (5.14) is an example of how the Encryption Rule is constructed.

$$\begin{aligned} \pi_e(2,5,1,3,4) \Longrightarrow \pi(1) &= 2 \\ \pi(2) &= 5 \\ \pi(3) &= 1 \\ \pi(4) &= 3 \\ \pi(5) &= 4 \end{aligned} \tag{5.14}$$

The Decryption Rule for Equation (5.14) is given in Equation (5.15).

$$\begin{aligned} \pi_d(4,3,1,5,2) \Longrightarrow \pi(1) &= 4 \\ \pi(2) &= 3 \\ \pi(3) &= 1 \\ \pi(4) &= 5 \\ \pi(5) &= 2 \end{aligned} \tag{5.15}$$

Remark 81.1. The number on the **right-hand side** is assigned to the position present on the **left-hand side**.

Example 5.3: Transposition Cipher. Lecture 5

Given the plaintext message **M** = findi, and the Encryption Rule shown in Equation (5.14), what is the resulting ciphertext message?

$$\begin{aligned} \pi(1) &= 2 \\ \pi(2) &= 5 \\ \pi(3) &= 1 \\ \pi(4) &= 3 \\ \pi(5) &= 4 \end{aligned}$$

So, each character in the input "findi" is moved around to result in "iifnd".

5.4.4 The Hill Cipher

The Hill Cipher acts on t-grams from $\mathbb{Z}_{26}$ through a key that is an Invertible $t \times t$ matrix.

6 Information Theory

7 Shannon's Theory of Secrecy

Defn 82 (Perfect Secrecy)**.** A cryptosystem hsa *perfect secrecy* if Equation (7.1) is true.

$$\mathrm{I}(M;C) = 0 = H(M) - H(M \mid C) \tag{7.1}$$

A Complex Numbers

Complex numbers are numbers that have both a real part and an imaginary part.

$$z = a \pm bi \tag{A.1}$$

where

$$i = \sqrt{-1} \tag{A.2}$$

Remark (i vs. j for Imaginary Numbers). Complex numbers are generally denoted with either i or j. Since this is an appendix section, I will denote complex numbers with i, to make it more general. However, electrical engineering regularly makes use of j as the imaginary value. This is because alternating current i is already taken, so j is used as the imaginary value instad.

$$Ae^{-ix} = A\left[\cos\left(x\right) + i\sin\left(x\right)\right] \tag{A.3}$$

A.1 Complex Conjugates

If we have a complex number as shown below,

$$z = a \pm bi$$

then, the conjugate is denoted and calculated as shown below.

$$\overline{z} = a \mp bi \tag{A.4}$$

Defn A.1.1 (Complex Conjugate)**.** The conjugate of a complex number is called its *complex conjugate*. The complex conjugate of a complex number is the number with an equal real part and an imaginary part equal in magnitude but opposite in sign.

The complex conjugate can also be denoted with an asterisk ($*$). This is generally done for complex functions, rather than single variables.

$$z^* = \overline{z} \tag{A.5}$$

A.1.1 Complex Conjugates of Exponentials

$$\overline{e^z} = e^{\overline{z}} \tag{A.6}$$

$$\overline{\log(z)} = \log(\overline{z}) \tag{A.7}$$

A.1.2 Complex Conjugates of Sinusoids

Since sinusoids can be represented by complex exponentials, as shown in Appendix B.2, we could calculate their complex conjugate.

$$\begin{aligned} \overline{\cos(x)} &= \cos(x) \\ &= \frac{1}{2}\left(e^{ix} + e^{-ix}\right) \end{aligned} \tag{A.8}$$

$$\begin{aligned} \overline{\sin(x)} &= \sin(x) \\ &= \frac{1}{2i}\left(e^{ix} - e^{-ix}\right) \end{aligned} \tag{A.9}$$

B Trigonometry

B.1 Trigonometric Formulas

$$\sin(\alpha) + \sin(\beta) = 2\sin\left(\frac{\alpha+\beta}{2}\right)\cos\left(\frac{\alpha-\beta}{2}\right) \tag{B.1}$$

$$\cos(\theta)\sin(\theta) = \frac{1}{2}\sin(2\theta) \tag{B.2}$$

B.2 Euler Equivalents of Trigonometric Functions

$$e^{\pm j\alpha} = \cos(\alpha) \pm j\sin(\alpha) \tag{B.3}$$

$$\cos(x) = \frac{e^{jx} + e^{-jx}}{2} \tag{B.4}$$

$$\sin(x) = \frac{e^{jx} - e^{-jx}}{2j} \tag{B.5}$$

$$\sinh(x) = \frac{e^{x} - e^{-x}}{2} \tag{B.6}$$

$$\cosh(x) = \frac{e^{x} + e^{-x}}{2} \tag{B.7}$$

B.3 Angle Sum and Difference Identities

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta) \tag{B.8}$$

$$\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta) \tag{B.9}$$

B.4 Double-Angle Formulae

$$\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha) \tag{B.10}$$

$$\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha) \tag{B.11}$$

B.5 Half-Angle Formulae

$$\sin\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1-\cos(\alpha)}{2}} \tag{B.12}$$

$$\cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1+\cos(\alpha)}{2}} \tag{B.13}$$

