Cryptography and Embedded System Security
CRAESS_I

Xiaolu Hou

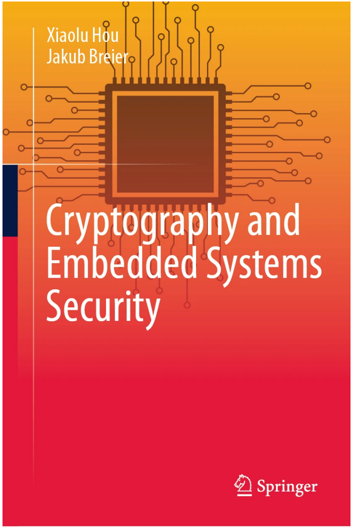
FIIT, STU
xiaolu.hou @ stuba.sk

Course Outline

- Abstract algebra and number theory
- Introduction to cryptography
- Symmetric block ciphers and their implementations
- RSA, RSA signatures, and their implementations
- Probability theory and introduction to SCA
- SPA and non-profiled DPA
- Profiled DPA
- SCA countermeasures
- FA on RSA and countermeasures
- FA on symmetric block ciphers
- FA countermeasures for symmetric block cipher
- Practical aspects of physical attacks
    - Invited speaker: Dr. Jakub Breier, Senior security manager, TTControl GmbH

Recommended reading

- Textbook
  - Sections 1.1 – 1.5



Lecture Outline

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Set theory

- $\emptyset$: empty set
- $|S|$: cardinality of S
- $a \in S$: a is an element in set S
- $a \notin S$: a is not an element in set S
- $S \subseteq T$: if $s \in S$, then $s \in T$, S is a subset of T
- $S = T$: $S \subseteq T$ and $T \subseteq S$
- The *power set* of a set S, denoted by 2^S, is the set of all subsets of S.

Example

Let $T = \{ 0, 1, 2, 3 \}$ and $S = \{ 2, 3 \}$, then

- $S \ ? \ T$ and $T \ ? \ S$.
- $2 \ ? \ S$, $0 \ ? \ S$.
- $|S| =?$, $|T| =?$.
- $2^S =?$.

Set theory

- $\emptyset$: empty set
- $|S|$: cardinality of S
- $a \in S$: a is an element in set S
- $a \notin S$: a is not an element in set S
- $S \subseteq T$: if $s \in S$, then $s \in T$, S is a subset of T
- $S = T$: $S \subseteq T$ and $T \subseteq S$
- The *power set* of a set S, denoted by 2^S, is the set of all subsets of S.

Example

Let $T = \{ 0, 1, 2, 3 \}$ and $S = \{ 2, 3 \}$, then

- $S \subseteq T$ and $T \nsubseteq S$.
- $2 \in S$, $0 \notin S$.
- $|S| = 2$, $|T| = 4$.
- $2^S = \{ \emptyset, S, \{ 2 \}, \{ 3 \} \}$.

Set theory

- Union: $A \cup B$
- Intersection: $A \cap B$
- Difference: $A - B = \{ a \in A, a \notin B \}$
- Complement of A in S: $A^c = S - A$
- Cartesian product $A \times B = \{ (a, b) \mid a \in A, b \in B \}$
  - ordered pairs

Example

- $A = \{ 0, 1, 2 \}$, $B = \{ 2, 3, 4 \}$
- $A \cup B = \{ 0, 1, 2, 3, 4 \}$, $A \cap B = \{ 2 \}$

Example

- $A = \{ 2, 4, 6 \}$, $B = \{ 1, 3, 5 \}$, $S = A \cup B$
- $A - B =?$ Complement of A in S is ?

$$A \times B =?$$

Set theory

- Union: $A \cup B$
- Intersection: $A \cap B$
- Difference: $A - B = \{ a \in A, a \notin B \}$
- Complement of A in S: $A^c = S - A$
- Cartesian product $A \times B = \{ (a, b) \mid a \in A, b \in B \}$
  - ordered pairs

Example

- $A = \{ 0, 1, 2 \}$, $B = \{ 2, 3, 4 \}$
- $A \cup B = \{ 0, 1, 2, 3, 4 \}$, $A \cap B = \{ 2 \}$

Example

- $A = \{ 2, 4, 6 \}$, $B = \{ 1, 3, 5 \}$, $S = A \cup B$
- $A - B = A$. Complement of A in S is B

$$A \times B = \{ (2, 1), (2, 3), (2, 5), (4, 1), (4, 3), (4, 5), (6, 1), (6, 3), (6, 5) \} .$$

Functions

Definition

A *function/map* $f : S \to T$ is a rule that assigns each element $s \in S$ a **unique** element $t \in T$.

- S – *domain* of f; T – *codomain* of f.
- If $f(s) = t$, then t is called the *image* of s, s is a *preimage* of t.
- For any $A \subseteq T$, *preimage of A under f* is

$$f^{-1}(A) := \{\, s \in S \mid f(s) \in A \,\}$$

Example

Define

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

where $\mathbb{R}$ is the set of real numbers. Then f has domain $\mathbb{R}$ and codomain $\mathbb{R}$.

Functions

Example

Define

$$f : \mathbb{R} \rightarrow \mathbb{R}$$
$$x \mapsto x^2$$

where $\mathbb{R}$ is the set of real numbers. Then f has domain $\mathbb{R}$ and codomain $\mathbb{R}$.
Let $A = \{ 1 \} \subseteq \mathbb{R}$, the preimage of A under f is given by

$$f^{-1}(A) = ?$$

Let $B = \{ -1 \} \subseteq \mathbb{R}$, then $f^{-1}(B) = ?$

Functions – Example

Example

Define

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

where $\mathbb{R}$ is the set of real numbers. Then f has domain $\mathbb{R}$ and codomain $\mathbb{R}$.
Let $A = \{ 1 \} \subseteq \mathbb{R}$, the preimage of A under f is given by

$$f^{-1}(A) = \{ -1, 1 \} .$$

1 is the image of -1 and -1 is a preimage of 1. 1 is another preimage of 1.
Let $B = \{ -1 \} \subseteq \mathbb{R}$, then $f^{-1}(B) = \emptyset$.

Functions

Definition

- A function $f : S \to T$ is called *onto* or *surjective* if given any $t \in T$, there exists $s \in S$, such that $t = f(s)$.
- A function $f : S \to T$ is said to be *one-to-one* (written 1-1) or *injective* if for any $s_1, s_2 \in S$ such that $s_1 \neq s_2$, we have $f(s_1) \neq f(s_2)$.
- f is called *1-1 correspondence* or *bijective* if f is 1-1 and onto.

Example

f is ?, g is ?

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto x^2 \end{aligned}$$

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x \end{aligned}$$

Functions

Example

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto x^2, \end{aligned}$$

f is surjective as for any $y \in \mathbb{R}_{\geq 0}$, we can find a preimage of y by calculating $x = \sqrt{y}$.
But f is not injective, since $f(-1) = f(1) = 1$.

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x. \end{aligned}$$

It can be easily seen that g is bijective.

Inverse of a function

- When f is bijective, $f^{-1} : T \to S$ is a function – it assigns each $t \in T$ a unique element $s \in S$.
- f^{-1} is called the *inverse* of f.

Example

Define f

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3. \end{aligned}$$

Then, the inverse of f is ?

Inverse of a function

- When f is bijective, $f^{-1}: T \to S$ is a function – it assigns each $t \in T$ a unique element $s \in S$.
- f^{-1} is called the *inverse* of f.

Example

Define f

$$\begin{aligned} f: \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3. \end{aligned}$$

Then, the inverse of f exists and is given by

$$\begin{aligned} f^{-1}: \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sqrt[3]{x}. \end{aligned}$$

Composition of functions

Definition

For two functions $f : T \to U$, $g : S \to T$, the *composition* of f and g, denoted by $f \circ g$, is the function

$$\begin{aligned} f \circ g : S &\to U \\ s &\mapsto f(g(s)). \end{aligned}$$

Example

What is $f \circ g$?

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2, \end{aligned}$$

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3. \end{aligned}$$

Composition of functions

Example

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2, \end{aligned}$$

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3. \end{aligned}$$

$$\begin{aligned} f \circ g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto (x^3)^2 = x^6. \end{aligned}$$

Composition of functions

Remark

- $f : S \to S$
- We write $f \circ f \circ \cdots \circ f$ as f^n
- If f is bijective, we write $f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}$ as f^{-m}

Example

Define

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2, \end{aligned}$$

then what is f^n?

Composition of functions

Remark

- $f : S \to S$
- We write $f \circ f \circ \cdots \circ f$ as f^n
- If f is bijective, we write $f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}$ as f^{-m}

Example

Define

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2, \end{aligned}$$

then

$$\begin{aligned} f^n : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^{2^n}. \end{aligned}$$

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Representation of a positive integer

- We write one hundred and twenty-three as 123 because

$$123 = 1 \times 100 + 2 \times 10 + 3 \times 1.$$

Theorem

Let $b \geq 2$ be an integer. Then any $n \in \mathbb{Z}$, $n > 0$ can be expressed uniquely in the form

$$n = \sum_{i=0}^{\ell-1} a_i b^i,$$

where $0 \leq a_i < b$ $(0 \leq i < \ell)$, $a_{\ell-1} \neq 0$, and $\ell \geq 1$. $a_{\ell-1}a_{\ell-2}\ldots a_1a_0$ is called a base$-b$ representation for n. ℓ is called the length of n in base$-b$ representation.

- $b = 2$, binary representation

Representation of a positive integer

Example

$$3_{10} = ?_2 = ?_{16}.$$
$$4_{10} = ?_2 = ?_{16}.$$
$$60_{10} = ?_2 = ?_{16}.$$

Base 10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Base 16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Table: Correspondence between decimal and hexadecimal (base $b = 16$) numerals.

Representation of a positive integer

Example

$$3_{10} = 11_2 = \texttt{3}_{16}.$$
$$4_{10} = 100_2 = \texttt{4}_{16}.$$
$$60_{10} = 111100_2 = \texttt{3C}_{16}.$$

Base 10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Base 16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Table: Correspondence between decimal and hexadecimal (base $b = 16$) numerals.

Divisor and multiple

Theorem

If $m, n \in \mathbb{Z}$, $n > 0$, *then* $\exists q, r \in \mathbb{Z}$, *such that* $0 \leq r < n$ *and* $n = qm + r$.

q is called the *quotient* and r is called the *remainder*.

