EDIN01: Cryptography - Reference Sheet

Karl Hallsby

Last Edited: November 8, 2019

Contents

1 Cryptography Introduction

Defn 1 (Cryptographic Primitive)**.** A *cryptographic primitive* is an algorithm with basic cryptographic properties.

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

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 3 (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 4 (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 5 (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:

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

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

2 Number Theory

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

Defn 7 (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 8 (Divides)**.** For $a, b \in \mathbb{Z}$, we say that a *divides* b (written $a \mid b$) if there exists an integer c such that $b = ac$.

Properties:

(i) $a \mid a$
(ii) If $a \mid b$ and $b \mid c$, then $a \mid c$.
(iii) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.
(iv) If $a \mid b$ and $b \mid a$, 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 9 (Quotient)**.** The *quotient*, q, of a divided by b is denoted $a \operatorname{div} b$.

Defn 10 (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 $a \bmod b$?

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

2.2 Greatest Common Divisor

Defn 11 (Common Divisor)**.** An integer c is a *common divisor* of a and b if $c \mid a$ and $c \mid b$.

Defn 12 (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 12.1. If $a, b \in \mathbb{Z}^+$, then $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$

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 13 (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

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

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

Remark 13.1. If $a, b \in \mathbb{Z}^+$, then $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$

2.4 Primality

Defn 14 (Relatively Prime)**.** a, b are called *relatively prime* if $\gcd(a, b) = 1$.

Defn 15 (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 16 (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 17 (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 17.1. 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 18 (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 19 (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 20 (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 21 (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 21.1. 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 22 ($\mathbb{Z}_n$)**.** 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 23 (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 24 (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 25 (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 26 (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 27 (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 27.1. 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 28 (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 29 (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 29.1 (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 30 (Element Order)**.** The *order of an element* $a \in \mathbb{Z}_n^*$, denoted 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*$(a) \,|\, s$*. In particular, ord*$(a) \,|\, \phi(n)$ *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 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 ord$(a) \,|\, s$. ■

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

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

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

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

Remark 31.1. 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 $\text{ord}(a) = \phi(n)$. 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

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

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 $\text{ord}\, a = 4$, $a \in \mathbb{Z}_8^*$.

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

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

3.8 Quadratic Residues

Defn 32 (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 32.1 (Square Root). If $x^2 = a$, then x is called the *square root* of $a \bmod n$.

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

Defn 33 (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 34 (Binary Operation)**.** A *binary operation*, denoted $*$ on a set S, is a mapping from $S * S$ to S.

Remark 34.1. Note that $*$ is **NOT** multiplication nor any kind of convolution. It is just a placeholder for some Binary Operation that can be done.

Defn 35 (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 **TODO, Finish**

Defn 36 (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 37 (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?

Defn 38 (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 39 (Element Order)**.** The *order of an element* a, denoted $\text{ord}(a)$ 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 39.1. **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 39.1, 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 $\text{ord}\big[(1, 1, 1)\big] = 2$.

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 40 (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 $ElementOrder(a) \mid n$.

1. Write $n = k \cdot \text{ord}(a) + r$, where $0 \leq r \leq \text{ord}(a)$.
2. Then, $1 = a^n = a^{k \cdot \text{ord}(a) + r} = a^r$ 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 41 (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 41.1 (Ring Multiplicative Inverses). Note that we haven't said anything about multiplicative inverses yet.

Defn 42 (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 42.1. 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 42.2 (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 43 (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.

Defn 44 (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 45 (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 46 (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 46.1 (Extension Field). Likewise, we say E is an *extension field* of F.

Defn 47 (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 48 (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 $a_i inR$, $a_n neq 0$, and $n \geq 0$.

Remark 48.1. **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 49 (Degree)**.** We say that $f(x)$ has *degree* n, denoted

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

Remark 49.1. 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 50 (Monic)**.** A Polynomial is said to be *monic* if the leading coefficient is equal to 1.

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

Defn 51 (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 52 (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 52.1 (Relation Between Irreducible Polynomials and Prime Numbers)*.* Irreducible polynomials are the Polynomial Ring counterpart of Prime numbers.

4.5.1 Long Division of Polynomials

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

Defn 53 (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 54 (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 55 (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 4.7: Long Division of Polynomials. Lecture 3

TODO

4.5.2 Properties of Polynomial Rings

Defn 56 (Divide)**.** If $g(x), h(x) \in F[x]$, then $h(x)$ is said to *divide* $g(x)$, written

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

Defn 57 (Congruent)**.** Let $g(x), h(x) \in F[x]$. Then, $g(x)$ is said to be *congruent* to $h(x) \bmod f(x)$ 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 58 (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 $\mod f(x)$.

Defn 59 (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 60 (Commutative Ring)**.** A commutative Ring for Polynomials is defined as

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

Remark 60.1. Note that this is the inverse condition of when a Polynomial Ring is a Field.

Defn 61 (Field)**.** If $f(x) \in F[x]$ is Irreducible, then $F[x]/f(x)$ is a Field.

Remark 61.1. Note that this is the inverse condition of when a Polynomial Ring is a Commutative Ring

Defn 62 (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 $GF(p^m)$.
(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 63 (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 64 (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 65 (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 65.1. 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 66 (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 4.8

Example 4.8: Polynomial Euclidean Algorithm. Lecture 3
TODO

Defn 67 (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 4.9

Example 4.9: Polynomial Extended Euclidean Algorithm. Lecture 3
TODO

Defn 68 (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 69 (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*
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 $x \in \mathcal{P}$.

Defn 70 (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, Alice does not want Oscar to be able to understand what she sends to Bob.

Defn 71 (Ciphertext)**.** A *ciphertext* is a piece of Plaintext information that has been run through an element of Encryption Rule set.

Defn 72 (Keyspace)**.** *Keyspace*, denoted $\mathcal{K}$. **TODO**

Defn 73 (Encryption Rule)**.** The *encryption rule* is an element e_K from the set of all encryption rules, $\mathcal{E}$.

$$e_K : \mathcal{P} \to \mathcal{C} \text{ where } e_K \in \mathcal{E} \tag{5.1}$$

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.

Defn 74 (Decryption Rule)**.** The *decryption rule* is an element d_K from the set of all decryption rules, $\mathcal{D}$.

$$d_K : \mathcal{C} \to \mathcal{P} \text{ where } d_K \in \mathcal{D} \tag{5.2}$$

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.

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

$$\underset{x}{\operatorname{argmax}}$$

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

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