B.6 Exponent Reduction Formulae

$$\sin^2(\alpha) = \frac{1-\cos(2\alpha)}{2} \tag{B.14}$$

$$\cos^2(\alpha) = \frac{1+\cos(2\alpha)}{2} \tag{B.15}$$

B.7 Product-to-Sum Identities

$$2\cos(\alpha)\cos(\beta) = \cos(\alpha-\beta) + \cos(\alpha+\beta) \tag{B.16}$$

$$2\sin(\alpha)\sin(\beta) = \cos(\alpha-\beta) - \cos(\alpha+\beta) \tag{B.17}$$

$$2\sin(\alpha)\cos(\beta) = \sin(\alpha+\beta) + \sin(\alpha-\beta) \tag{B.18}$$

$$2\cos(\alpha)\sin(\beta) = \sin(\alpha+\beta) - \sin(\alpha-\beta) \tag{B.19}$$

B.8 Sum-to-Product Identities

$$\sin(\alpha) \pm \sin(\beta) = 2\sin\left(\frac{\alpha \pm \beta}{2}\right)\cos\left(\frac{\alpha \mp \beta}{2}\right) \tag{B.20}$$

$$\cos(\alpha) + \cos(\beta) = 2\cos\left(\frac{\alpha + \beta}{2}\right)\cos\left(\frac{\alpha - \beta}{2}\right) \tag{B.21}$$

$$\cos(\alpha) - \cos(\beta) = -2\sin\left(\frac{\alpha + \beta}{2}\right)\sin\left(\frac{\alpha - \beta}{2}\right) \tag{B.22}$$

B.9 Pythagorean Theorem for Trig

$$\cos^2(\alpha) + \sin^2(\alpha) = 1^2 \tag{B.23}$$

B.10 Rectangular to Polar

$$a + jb = \sqrt{a^2 + b^2}e^{j\theta} = re^{j\theta} \tag{B.24}$$

$$\theta = \begin{cases} \arctan\left(\frac{b}{a}\right) & a > 0 \\ \pi - \arctan\left(\frac{b}{a}\right) & a < 0 \end{cases} \tag{B.25}$$

B.11 Polar to Rectangular

$$re^{j\theta} = r\cos(\theta) + jr\sin(\theta) \tag{B.26}$$

C Calculus

C.1 Fundamental Theorems of Calculus

Defn C.1.1 (First Fundamental Theorem of Calculus)**.** The *first fundamental theorem of calculus* states that, if f is continuous on the closed interval $[a, b]$ and F is the indefinite integral of f on $[a, b]$, then

$$\int_a^b f(x)\,dx = F(b) - F(a) \tag{C.1}$$

Defn C.1.2 (Second Fundamental Theorem of Calculus)**.** The *second fundamental theorem of calculus* holds for f a continuous function on an open interval I and a any point in I, and states that if F is defined by

$$F(x) = \int_a^x f(t)\,dt,$$

then

$$\begin{aligned} \frac{d}{dx}\int_a^x f(t)\,dt &= f(x) \\ F'(x) &= f(x) \end{aligned} \tag{C.2}$$

Defn C.1.3 (argmax)**.** The arguments to the *argmax* function are to be maximized by using their derivatives. You must take the derivative of the function, find critical points, then determine if that critical point is a global maxima. This is denoted as

$$\operatorname*{argmax}_x$$

C.2 Rules of Calculus

C.2.1 Chain Rule

Defn C.2.1 (Chain Rule)**.** The *chain rule* is a way to differentiate a function that has 2 functions multiplied together.

If

$$f(x) = g(x) \cdot h(x)$$

then,

$$\begin{aligned} f'(x) &= g'(x) \cdot h(x) + g(x) \cdot h'(x) \\ \frac{df(x)}{dx} &= \frac{dg(x)}{dx} \cdot g(x) + g(x) \cdot \frac{dh(x)}{dx} \end{aligned} \tag{C.3}$$

D Laplace Transform

Defn D.0.1 (Laplace Transform)**.** The *Laplace transformation* operation is denoted as $\mathcal{L}\{x(t)\}$ and is defined as

$$X(s) = \int_{-\infty}^{\infty} x(t) e^{-st} dt \tag{D.1}$$