Definition

Given $m, n \in \mathbb{Z}$, if $m \neq 0$ and $n = am$ for some integer a, we say that m *divides* n, written $m|n$. We call m a *divisor* of n and n a *multiple* of m. If m does not divide n, we write $m \nmid n$.

Example

- $3|6$, $-2|4$, $1|8$, $5|5$.
- $7 \nmid 9$, $4 \nmid 6$.
- All the positive divisors of 4 are $1, 2, 4$.
- All the positive divisors of 6 are $1, 2, 3, 6$.

Greatest common divisor

Definition

Take $m, n \in \mathbb{Z}$, $m \neq 0$ or $n \neq 0$, the *greatest common divisor* of m and n, denoted $\gcd(m, n)$, is given by $d \in \mathbb{Z}$ such that

- $d > 0$,
- $d|m$, $d|n$, and
- if $c|m$ and $c|n$, then $c|d$.

Example

- We have discussed that all positive divisors of 4 and 6 are $1, 2, 4$ and $1, 2, 3, 6$ respectively. So $\gcd(4, 6) = 2$.
- All the positive divisors of 2 are 1 and 2. All the positive divisors of 3 are 1 and 3. So $\gcd(2, 3) = 1$.

Bézout's identity

Theorem (Bézout's identity)

For any $m, n \in \mathbb{Z}$*, such that* $m \neq 0$ *or* $n \neq 0$*.* $\gcd(m, n)$ *exists and is unique.*
Moreover, $\exists s, t \in \mathbb{Z}$ *such that* $\gcd(m, n) = sm + tn$*.*

Example

$$\begin{aligned} \gcd(4,6) &= 2 = ?\times 4 + ?\times 6. \\ \gcd(2,3) &= 1 = ?\times 2 + ?\times 3. \end{aligned}$$

Bézout's identity

Theorem (Bézout's identity)

For any $m, n \in \mathbb{Z}$*, such that* $m \neq 0$ *or* $n \neq 0$*.* $\gcd(m, n)$ *exists and is unique.*
Moreover, $\exists s, t \in \mathbb{Z}$ *such that* $\gcd(m, n) = sm + tn$*.*

Example

$$\begin{aligned} \gcd(4,6) &= 2 = (-1) \times 4 + 1 \times 6. \\ \gcd(2,3) &= 1 = (-4) \times 2 + 3 \times 3. \end{aligned}$$

Euclidean algorithm

Theorem (Euclid's division)

Given $m, n \in \mathbb{Z}$*, take* q, r *such that* $n = qm + r$*, then* $\gcd(m, n) = \gcd(m, r)$*.*

Thus, to find $\gcd(m, n)$, we can compute Euclid's division repeatedly until we get $r = 0$.

Example

We can calculate $\gcd(120, 35)$ as follows:

$$\begin{aligned} 120 &= 35 \times 3 + 15 \quad & \gcd(120, 35) &= \gcd(35, 15), \\ 35 &= 15 \times 2 + 5 \quad & \gcd(35, 15) &= ? \end{aligned}$$

Euclidean algorithm

Theorem (Euclid's division)

Given $m, n \in \mathbb{Z}$, *take* q, r *such that* $n = qm + r$, *then* $\gcd(m,n) = \gcd(m,r)$.

Thus, to find $\gcd(m,n)$, we can compute Euclid's division repeatedly until we get $r = 0$.

Example

We can calculate $\gcd(120, 35)$ as follows:

$$\begin{aligned} 120 &= 35 \times 3 + 15 && \gcd(120,35) = \gcd(35,15), \\ 35 &= 15 \times 2 + 5 && \gcd(35,15) = \gcd(15,5), \\ 15 &= 5 \times 3 && \gcd(15,5) = 5 \implies \gcd(120,35) = 5. \end{aligned}$$

Example

Find $\gcd(160, 21)$

Euclidean algorithm

Example

We can calculate $\gcd(160, 21)$ using the Euclidean algorithm

$$
\begin{aligned}
160 &= 21 \times 7 + 13 && \gcd(160, 21) = \gcd(21, 13), \\
21 &= 13 \times 1 + 8 && \gcd(21, 13) = \gcd(13, 8), \\
13 &= 8 \times 1 + 5 && \gcd(13, 8) = \gcd(8, 5), \\
8 &= 5 \times 1 + 3 && \gcd(8, 5) = \gcd(5, 3), \\
5 &= 3 \times 1 + 2 && \gcd(5, 3) = \gcd(3, 2), \\
3 &= 2 \times 1 + 1 && \gcd(3, 2) = \gcd(2, 1), \\
2 &= 1 \times 2 && \gcd(2, 1) = 1 \Longrightarrow \gcd(160, 21) = 1
\end{aligned}
$$

Euclidean Algorithm

Algorithm 1: Euclidean algorithm.

Input: m, n// $m, n \in \mathbb{Z}$, $m \neq 0$

Output: $\gcd(m, n)$

```
while m ≠ 0 do
    r = m
    m = n%m// remainder of n divided by m
    n = r
return n
```

Extended Euclidean algorithm

Note

With the intermediate results we have from the Euclidean algorithm, we can also find s, t such that $\gcd(m, n) = sm + tn$ (Bézout's identity).

Example

We have calculated $\gcd(120, 35)$ as follows:

$$\begin{aligned} &120 = 35 \times 3 + 15 && \gcd(120, 35) = \gcd(35, 15), \\ &35 = 15 \times 2 + 5 && \gcd(35, 15) = \gcd(15, 5), \\ &15 = 5 \times 3 && \gcd(15, 5) = 5 \implies \gcd(120, 35) = 5. \end{aligned}$$

Then

$$\begin{aligned} &5 = 35 - 15 \times 2, \\ &15 = 120 - 35 \times 3, \\ &5 = 35 - (120 - 35 \times 3) \times 2 = 120 \times (-2) + 35 \times 7. \end{aligned}$$

Extended Euclidean algorithm

Example

We have calculated $\gcd(160, 21)$ using the Euclidean algorithm

$$\begin{aligned}
160 &= 21 \times 7 + 13 & \gcd(160, 21) &= \gcd(21, 13), \\
21 &= 13 \times 1 + 8 & \gcd(21, 13) &= \gcd(13, 8), \\
13 &= 8 \times 1 + 5 & \gcd(13, 8) &= \gcd(8, 5), \\
8 &= 5 \times 1 + 3 & \gcd(8, 5) &= \gcd(5, 3), \\
5 &= 3 \times 1 + 2 & \gcd(5, 3) &= \gcd(3, 2), \\
3 &= 2 \times 1 + 1 & \gcd(3, 2) &= \gcd(2, 1), \\
2 &= 1 \times 2 & \gcd(2, 1) &= 1 \implies \gcd(160, 21) = 1
\end{aligned}$$

Using the extended Euclidean algorithm, find integers s, t such that $\gcd(160, 21) = s160 + t35$

Extended Euclidean algorithm

Example

By the extended Euclidean algorithm,

$$\begin{aligned} 1 &= 3 - 2, & 2 &= 5 - 3, \\ 3 &= 8 - 5, & 5 &= 13 - 8, \\ 8 &= 21 - 13, & 13 &= 160 - 21 \times 7. \end{aligned}$$

We have

$$\begin{aligned} 1 &= 3 - (5 - 3) = 3 \times 2 - 5 = 8 \times 2 - 5 \times 3 = 8 \times 2 - (13 - 8) \times 3 \\ &= 8 \times 5 - 13 \times 3 = 21 \times 5 - 13 \times 8 = 21 \times 5 - (160 - 21 \times 7) \times 8 \\ &= (-8) \times 160 + 61 \times 21. \end{aligned}$$

Prime numbers

Definition

- For $m, n \in \mathbb{Z}$ such that $m \neq 0$ or $n \neq 0$, m and n are said to be *relatively prime/coprime* if $\gcd(m, n) = 1$.
- Given $p \in \mathbb{Z}$. p is said to be *prime* (or a *prime number*) if for any $m \in \mathbb{Z}$, either m is a multiple of p (i.e. $p|m$) or m and p are coprime (i.e. $\gcd(p, m) = 1$).

Example

- 4 and 9 are relatively prime.
- 8 and 6 are not coprime.
- $2, 3, 5, 7$ are prime numbers.
- $6, 9, 21$ are not prime numbers.

Prime factorization

Theorem (The Fundamental Theorem of Arithmetic)

For any $n \in \mathbb{Z}$, $n > 1$, n can be written in the form

$$n = \prod_{i=1}^{k} p_i^{e_i},$$

where the exponents e_i are positive integers, $p_1, p_2, \ldots, p_k$ are prime numbers that are pairwise distinct and unique up to permutation.

Example

$20 = 2^2 \times 5$, $135 = 3^3 \times 5$.

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Definition

Definition

A *group* $(G, \cdot)$ is a non-empty set G with a binary operation $\cdot$ satisfying the following conditions:

- G is closed under $\cdot$ (closure property), $\forall g_1, g_2 \in G$, $g_1 \cdot g_2 \in G$.
- $\cdot$ is associative, $\forall g_1, g_2, g_3 \in G$, $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$.
- $\exists e \in G$, an identity element, such that $\forall g \in G$, $e \cdot g = g \cdot e = g$.
- Every $g \in G$ has an inverse $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Example

- $(\mathbb{Z}, +)$, the set of integers with addition is a group. The identity element is ?.
- Similarly, $(\mathbb{Q}, +)$ and $(\mathbb{C}, +)$ are groups.
- Is $(\mathbb{Q}, \times)$ a group?
- How about $(\mathbb{Q} \backslash \{ 0 \}, \times)$?

Definition

Definition

A *group* $(G, \cdot)$ is a non-empty set G with a binary operation $\cdot$ satisfying the following conditions:

- G is closed under $\cdot$ (closure property), $\forall g_1, g_2 \in G$, $g_1 \cdot g_2 \in G$.
- $\cdot$ is associative, $\forall g_1, g_2, g_3 \in G$, $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$.
- $\exists e \in G$, an identity element, such that $\forall g \in G$, $e \cdot g = g \cdot e = g$.
- Every $g \in G$ has an inverse $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Example

- $(\mathbb{Z}, +)$, the set of integers with addition is a group. The identity element is 0.
- Similarly, $(\mathbb{Q}, +)$ and $(\mathbb{C}, +)$ are groups.
- $(\mathbb{Q}, \times)$ is not a group. Because $0 \in \mathbb{Q}$ does not have an inverse with respect to multiplication.
- But $(\mathbb{Q} \setminus \{ 0 \}, \times)$ is a group. The identity element is 1.

Prove a set with a binary operation is a group

Let $G = \mathbb{R}^+$ be the set of positive real numbers and let $\cdot$ be the multiplication of real numbers, denoted $\times$. We will show that $(\mathbb{R}^+, \times)$ is a group.

1. $\mathbb{R}^+$ is closed under $\times$: for any $a_1, a_2 \in \mathbb{R}^+$, $a_1 \times a_2 \in \mathbb{R}$ and $a_1 \times a_2 > 0$, hence $a_1 \times a_2 \in \mathbb{R}^+$.
2. $\times$ is associative: $\forall a_1, a_2, a_3 \in \mathbb{R}^+$, $a_1 \times (a_2 \times a_3) = (a_1 \times a_2) \times a_3$.
3. 1 is the identity element in $\mathbb{R}^+$: $\forall a \in \mathbb{R}^+$, $1 \times a = a \times 1 = a$.
4. Take any $a \in \mathbb{R}^+$, $\frac{1}{a} \in \mathbb{R}$ and $\frac{1}{a} > 0$, so $\frac{1}{a} \in \mathbb{R}^+$. Moreover,

$$a \times \frac{1}{a} = \frac{1}{a} \times a = 1$$

   hence $a^{-1} = \frac{1}{a} \in \mathbb{R}^+$

By definition, we have proved that, $(\mathbb{R}^+, \times)$ is a group.

Abelian group

Definition

Let $(G, \cdot)$ be a group. If $\cdot$ is commutative, i.e.

$$\forall g_1, g_2 \in G, g_1 \cdot g_2 = g_2 \cdot g_1,$$

then the group is called *abelian*.

The name abelian is in honor of the great mathematician Niels Henrik Abel (1802-1829).

Example

The groups we have seen before, $(\mathbb{Z}, +)$, $(\mathbb{R}^+, \times)$, $(\mathbb{Q} \backslash \{ 0 \}, \times)$, $(\mathbb{Q}, +)$, and $(\mathbb{C}, +)$ are all abelian groups.

Abelian group

Example

- $\mathcal{M}_{2\times 2}(\mathbb{R})$: 2×2 matrices with coefficients in $\mathbb{R}$.
- Matrix addition, denoted by $+$, is defined component-wise.

$$\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix} + \begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00} + b_{00} & a_{10} + b_{10} \\ a_{01} + b_{01} & a_{11} + b_{11} \end{pmatrix}.$$

$(\mathcal{M}_{2\times 2}(\mathbb{R}), +)$ is an abelian group:

- closure, associativity and commutativity of $+$ are easy to show
- The identity element is ?
- The inverse of matrix $\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix}$ is ? Does it belong to the set?

Abelian group

Example

- $\mathcal{M}_{2\times 2}(\mathbb{R})$: 2×2 matrices with coefficients in $\mathbb{R}$.
- Matrix addition, denoted by $+$, is defined component-wise.

$$\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix} + \begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}+b_{00} & a_{10}+b_{10} \\ a_{01}+b_{01} & a_{11}+b_{11} \end{pmatrix}.$$

$(\mathcal{M}_{2\times 2}(\mathbb{R}), +)$ is an abelian group:

- closure, associativity and commutativity of $+$ are easy to show
- The identity element is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- The inverse of a matrix $\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix}$ is $\begin{pmatrix} -a_{00} & -a_{10} \\ -a_{01} & -a_{11} \end{pmatrix}$, which is also in $(\mathcal{M}_{2\times 2}(\mathbb{R}), +)$.

Abelian group

Example

Let $\mathbb{F}_2 := \{ 0, 1 \}$. We define *logical XOR*, denoted $\oplus$, in $\mathbb{F}_2$ as follows:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

Closure, associativity, and commutativity can be directly seen from the definition. The identity element is ? and the inverse of the other element is ?

Abelian group

Example

Let $\mathbb{F}_2 := \{ 0, 1 \}$. We define *logical XOR*, denoted $\oplus$, in $\mathbb{F}_2$ as follows:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

Closure, associativity, and commutativity can be directly seen from the definition. The identity element is 0 and the inverse of 1 is 1. Hence $(\mathbb{F}_2, \oplus)$ is an abelian group.

Abelian group

Example

Let $E = \{ a, b \}$, $a \neq b$. Define addition in E as follows:

$$a + a = a, \quad a + b = b + a = b, \quad b + b = a.$$

Closure, associativity, and commutativity can be directly seen from the definition. The identity element is ? and the inverse of the other element is ?

Abelian group

Example

Let $E = \{ a, b \}$. Define addition in E as follows:

$$a + a = a, \quad a + b = b + a = b, \quad b + b = a.$$

Closure, associativity, and commutativity can be directly seen from the definition. The identity element is a and the inverse of b is b. Hence $(E, +)$ is an abelian group.

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Definition

Definition

A set R together with two binary operations $(R, +, \cdot)$ is a *ring* if $(R, +)$ is an abelian group, and for any $a, b, c \in R$, the following conditions are satisfied:

- R is closed under $\cdot$ (closure), $a \cdot b \in R$.
- $\cdot$ is associative, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- The distributive laws holds: $a \cdot (b + c) = a \cdot b + a \cdot c$.
- The identity element for $\cdot$ exists, which is different from the identity element for $+$.

Remark

The last condition in the definition implies that a set consisting of only 0 is not a ring.

Definition

If $a \cdot b = b \cdot a$ for all $a, b \in R$, R is a *commutative ring*.

Examples

Example

- We have seen that $(\mathbb{Z}, +)$ is an abelian group and the identity element is 0. It can be easily shown that $(\mathbb{Z}, +, \times)$ is a commutative ring. The identity element for $\times$ is ?
- Similarly $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are all commutative rings with ? as the identity element for $+$ and ? as the identity element for $\times$.

Examples

Example

- We have seen that $(\mathbb{Z}, +)$ is an abelian group and the identity element is 0. It can be easily shown that $(\mathbb{Z}, +, \times)$ is a commutative ring. The identity element for $\times$ is 1.
- Similarly $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are all commutative rings with 0 as the identity element for $+$ and 1 as the identity element for $\times$.

Notations

Remark

- For most cases, we will denote the identity element for $+$ as 0 and the identity element for $\cdot$ as 1.
- We normally refer to the operation $+$ as addition, and 0 as *additive identity*. Similarly, we refer to the operation $\cdot$ as multiplication and 1 as *multiplicative identity*.
- The inverse of an element $a \in R$ with respect to $+$ is called the *additive inverse* of a, usually denoted by $-a$.
- For simplicity, we sometimes write ab instead of $a \cdot b$.
- When the operations in $(R, +, \cdot)$ are clear from the context, we omit them and write R.

Example of a ring

Example

We have shown that $(\mathcal{M}_{2\times 2}(\mathbb{R}), +)$ is an abelian group. We recall matrix multiplication, denoted by $\times$, for 2×2 matrices: for any $\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix}, \begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix}$ in $\mathcal{M}_{2\times 2}(\mathbb{R})$,

$$\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix} \times \begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}b_{00} + a_{10}b_{01} & a_{00}b_{10} + a_{10}b_{11} \\ a_{01}b_{00} + a_{11}b_{01} & a_{01}b_{10} + a_{11}b_{11} \end{pmatrix}.$$

$(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \times)$ is a ring: associativity and distributive laws are easy to show. The identity element for $\times$ is ? Is $(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \times)$ a commutative ring? why?

Example of a ring

Example

We have shown that $(\mathcal{M}_{2\times 2}(\mathbb{R}), +)$ is an abelian group. We recall matrix multiplication, denoted by $\times$, for 2×2 matrices: for any $\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix}, \begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix}$ in $\mathcal{M}_{2\times 2}(\mathbb{R})$,

$$\begin{pmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{pmatrix} \times \begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}b_{00} + a_{10}b_{01} & a_{00}b_{10} + a_{10}b_{11} \\ a_{01}b_{00} + a_{11}b_{01} & a_{01}b_{10} + a_{11}b_{11} \end{pmatrix}.$$

$(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \times)$ is a ring: associativity and distributive laws are easy to show. The identity element for $\times$ is the 2×2 identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We note that $(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \times)$ is not a commutative ring. For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{ but } \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Example of a ring

Example

Recall an example of a group we have seen: $\mathbb{F}_2 = \{ 0, 1 \}$, *logical XOR*, denoted $\oplus$,

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

$(\mathbb{F}_2, \oplus)$ is an abelian group. Let us define *logical AND*, denoted $\&$, in $\mathbb{F}_2$ as follows:

$$0 \mathbin{\&} 0 = 0, \quad 1 \mathbin{\&} 0 = 0 \mathbin{\&} 1 = 0, \quad 1 \mathbin{\&} 1 = 1.$$

Closure of $\mathbb{F}_2$ with respect to $\&$, associativity and commutativity of $\&$, and the distributive laws are easy to see from the definitions. The identity element for $\&$ is ?
$(\mathbb{F}_2, \oplus, \&)$ is a commutative ring.

Example of a ring

Example

Recall an example of a group we have seen: $\mathbb{F}_2 = \{ 0, 1 \}$, *logical XOR*, denoted $\oplus$,

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

$(\mathbb{F}_2, \oplus)$ is an abelian group. Let us define *logical AND*, denoted $\&$, in $\mathbb{F}_2$ as follows:

$$0 \; \& \; 0 = 0, \quad 1 \; \& \; 0 = 0 \; \& \; 1 = 0, \quad 1 \; \& \; 1 = 1.$$

Closure of $\mathbb{F}_2$ with respect to $\&$, associativity and commutativity of $\&$, and the distributive laws are easy to see from the definitions. The identity element for $\&$ is 1. $(\mathbb{F}_2, \oplus, \&)$ is a commutative ring.

Example of a ring

Example

We have also seen $E = \{ a, b \}$ with addition:

$$a + a = a, \quad a + b = b + a = b, \quad b + b = a.$$

$(E, +)$ is an abelian group. Define multiplication in E as follows:

$$a \cdot a = a, \quad a \cdot b = b \cdot a = a, \quad b \cdot b = b.$$

Closure of E with respect to $\cdot$, associativity of $\cdot$, commutativity of $\cdot$, and the distributive laws are easy to see from the definitions. The identity element for $\cdot$ is ?

Example of a ring

Example

We have also seen $E = \{ a, b \}$ with addition:

$$a + a = a, \quad a + b = b + a = b, \quad b + b = a.$$

$(E, +)$ is an abelian group. Define multiplication in E as follows:

$$a \cdot a = a, \quad a \cdot b = b \cdot a = a, \quad b \cdot b = b.$$

Closure of E with respect to $\cdot$, associativity of $\cdot$, commutativity of $\cdot$, and the distributive laws are easy to see from the definitions. The identity element for $\cdot$ is b. Thus $(E, +, \cdot)$ is a commutative ring.

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Definition

Definition

Let $(R, +, \cdot)$ be a ring with identity element 0 for $+$ and identity element 1 for $\cdot$. Let $a, b \in R$. If $a \cdot b = b \cdot a = 1$, a (also b) is said to be *invertible* and it is called a *unit*.

Definition

A *field* is a commutative ring in which every non-zero element is invertible.

Example

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are all fields.
- $(\mathbb{Z}, +, \times)$ is not a field, why?

Definition

Definition

Let $(R, +, \cdot)$ be a ring with identity element 0 for $+$ and identity element 1 for $\cdot$. Let $a, b \in R$. If $a \cdot b = b \cdot a = 1$, a (also b) is said to be *invertible* and it is called a *unit*.

Definition

A *field* is a commutative ring in which every non-zero element is invertible.

Example

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are all fields.
- $(\mathbb{Z}, +, \times)$ is not a field. For example, $2 \in \mathbb{Z}$ is not invertible and $2 \neq 0$.

Multiplicative inverse

- By definition, for any $a \in F$, $a \neq 0$ there exists $b \in F$ such that $ab = ba = 1$.
- Then b is called the *multiplicative inverse* of a.
- It is easy to show that the multiplicative inverse of an element a is unique: let $b, c \in F$ be such that

  $$ab = ac = 1.$$

  Multiplying by b on the left, we get

  $$bab = bac = b \Longrightarrow b = c = b.$$

- We will denote the multiplicative inverse of a nonzero element $a \in F$ by a^{-1}.

Example of a field

Example

Recall an example of a commutative ring we have seen: $\mathbb{F}_2 = \{ 0, 1 \}$, *logical* *XOR*, denoted $\oplus$,

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

logical *AND*, denoted $\&$,

$$0 \ \& \ 0 = 0, \quad 1 \ \& \ 0 = 0 \ \& \ 1 = 0, \quad 1 \ \& \ 1 = 1.$$

The only nonzero element is ?, which has inverse ? with respective to $\&$.

Example of a field

Example

Recall an example of a commutative ring we have seen: $\mathbb{F}_2 = \{ 0, 1 \}$, *logical XOR*, denoted $\oplus$,

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

logical AND, denoted $\&$,

$$0 \ \& \ 0 = 0, \quad 1 \ \& \ 0 = 0 \ \& \ 1 = 0, \quad 1 \ \& \ 1 = 1.$$

The only nonzero element is 1, which has inverse 1 with respective to $\&$. Thus $(\mathbb{F}_2, \oplus, \&)$ is a field.

Example of a field

Example

We have also seen $E = \{ a, b \}$ with addition:

$$a + a = a, \quad a + b = b + a = b, \quad b + b = a.$$

and multiplication:

$$a \cdot a = a, \quad a \cdot b = b \cdot a = a, \quad b \cdot b = b.$$

$(E, +, \cdot)$ is a commutative ring. The only nonzero element, i.e. the element not equal to the additive identity, is ?, which has multiplicative inverse ?

Example of a field

Example

We have also seen $E = \{ a, b \}$ with addition:

$$a + a = a, \quad a + b = b + a = b, \quad b + b = a.$$

and multiplication:

$$a \cdot a = a, \quad a \cdot b = b \cdot a = a, \quad b \cdot b = b.$$

$(E, +, \cdot)$ is a commutative ring. The only nonzero element, i.e. the element not equal to the additive identity, is b, which has multiplicative inverse b since $b \cdot b = b$. Hence $(E, +, \cdot)$ is a field.

Finite field

Definition

A field with finite many elements is called a *finite field*.

Example

$(\mathbb{F}_2, \oplus, \&)$ is a finite field. $(E, +, \cdot)$ is a finite field.

Field isomorphism

Definition

Let $(F, +_F, \cdot_F), (E, +_E, \cdot_E)$ be two fields. F is said to be *isomorphic* to E, written $F \cong E$ if there is a bijective function $f : F \to E$ such that for any $a, b \in F$,

- $f(a +_F b) = f(a) +_E f(b)$, and
- $f(a \cdot_F b) = f(a) \cdot_E f(b)$.

Example

Let us consider the fields $(\mathbb{F}_2, \oplus, \&)$ and $(E, +, \cdot)$. Define $f : F \to E$, such that

$$f(0) = a, \quad f(1) = b.$$

f is bijective. f preserves both addition and multiplication. For example,

$$f(1 \oplus 0) = f(1) = b,\ f(1) + f(0) = b + a = b \Longrightarrow f(1 \oplus 0) = f(1) + f(0).$$

We have $\mathbb{F}_2 \cong E$.

Finite field

- It can be shown that any finite field with two elements is always isomorphic to $\mathbb{F}_2$.
- The next theorem says that, in general, there is only one finite field up to isomorphism.

Theorem

- *A finite field K contains p^n elements for a prime number p.*
- *For any prime p and any positive integer n, there exists, up to isomorphism, a unique field with p^n elements.*

Remark

We will use $\mathbb{F}_{p^n}$ to denote the unique finite field with p^n elements.

Example

$\mathbb{F}_2 = \{0, 1\}$

Bits

Definition

- Variables that range over $\mathbb{F}_2$ are called *Boolean variables* or *bits*.
- Addition of two bits is defined to be logical `XOR` , also called *exclusive or*.
- Multiplication of two bits is defined to be logical `AND`.
- When the value of a bit is changed, we say the bit is *flipped*.

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Definition

Definition (Vector space)

Let F be a field. A nonempty set V, together with two binary operations – *vector addition* (denoted by $+$) and *scalar multiplication by elements of* F (a map $V \times F \to V$), is called a *vector space* over F if $(V, +)$ is an abelian group and for any $\boldsymbol{v}, \boldsymbol{w} \in V$ and any $a, b \in F$, we have

- $a(\boldsymbol{v} + \boldsymbol{w}) = a\boldsymbol{v} + a\boldsymbol{w}$.
- $(a + b)\boldsymbol{v} = a\boldsymbol{v} + b\boldsymbol{v}$.
- $a(b\boldsymbol{v}) = (ab)\boldsymbol{v}$.
- $1\boldsymbol{v} = \boldsymbol{v}$, where 1 is the multiplicative identity of F.

Elements of V are called *vectors* and elements of F are called *scalars*.

Example

The set of complex numbers $\mathbb{C} = \{ x + iy \mid x, y \in \mathbb{R} \}$ is a vector space over $\mathbb{R}$. How are vector addition and scalar multiplication defined?

Example of a vector space

Example

The set of complex numbers $\mathbb{C} = \{\, x + iy \mid x, y \in \mathbb{R} \,\}$ is a vector space over $\mathbb{R}$. Note that for any $a_1 + b_1 i, a_2 + b_2 i \in \mathbb{C}$, vector addition is defined as

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i.$$

And for any $a \in \mathbb{R}$, scalar multiplication by elements of $\mathbb{R}$ is defined as

$$a(a_1 + b_1 i) = aa_1 + ab_1 i.$$

The identity element for vector addition is ? Furthermore, for any $a + bi \in \mathbb{C}$, its inverse with respect to vector addition is given by ?

Example of a vector space

Example

The set of complex numbers $\mathbb{C} = \{ x + iy \mid x, y \in \mathbb{R} \}$ is a vector space over $\mathbb{R}$. Note that for any $a_1 + b_1 i, a_2 + b_2 i \in \mathbb{C}$, vector addition is defined as

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i.$$

And for any $a \in \mathbb{R}$, scalar multiplication by elements of $\mathbb{R}$ is defined as

$$a(a_1 + b_1 i) = aa_1 + ab_1 i.$$

The identity element for vector addition is 0. Furthermore, for any $a + bi \in \mathbb{C}$, its inverse with respect to vector addition is given by $-a - bi$.

F^n

- Let F be a field
- Let $F^n = \{ (v_0, v_1, \ldots, v_{n-1}) \mid v_i \in F \ \forall i \}$ be the set of $n-$tuples over F.
- We define vector addition and scalar multiplication by elements of F component-wise as follows

for any $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1}) \in F^n$, $\boldsymbol{w} = (w_0, w_1, \ldots, w_{n-1}) \in F^n$, and any $a \in F$,

$$\boldsymbol{v} + \boldsymbol{w} := (v_0 + w_0, v_1 + w_1, \ldots, v_{n-1} + w_{n-1}),$$

$$a\boldsymbol{v} := (av_0, av_1, \ldots, av_{n-1}).$$

Theorem

$F^n = \{ (v_0, v_1, \ldots, v_{n-1}) \mid v_i \in F \ \forall i \}$ together with vector addition and scalar multiplication defined above is a vector space over F.

$\mathbb{F}_2^n$

Example

- Let $F = \mathbb{F}_2$, the unique finite field with two elements.
- Let n be a positive integer, it follows from the previous theorem that $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2$.
- The identity element for vector addition is ?
- For any $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_2^n$, the inverse of $\boldsymbol{v}$ with respect to vector addition is ?

$\mathbb{F}_2^n$

Example

- Let $F = \mathbb{F}_2$, the unique finite field with 2 elements.
- Let n be a positive integer, it follows from the previous theorem that $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2$.
- The identity element for vector addition is $\mathbf{0}$.
- For any $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_2^n$, the inverse of $\boldsymbol{v}$ with respect to vector addition is $(-v_0, -v_1, \ldots, -v_{n-1}) = \boldsymbol{v}$.

$\mathbb{F}_2^n$

- Recall that variables ranging over $\mathbb{F}_2$ are called bits. We have shown that $(\mathbb{F}_2, \oplus, \&)$ is a finite field, where $\oplus$ is logical `XOR`, and $\&$ is logical `AND`.

Definition

Vector addition in $\mathbb{F}_2^n$ is called *bitwise XOR*, also denoted $\oplus$. Similarly, we define *bitwise AND* between any two vectors $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$, $\boldsymbol{w} = (w_0, w_1, \ldots, w_{n-1})$ from $\mathbb{F}_2^n$ as follows:

$$\boldsymbol{v} \,\&\, \boldsymbol{w} := (v_0 \,\&\, w_0, v_1 \,\&\, w_1, \ldots, v_{n-1} \,\&\, w_{n-1}).$$

Another useful binary operation, logical `OR`, denoted $\vee$, on $\mathbb{F}_2$ is defined as follows:

$$0 \vee 0 = 0, \quad 1 \vee 0 = 1, \quad 0 \vee 1 = 1, \quad 1 \vee 1 = 1.$$

It can also be extended to $\mathbb{F}_2^n$ in a bitwise manner and we get *bitwise OR*.

$\mathbb{F}_2^n$

For simplicity, we sometimes write $v_0 v_1 \dots v_{n-1}$ instead of $(v_0, v_1, \dots, v_{n-1})$.

Example

Let $n = 3$, take $111, 101 \in \mathbb{F}_2^3$,

$$111 \oplus 101 = 010$$

$$111 \ \& \ 101 = 101$$

$$111 \vee 101 = 111.$$

Byte

Definition

A vector in $\mathbb{F}_2^n$ is called an n*-bit binary string*. A $4-$bit binary string is called a *nibble*. An $8-$bit binary string is called a *byte*.

Example

- $1010, 0011 \in \mathbb{F}_2^4$ are two nibbles. Furthermore,

$$1010 \oplus 0011 = 1001, \quad 1010 \ \& \ 0011 = 0010.$$

- 00101100 is a byte.

Remark

A byte can be considered as a base-2 representation/binary representation of an integer. The value of this integer is between 0 and 255 or between 00_{16} and $\mathtt{FF}_{16}$ with base-16 representation/hexadecimal representation.

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Congruent modulo n

- Let $n > 1$ be an integer.
- We are interested in the set $\{ 0, 1, 2 \ldots, n - 1 \}$.
- It can be considered as the set of possible remainders when dividing by n
- We will also associate each integer with one element in the set – namely the remainder of this integer divided by n.

Formally, we define

Definition

If $n|(b - a)$, then we say a *is congruent to* b *modulo* n, written $a \equiv b \bmod n$. n is called the *modulus*.

Remark

Saying a is congruent to b modulo n is equivalent to saying that the remainder of a divided by n is the same as the remainder of b divided by n.

Congruence class

Definition

For any $a \in \mathbb{Z}$, the *congruence class of* a *modulo* n, denoted $\overline{a}$, is given by

$$\overline{a} := \{ b \mid b \in \mathbb{Z}, b \equiv a \bmod n \} .$$

Lemma

Let $\mathbb{Z}_n$ *denote the set of all congruence classes of* $a \in \mathbb{Z}$ *modulo* n. *Then* $\mathbb{Z}_n = \{ \overline{0}, \overline{1}, \ldots, \overline{n-1} \}$.

Example

Let $n = 5$. We have $\overline{1} = \overline{6} = \overline{-4}$. $\mathbb{Z}_5 = \{ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \}$.

Addition and multiplication in $\mathbb{Z}_n$

Define addition on the set $\mathbb{Z}_n$ as follows:

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Example

- Let $n = 7$, $\overline{3} + \overline{2} = \overline{5}$.
- Let $n = 4$, $\overline{2} + \overline{2} = \overline{4} = \overline{0}$.

Define multiplication on $\mathbb{Z}_n$ as follows

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Example

Let $n = 5$,

$$\overline{-2} \cdot \overline{13} = \overline{3} \cdot \overline{3} = \overline{9} = \overline{4}$$

$\mathbb{Z}_n$

Theorem

$(\mathbb{Z}_n, +, \cdot)$, the set $\mathbb{Z}_n$ together with addition multiplication defined just now is a commutative ring.

Remark

For simplicity, we write a instead of $\overline{a}$ and to make sure there is no confusion we would first say $a \in \mathbb{Z}_n$. In particular, $\mathbb{Z}_n = \{ 0, 1, 2, \ldots, n-1 \}$. Furthermore, to emphasize that multiplication or addition is done in $\mathbb{Z}_n$, we write $ab \bmod n$ or $a + b \bmod n$.

Example

Let $n = 5$, we write

$$4 \times 2 \bmod 5 = 8 \bmod 5 = 3, \text{ or } 4 \times 2 \equiv 8 \equiv 3 \bmod 5.$$

Multiplicative inverse in $\mathbb{Z}_n$

Lemma

For any $a \in \mathbb{Z}_n$, $a \neq 0$, a has a multiplicative inverse, denoted $a^{-1} \mod n$, if and only if $\gcd(a, n) = 1$.

Proof.

We provide part of the proof.
By Bézout's identity, $\gcd(a, n) = sa + tn$ for some $s, t \in \mathbb{Z}$. If $\gcd(a, n) = 1$, then $sa + tn = 1$, i.e. $n | (1 - sa)$.
By definition, $sa \equiv 1 \mod n$, thus $a^{-1} \mod n = s$. □

Corollary

$\mathbb{Z}_n$ is a field if and only if n is prime.

Proof.

We know that $\mathbb{Z}_n$ is a commutative ring.
By Definition of a field and the previous Lemma, $\mathbb{Z}_n$ is a field if and only if for any $a \in \mathbb{Z}_n$ such that $a \neq 0$, we have $\gcd(a, n) = 1$, which is true if and only if n is a prime. □

Find multiplicative inverse in $\mathbb{Z}_n$

- Recall that by the extended Euclidean algorithm, we can find integers s, t such that
$$\gcd(a, n) = sa + tn$$
for any $a, n \in \mathbb{Z}$.
- In particular, when $\gcd(a, n) = 1$, we can find s, t such that $1 = as + tn$, which gives $as \bmod n = 1$.
- Thus, we can find $a^{-1} \bmod n = s \bmod n$ by the extended Euclidean algorithm.

Example – Find multiplicative inverse in $\mathbb{Z}_n$

Example

We have calculated $\gcd(160, 21) = 1$ using the Euclidean algorithm. By the extended Euclidean algorithm,

$$\begin{aligned} 1 &= 3 - 2, & 2 &= 5 - 3, \\ 3 &= 8 - 5, & 5 &= 13 - 8, \\ 8 &= 21 - 13, & 13 &= 160 - 21 \times 7. \end{aligned}$$

We have

$$\begin{aligned} 1 &= 3 - (5 - 3) = 3 \times 2 - 5 = 8 \times 2 - 5 \times 3 = 8 \times 2 - (13 - 8) \times 3 \\ &= 8 \times 5 - 13 \times 3 = 21 \times 5 - 13 \times 8 = 21 \times 5 - (160 - 21 \times 7) \times 8 \\ &= (-8) \times 160 + 61 \times 21. \end{aligned}$$

Thus

$$21^{-1} \bmod 160 = ?$$

Example – Find multiplicative inverse in $\mathbb{Z}_n$

Example

By the extended Euclidean algorithm,

$$\begin{aligned} 1 &= 3 - 2, & 2 &= 5 - 3, \\ 3 &= 8 - 5, & 5 &= 13 - 8, \\ 8 &= 21 - 13, & 13 &= 160 - 21 \times 7. \end{aligned}$$

$$\begin{aligned} 1 &= 3 - (5 - 3) = 3 \times 2 - 5 = 8 \times 2 - 5 \times 3 = 8 \times 2 - (13 - 8) \times 3 \\ &= 8 \times 5 - 13 \times 3 = 21 \times 5 - 13 \times 8 = 21 \times 5 - (160 - 21 \times 7) \times 8 \\ &= (-8) \times 160 + 61 \times 21. \end{aligned}$$

Thus

$$21^{-1} \bmod 160 = 61.$$

Similarly

$$160^{-1} \bmod 21 =?$$

Example – Find multiplicative inverse in $\mathbb{Z}_n$

Example

By the extended Euclidean algorithm,

$$\begin{array}{ll} 1 = 3 - 2, & 2 = 5 - 3, \\ 3 = 8 - 5, & 5 = 13 - 8, \\ 8 = 21 - 13, & 13 = 160 - 21 \times 7. \end{array}$$

$$\begin{aligned} 1 &= 3 - (5-3) = 3 \times 2 - 5 = 8 \times 2 - 5 \times 3 = 8 \times 2 - (13 - 8) \times 3 \\ &= 8 \times 5 - 13 \times 3 = 21 \times 5 - 13 \times 8 = 21 \times 5 - (160 - 21 \times 7) \times 8 \\ &= (-8) \times 160 + 61 \times 21. \end{aligned}$$

Thus

$$21^{-1} \bmod 160 = 61.$$

Similarly

$$160^{-1} \bmod 21 = -8 \bmod 21 = 13.$$

$\mathbb{Z}_n^*$

Definition

Let $\mathbb{Z}_n^*$ denote the set of congruence classes in $\mathbb{Z}_n$ which have multiplicative inverses:

$$\mathbb{Z}_n^* := \{\, a \mid a \in \mathbb{Z}_n, \gcd(a, n) = 1 \,\}.$$

The *Euler's totient function*, φ, is a function defined on the set of integers bigger than 1 such that $\varphi(n)$ gives the cardinality of $\mathbb{Z}_n^*$:

$$\varphi(n) = |\mathbb{Z}_n^*|.$$

Example

- Let $n = 3$, $\mathbb{Z}_3^* = \{\, 1, 2 \,\}$, $\varphi(3) =?$
- Let $n = 4$, $\mathbb{Z}_4^* =?$ $\varphi(4) =?$
- Let $n = p$ be a prime number, $\mathbb{Z}_p^* =?$ $\varphi(p) =?$

$\mathbb{Z}_n^*$

Definition

Let $\mathbb{Z}_n^*$ denote the set of congruence classes in $\mathbb{Z}_n$ which have multiplicative inverses:

$$\mathbb{Z}_n^* := \{ a \mid a \in \mathbb{Z}_n, \gcd(a, n) = 1 \} .$$

The *Euler's totient function*, φ, is a function defined on the set of integers bigger than 1 such that $\varphi(n)$ gives the cardinality of $\mathbb{Z}_n^*$:

$$\varphi(n) = |\mathbb{Z}_n^*|.$$

Example

- Let $n = 3$, $\mathbb{Z}_3^* = \{ 1, 2 \}$, $\varphi(3) = 2$.
- Let $n = 4$, $\mathbb{Z}_4^* = \{ 1, 3 \}$, $\varphi(4) = 2$.
- Let $n = p$ be a prime number, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{ 0 \} = \{ 1, 2, \ldots, p - 1 \}$, $\varphi(p) = p - 1$.

Euler's totient function

Theorem

For any $n \in \mathbb{Z}$, $n > 1$,

$$\textit{if} \quad n = \prod_{i=1}^{k} p_i^{e_i}, \quad \textit{then} \quad \varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right), \tag{1}$$

where p_i *are distinct primes.*

Example

- Let $n = 10$. $10 = 2 \times 5$. We can count the elements in $\mathbb{Z}_{10}$ that are coprime to 10 (there are four of them): $\mathbb{Z}_{10} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \}$. By the above theorem, we also have

$$\varphi(10) = 10 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 4.$$

Euler's totient function

Example

- Let $n = 120$. $120 = 2^3 \times 3 \times 5$.

$$\varphi(120) = ?$$

- Let $n = pq$, where p and q are two distinct primes. Then

$$\varphi(n) = ?$$

- Let $n = p^k$, where p is a prime and $k \in \mathbb{Z}$, $k \geq 1$, then

$$\varphi(p^k) = ?$$

- In particular, if $p = 2$,

$$\varphi(2^k) = ?$$

Euler's totient function

Example

- Let $n = 120$. $120 = 2^3 \times 3 \times 5$.

$$\varphi(120) = 120 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right) = 32.$$

- Let $n = pq$, where p and q are two distinct primes. Then

$$\varphi(n) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1).$$

- Let $n = p^k$, where p is a prime and $k \in \mathbb{Z}$, $k \geq 1$, then

$$\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1).$$

- In particular, if $p = 2$,

$$\varphi(2^k) = 2^{k-1}.$$

$\mathbb{Z}_n^*$

Lemma

$(\mathbb{Z}_n^*, \cdot)$, the set $\mathbb{Z}_n^*$ together with the multiplication defined in $\mathbb{Z}_n$, is an abelian group.

Recall multiplication in $\mathbb{Z}_n$:

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Example

Let $n = 5$,

$$\overline{-2} \cdot \overline{13} = \overline{3} \cdot \overline{3} = \overline{9} = \overline{4}$$

Euler's Theorem

Theorem (Euler's Theorem)

For any $a \in \mathbb{Z}$, $a^{\varphi(n)} \equiv 1 \mod n$ *if* $\gcd(a, n) = 1$.

Example

Let $n = 4$. We have calculated that $\varphi(4) = 2$. And

$$3^2 = 9 \equiv 1 \mod 4.$$

Let $n = 10$. we have calculated that $\varphi(10) = 4$. And

$$3^4 = 81 \equiv 1 \mod 10.$$

Fermat's Little Theorem

Note that $\varphi(p) = p - 1$, a direct corollary of Euler's Theorem is Fermat's Little Theorem.

Theorem (Fermat's Little Theorem)

Let p be a prime. For any $a \in \mathbb{Z}$, if $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

Example

- Let $p = 3$. $2^2 = 4 \equiv 1 \mod 3$.
- Let $p = 5$. $2^4 = 16 \equiv 1 \mod 5$.

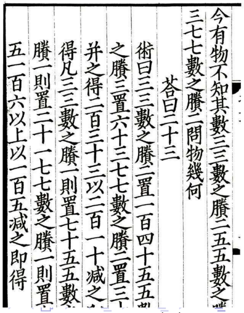
An ancient problem from the 3rd century

Sun Zi Suan Jing

"There is something whose amount is unknown. If we count by threes, 2 are remaining; by fives, 3 are remaining; and by sevens, 2 are remaining. How many things are there?"

Translating to our notations, the question is

$$
\begin{aligned}
x &\equiv 2 \bmod 3 \\
x &\equiv 3 \bmod 5 \\
x &\equiv 2 \bmod 7 \\
x &= ?
\end{aligned}
$$


今有物不知其數三三數之賸二五五數之
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五
之賸三置六十三七七數之賸二置三
并之得二百三十三以二百一十減之
得凡三三數之賸一則置七十五五數
賸一則置二十一七七數之賸一則置
五一百六以上以一百五減之即得

src: https://origin-view.inews.qq.com/a/20220129A09HWT0

Solving a system of simultaneous linear congruences

Before answering the question, we provide the solution for a more general case. Let us consider a system of simultaneous linear congruences

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_k \bmod m_k, \end{aligned}$$

where m_i are pairwise coprime positive integers, i.e $\gcd(m_i, m_j) = 1$ for $i \neq j$.

Solving a system of simultaneous linear congruences

$$
\begin{aligned}
x &\equiv a_1 \bmod m_1 \\
x &\equiv a_2 \bmod m_2 \\
&\vdots \\
x &\equiv a_k \bmod m_k,
\end{aligned}
$$

Define

$$m = \prod_{i=1}^{k} m_i, \quad M_i = \frac{m}{m_i}, \quad 1 \le i \le k.$$

Since m_i are pairwise coprime, m_i and M_i are coprime, and $y_i := M_i^{-1} \bmod m_i$ exists. It can be computed by the extended Euclidean algorithm. Let

$$x = \sum_{i=1}^{k} a_i y_i M_i \bmod m.$$

Then x is a solution.

An ancient problem from the 3rd century

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \\ x &= ? \end{aligned}$$

We have $m_1 = 3, m_2 = 5, m_3 = 7, a_1 = 2, a_2 = 3, a_3 = 2,$

$$m = 3 \times 5 \times 7 = 105,$$

$$M_1 = 35 \equiv 2 \bmod 3, \quad M_2 = 21 \equiv 1 \bmod 5, \quad M_3 = 15 \equiv 1 \bmod 7.$$

$$y_1 = M_1^{-1} \bmod 3 = 2, \quad y_2 = M_2^{-1} \bmod 5 = 1, \quad y_3 = M_3^{-1} \bmod 7 = 1.$$

$$x = \sum_{i=1}^{3} a_i y_i M_i = 2\times2\times35+3\times1\times21+2\times1\times15 \bmod 105 = 233 \bmod 105 = 23 \bmod 105.$$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_k$ *be pairwise coprime integers. For any* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$*, the system of simultaneous congruences*

$$x \equiv a_1 \text{ mod } m_1, \quad x \equiv a_2 \text{ mod } m_2, \quad \ldots \quad x \equiv a_k \text{ mod } m_k$$

has a unique solution modulo $m = \prod_{i=1}^{k} m_i$.

CRT – Example

Example

Find the unique solution $x \in \mathbb{Z}_{10}$ such that

$$x \equiv 10 \bmod 3, \quad x \equiv 10 \bmod 5.$$

We have

$$m_1 = ?, \quad m_2 = ?, \quad a_1 = ?, \quad a_2 = ?.$$

Hence

$$m = ?, \quad M_1 = ?, \quad M_2 = ?, \quad y_1 = ?, \quad y_2 = ?.$$

And

$$x = ?$$

CRT – Example

Example

Find the unique solution $x \in \mathbb{Z}_{15}$ such that

$$x \equiv 10 \bmod 3, \quad x \equiv 10 \bmod 5.$$

We have

$$m_1 = 3, \quad m_2 = 5, \quad a_1 = a_2 = 10.$$

Hence

$$m = 15, \quad M_1 = 5, \quad M_2 = 3, \quad y_1 = 5^{-1} \bmod 3 = 2, \quad y_2 = 3^{-1} \bmod 5 = 2.$$

And

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 \bmod n = 10 \times 2 \times 5 + 10 \times 2 \times 3 \bmod 15 = 160 \bmod 15 = 10.$$

CRT – Example

Example

p and q are distinct primes, $n = pq$, $a_p, a_q \in \mathbb{Z}$. Find the unique $x \in \mathbb{Z}_n$ such that

$$x \equiv a_p \bmod p, \quad x \equiv a_q \bmod q.$$

We have

$$M_1 = q, \quad M_2 = p,$$

$$y_q := y_1 = M_1^{-1} \bmod p = q^{-1} \bmod p, \; y_p := y_2 = M_2^{-1} \bmod q = p^{-1} \bmod q,$$

and

$$x = a_p y_q q + a_q y_p p \bmod n$$

CRT – Example

Example

Take two distinct primes p, q, and let $n = pq$. By CRT, for any $a \in \mathbb{Z}_n$, there is a unique solution $x \in \mathbb{Z}_n$ such that

$$x \equiv a \bmod p, \quad x \equiv a \bmod q.$$

Since $a \equiv a \bmod p$ and $a \equiv a \bmod q$, the unique solution is given by $x = a \in \mathbb{Z}_n$.

Abstract algebra and number theory

- Preliminaries
- Integers
- Groups
- Rings
- Fields
- Vector Spaces
- Modular Arithmetic
- Polynomial Rings

Definition

- We will introduce another example of a commutative ring – polynomial ring.
- Let $(F, +, \cdot)$ be a field with additive identity 0 and multiplicative identity 1.

Definition

- Define

$$F[x] := \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in F, n \geq 0 \right\}.$$

  An element $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ is called a *polynomial over* F.
- If $a_n \neq 0$, we define *degree of* $f(x)$, denoted $\deg(f(x))$, to be n. Following the convention, we define $\deg(0) = -\infty$.

Example

Let $F = \mathbb{R}$, then $f(x) = x + 1 \in \mathbb{R}[x]$ is a polynomial over $\mathbb{R}$ and $\deg(f(x)) = ?$

Polynomials

- We will introduce another example of a commutative, ring – polynomial ring.
- Let $(F, +, \cdot)$ be a field with additive identity 0 and multiplicative identity 1.

Definition

- Define
$$F[x] := \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in F, n \geq 0 \right\}.$$
An element $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ is called a *polynomial over* F.
- If $a_n \neq 0$, we define *degree of* $f(x)$, denoted $\deg(f(x))$, to be n. Following the convention, we define $\deg(0) = -\infty$.

Example

Let $F = \mathbb{R}$, then $f(x) = x + 1 \in \mathbb{R}[x]$ is a polynomial over $\mathbb{R}$ and $\deg(f(x)) = 1$.

Addition and multiplication

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$,
$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ in $F[x]$
Without loss of generality, let us assume $n \geq m$, write

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

where $b_i = 0$ for $i > m$. Then

$$f(x) +_{F[x]} g(x) := c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0, \text{ where } c_i = a_i + b_i.$$

And

$$f(x) \times_{F[x]} g(x) := d_n x^n + d_{n-1}x^{n-1} + \cdots + d_0, \text{ where } d_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Example

Let $F = \mathbb{R}$. Take $f(x) = x + 1, g(x) = x$ in $\mathbb{R}[x]$,

$$f(x) +_{\mathbb{R}[x]} g(x) = 2x + 1, \quad f(x) \times_{\mathbb{R}[x]} g(x) = x^2 + x.$$

Polynomial ring

Theorem

With the addition $+_{F[x]}$ and multiplication $\times_{F[x]}$ defined before, $(F[x], +_{F[x]}, \times_{F[x]})$ is a commutative ring. It is called the polynomial ring over F.

- The identity element for $+_{F[x]}$ is 0 – the identity element for $+$ in F.
- The identity element for $\times_{F[x]}$ is 1 – the identity element for $\cdot$ in F.
- For simplicity, we will write $f(x)g(x)$ and $f(x)+g(x)$ instead of $f(x) \times_{F[x]} g(x)$ and $f(x) +_{F[x]} g(x)$.

Example

Let $F = \mathbb{R}$, $\mathbb{R}[x]$ is a ring. The identity element for multiplication is 1. The identity element for addition is 0.

Division Algorithm

Theorem (Division Algorithm)

For any $f(x), g(x) \in F[x]$, *if* $\deg(f(x)) \geq 1$, *there exists* $s(x), r(x) \in F[x]$ *such that* $\deg(r(x)) < \deg(f(x))$ *and*

$$g(x) = s(x)f(x) + r(x).$$

$r(x)$ *is called the remainder and* $s(x)$ *is called the quotient.*

Definition

Let $f(x), g(x) \in F[x]$, if $f(x) \neq 0$ and $g(x) = s(x)f(x)$ for some $s(x) \in F[x]$, then we say $f(x)$ *divides* $g(x)$, written $f(x)|g(x)$.

Example

Take $g(x) = 4x^5 + x^3, f(x) = x^3 \in \mathbb{F}_3[x]$, then $g(x) = f(x)(4x^2 + 1)$ and $f(x)|g(x)$.

Irreducible polynomial

Definition

A polynomial $f(x) \in F[x]$ of positive degree is said to be *reducible (over F)* if there exist $g(x), h(x) \in F[x]$ such that

$$\deg(g(x)) < \deg(f(x)),\ \deg(h(x)) < \deg(f(x)),\ \text{and}\ f(x) = g(x)h(x).$$

Otherwise, it is said to be *irreducible (over F)*.

Example

Let $F = \mathbb{F}_2$. All the polynomials of degree 2 are $x^2, x^2+1, x^2+x+1, x^2+x$. Which polynomials are reducible?

Remark

$f(x) \in F[x]$ of degree 2 or 3 is reducible over F if and only if it has a root in F[a].

[a] An element $a \in F$ is a *root* of $f(x)$ if $f(a) = 0$.

Irreducible polynomial

Definition

A polynomial $f(x) \in F[x]$ of positive degree is said to be *reducible (over F)* if there exist $g(x), h(x) \in F[x]$ such that

$$\deg(g(x)) < \deg(f(x)),\ \deg(h(x)) < \deg(f(x)),\ \text{and } f(x) = g(x)h(x).$$

Otherwise, it is said to be *irreducible (over F)*.

Example

Let $F = \mathbb{F}_2$. All the polynomials of degree 2 are $x^2, x^2+1, x^2+x+1, x^2+x$. The only irreducible polynomial of degree 2 is x^2+x+1.

$$x^2 = x \cdot x,\ x^2+1 = (x+1)^2,\ x^2+x = x(x+1)$$

Congruence modulo $f(x)$

Definition

For any $g(x), h(x) \in F[x]$, if $f(x) | (g(x) - h(x))$, we say $h(x)$ *is congruent to* $g(x)$ *modulo* $f(x)$, written $g(x) \equiv h(x) \mod f(x)$.

Congruence class of $g(x)$ modulo $f(x)$ is given by $\{ h(x) \mid h(x) \equiv g(x) \mod f(x) \}$.

Lemma

Suppose $f(x)$ has degree n, where $n \geq 1$. Let $F[x]/(f(x))$ denote the set of all congruence classes of $g(x) \in F[x]$ modulo $f(x)$. Then

$$F[x]/(f(x)) = \left\{ \sum_{i=0}^{n-1} a_i x^i \;\middle|\; a_i \in F \text{ for } 0 \leq i < n \right\}.$$

Example

Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. $\mathbb{F}_2[x]/(f(x)) =?$

Congruence modulo $f(x)$

Example

Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Then

$$\mathbb{F}_2[x]/(f(x)) = \{ 0, 1, x, x+1 \} .$$

Similarly, let $g(x) = x^2 \in \mathbb{F}_2[x]$. Then

$$\mathbb{F}_2[x]/(g(x)) = \{ 0, 1, x, x+1 \} .$$

$\mathbb{F}_2[x]/(f(x))$ and $\mathbb{F}_2[x]/(g(x))$ contain equivalent classes generated by the same polynomials.

Addition and multiplication in $F[x]/(f(x))$

- Naturally, for any $g(x), h(x) \in F[x]/(f(x))$, same as in for $\mathbb{Z}_n$, addition and multiplication in $F[x]/(f(x))$ are computed modulo $f(x)$.

Example

Let $F = \mathbb{F}_2$, $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$, $g(x) = x \in \mathbb{F}_2[x]/(f(x))$, and $h(x) = x \in \mathbb{F}_2[x]/(f(x))$. We have

$$g(x) + h(x) \mod f(x) = ?$$
$$g(x)h(x) \mod f(x) = ?$$

Addition and multiplication in $F[x]/(f(x))$

- Naturally, for any $g(x), h(x) \in F[x]/(f(x))$, same as in for $\mathbb{Z}_n$, addition and multiplication in $F[x]/(f(x))$ are computed modulo $f(x)$.

Example

Let $F = \mathbb{F}_2$, $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$, $g(x) = x \in \mathbb{F}_2[x]/(f(x))$, and $h(x) = x \in \mathbb{F}_2[x]/(f(x))$. We have

$$g(x) + h(x) \bmod f(x) = x + x \bmod f(x) = 0,$$
$$g(x)h(x) \bmod f(x) = x^2 \bmod f(x) = x + 1.$$

Theorem

- *Together with addition and multiplication modulo $f(x)$, $F[x]/(f(x))$ is a commutative ring.*
- *It is a field if and only if $f(x)$ is irreducible.*
- *Let p be a prime, and let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of $\deg(f(x)) = n$. Then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n}$.*

Example

Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$, by the above theorem, $\mathbb{F}_2[x]/(f(x)) \cong ?$

$\mathbb{F}_{p^n}$

Theorem

- *Together with addition and multiplication modulo* $f(x)$, $F[x]/(f(x))$ *is a commutative ring.*
- *It is a field if and only if* $f(x)$ *is irreducible.*
- *Let* p *be a prime, and let* $f(x) \in \mathbb{F}_p[x]$ *be an irreducible polynomial of* $\deg(f(x)) = n$*. Then* $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n}$.

Example

Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$, by the above theorem, $\mathbb{F}_2[x]/(f(x)) \cong \mathbb{F}_{2^2}$.

Similarity to integers

$\mathbb{Z}_n$	$F[x]/(f(x))$
$a + b := (a + b) \bmod n$	$g(x) + h(x) := (g(x) + h(x)) \bmod f(x)$
$a \cdot b := (a \cdot b) \bmod n$	$g(x) \cdot h(x) := (g(x) \cdot h(x)) \bmod f(x)$
$\mathbb{Z}_n$ is a ring	$F[x]/(f(x))$ is a ring
$\mathbb{Z}_n$ is a field $\iff$ n is prime	$F[x]/(f(x))$ is a field $\iff$ $f(x)$ is irreducible

- Additive identity and multiplicative identity in $F[x]/(f(x))$ are the same as those in F.
- Multiplicative inverse can be found using the extended Euclidean algorithm

$\mathbb{F}_{2^8}$

- Let $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$.
- It can be shown that $f(x)$ is irreducible over $\mathbb{F}_2$
- Based on the previous results, we know that

$$\mathbb{F}_2[x]/(f(x)) = \left\{ \sum_{i=0}^{7} b_i x^i \;\middle|\; b_i \in \mathbb{F}_2 \ \forall i \right\},$$

and

$$\mathbb{F}_2[x]/(f(x)) \cong \mathbb{F}_{2^8}.$$

Bytes

- We note that any

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_2[x]/(f(x))$$

  can be stored as a byte $b_7b_6b_5b_4b_3b_2b_1b_0 \in \mathbb{F}_2^8$
- Define φ:

$$\begin{aligned} \varphi : \mathbb{F}_2[x]/(f(x)) &\rightarrow \mathbb{F}_2^8 \\ b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 &\mapsto b_7b_6b_5b_4b_3b_2b_1b_0 \end{aligned}$$

- φ is bijective

Example

- $x^6 + x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]/(f(x))$ corresponds to $01010111_2 =$ 57$_{16}$
- $x^7 + x + 1 \in \mathbb{F}_2[x]/(f(x))$ corresponds to $10000011_2 =$ 83$_{16}$.

Addition and multiplication between bytes

With addition and multiplication modulo $f(x)$ in $\mathbb{F}_2[x]/(f(x))$, we can define the corresponding addition and multiplication between bytes.

Definition

For any two bytes $\boldsymbol{v} = v_7 v_6 \ldots v_1 v_0$ and $\boldsymbol{w} = w_7 w_6 \ldots w_1 w_0$, let $g_{\boldsymbol{v}}(x) = v_7 x^7 + v_6 x^6 + \cdots + v_1 x + v_0$ and $g_{\boldsymbol{w}}(x) = w_7 x^7 + w_6 x^6 + \cdots + w_1 x + w_0$ be the corresponding polynomials in $\mathbb{F}_2[x]/(f(x))$. We define

$$\boldsymbol{v} + \boldsymbol{w} = g_{\boldsymbol{v}}(x) + g_{\boldsymbol{w}}(x) \mod f(x), \quad \boldsymbol{v} \times \boldsymbol{w} = g_{\boldsymbol{v}}(x) g_{\boldsymbol{w}}(x) \mod f(x).$$

Example

$f(x) = x^8 + x^4 + x^3 + x + 1$. Compute the sum and product between

$$x^6 + x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]/(f(x)) \quad \text{i.e.} \quad 01010111_2 = 57_{16}$$

and

$$x^7 + x + 1 \in \mathbb{F}_2[x]/(f(x)) \quad \text{i.e.} \quad 10000011_2 = 83_{16}$$

Addition and multiplication between bytes

Example

$$
\begin{aligned}
f(x) &= x^8 + x^4 + x^3 + x + 1. \\
\mathtt{57}_{16} + \mathtt{83}_{16} &= (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) \bmod f(x) \\
&= x^7 + x^6 + x^4 + x^2 \bmod f(x) = 11010100_2 = \mathtt{D4}_{16}.
\end{aligned}
$$

Addition and multiplication between bytes

Example

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

$$\begin{aligned}
\mathtt{57}_{16} \times \mathtt{83}_{16} &= (x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) \\
(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1, \\
x^8 &= x^4 + x^3 + x + 1 \mod f(x) \\
x^9 &= x^5 + x^4 + x^2 + x \mod f(x) \\
x^{11} &= x^7 + x^6 + x^4 + x^3 \mod f(x) \\
x^{13} &= x^9 + x^8 + x^6 + x^5 \mod f(x).
\end{aligned}$$

$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 = x^{11} + x^4 + x^3 + 1 = x^7 + x^6 + 1 \mod f(x).$$

$\mathtt{57}_{16} \times \mathtt{83}_{16} = 11000001_2 = \mathtt{C1}_{16}.$

Addition between bytes

For any

$$g(x) = \sum_{i=0}^{n-1} a_i x^i, \quad h(x) = \sum_{i=0}^{n-1} b_i x^i$$

from $\mathbb{F}_2[x]/(f(x))$, we have

$$g(x) + h(x) \bmod f(x) = \sum_{i=0}^{n-1} c_i x^i, \quad \text{where} \quad c_i = a_i + b_i \bmod 2.$$

Recall that a byte is also a vector in $\mathbb{F}_2^8$, we have defined vector addition as bitwise `XOR`, and

$$\boldsymbol{v} +_{\mathbb{F}_2^8} \boldsymbol{w} = \boldsymbol{u} = u_7 u_6 \dots u_1 u_0, \text{ where } u_i = v_i \oplus w_i.$$

We note that $a + b \bmod 2 = a \oplus b$ for $a, b \in \mathbb{F}_2$. Thus, our definition of addition between two bytes agrees with the vector addition between two vectors in $\mathbb{F}_2^8$.

Multiplication by 02

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

We will compute the formula for a byte multiplied by $02_{16} = x$. Take any $g(x) = b_7x^7 + b_6x^6 + \cdots + b_1x + b_0 \in \mathbb{F}_2[x]/(f(x))$

$$\begin{aligned}
& g(x)x \bmod f(x) \\
= \;& (b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0)x \bmod f(x) \\
= \;& b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \bmod f(x) \\
= \;& b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x + b_7x^4 + b_7x^3 + b_7x + b_7 \bmod f(x) \\
= \;& b_6x^7 + b_5x^6 + b_4x^5 + (b_3 + b_7)x^4 + (b_2 + b_7)x^3 + b_1x^2 + (b_0 + b_7)x + b_7 \bmod f(x).
\end{aligned}$$

Thus, for any byte $b_7b_6 \ldots b_1b_0$, multiplication by 02_{16} is equivalent to left shift by 1 and `XOR` with $00011011_2 = \mathtt{1B}_{16}$ if $b_7 = 1$.

Multiplication by 02

For any byte $b_7 b_6 \ldots b_1 b_0$, multiplication by $\texttt{02}_{16}$ is equivalent to left shift by 1 and $\texttt{XOR}$ with $00011011_2 = \texttt{1B}_{16}$ if $b_7 = 1$.

Example

- $\texttt{57}_{16} = 01010111_2$, $\texttt{02}_{16} \times \texttt{57}_{16} = 10101110 = \texttt{AE}_{16}$.
- $\texttt{83}_{16} = 10000011_2$, $\texttt{02}_{16} \times \texttt{83}_{16} =?$
- $\texttt{D4}_{16} = 11010100_2$, $\texttt{02}_{16} \times \texttt{D4}_{16} =?$

Multiplication by 02

Example

- $\mathtt{57}_{16} = 01010111_2$, $\mathtt{02}_{16} \times \mathtt{57}_{16} = 10101110 = \mathtt{AE}_{16}$.
- $\mathtt{83}_{16} = 10000011_2$, $\mathtt{02}_{16} \times \mathtt{83}_{16} = 00000110_2 \oplus 00011011_2 = 00011101_2 = \mathtt{1D}_{16}$.
- $\mathtt{D4}_{16} = 11010100_2$, $\mathtt{02}_{16} \times \mathtt{D4}_{16} = 10101000_2 \oplus 00011011_2 = 10110011_2 = \mathtt{B3}_{16}$.

Multiplication by 03

Let us compute the multiplication of a byte by $\texttt{03}_{16} = x + 1$. Take any $h(x) = b_7x^7 + b_6x^6 + \cdots + b_1x + b_0 \in \mathbb{F}_2[x]/(f(x))$, then

$$h(x)(x+1) \bmod f(x) = h(x)x + h(x) \bmod f(x).$$

Thus, for any byte $b_7b_6 \ldots b_1b_0$, multiplication by $\texttt{03}_{16}$ is equivalent to first multiplying by $\texttt{02}_{16}$ (left shift by 1 and XOR with $00011011_2 = \texttt{1B}_{16}$ if $b_7 = 1$) and then XOR with the byte itself $(b_7b_6 \ldots b_1b_0)$.

Example

We have computed

$$\texttt{02}_{16} \times \texttt{57}_{16} = \texttt{AE}_{16}, \quad \texttt{02}_{16} \times \texttt{83}_{16} = \texttt{1D}_{16}, \quad \texttt{02}_{16} \times \texttt{D4}_{16} = \texttt{B3}_{16}.$$

We have

- $\texttt{03}_{16} \times \texttt{57}_{16} = \texttt{AE}_{16} \oplus \texttt{57}_{16} = 10101110 \oplus 01010111 = \texttt{F9}_{16}$.
- $\texttt{03}_{16} \times \texttt{83}_{16} = \texttt{1D}_{16} \oplus \texttt{83}_{16} = \texttt{9E}_{16}$.
- $\texttt{03}_{16} \times \texttt{D4}_{16} = \texttt{B3}_{16} \oplus \texttt{D4}_{16} = \texttt{67}_{16}$.

Inverse of a byte as an element in $\mathbb{F}_2[x]/(f(x))$.

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

As mentioned before, multiplicative inverse of $g(x) \in \mathbb{F}_2[x]/(f(x))$ can be found using the extended Euclidean algorithm

Example

$03_{16} = 00000011_2 = x + 1$. By the Euclidean algorithm,

$$f(x) = (x+1)(x^7 + x^6 + x^5 + x^4 + x^2 + x) + 1 \Longrightarrow \gcd(f(x), (x+1)) = 1.$$

Long division

In primary school, we learned to do long division for calculating the quotient and remainder of dividing one integer by another integer. For example, to compute

$$1346 = 25 \times q + r,$$

we can write

$$\begin{array}{r} 53 \\ 25\,\overline{)\,1346} \\ \underline{125} \\ 96 \\ \underline{75} \\ 21 \end{array}$$

and we get $q = 53$, $r = 21$.

Similarly, let us take two polynomials $f(x), g(x) \in F[x]$, where F is a field. We can also compute $f(x)$ divided by $g(x)$ using long division.

Long division

Let

$$f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x], \quad g(x) = x + 1 \in \mathbb{F}_2[x].$$

We have

$$\begin{array}{r l}
 & x^7 + \ ? \\
x + 1 \big) & \overline{x^8 + x^4 + x^3 + x + 1} \\
 & \underline{x^8 + x^7}
\end{array}$$

Long division

$$
\begin{array}{r}
x^7 + x^6 + x^5 + x^4 + x^2 + x + 1 \\
x+1 \overline{\big) x^8 + x^4 + x^3 + x + 1} \\
\underline{x^8 + x^7} \\
x^7 + x^4 + x^3 + x + 1 \\
\underline{x^7 + x^6} \\
x^6 + x^4 + x^3 + x + 1 \\
\underline{x^6 + x^5} \\
x^5 + x^4 + x^3 + x + 1 \\
\underline{x^5 + x^4} \\
x^3 + x + 1 \\
\underline{x^3 + x^2} \\
x^2 + x + 1 \\
\underline{x^2 + x} \\
1
\end{array}
$$

$$f(x) = (x+1)(x^7+x^6+x^5+x^4+x^2+x+1)+1.$$

Inverse of a byte as an element in $\mathbb{F}_2[x]/(f(x))$.

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

As mentioned before, multiplicative inverse of $g(x) \in \mathbb{F}_2[x]/(f(x))$ can be found using the extended Euclidean algorithm

Example

$\texttt{03}_{16} = 00000011_2 = x + 1$. By the Euclidean algorithm,

$$f(x) = (x+1)(x^7 + x^6 + x^5 + x^4 + x^2 + x) + 1 \Longrightarrow \gcd(f(x), (x+1)) = 1.$$

By the extended Euclidean algorithm,

$$1 = f(x) + (x+1)(x^7 + x^6 + x^5 + x^4 + x^2 + x).$$

We have

$$\texttt{03}_{16}^{-1} = (x+1)^{-1} \bmod f(x) = x^7 + x^6 + x^5 + x^4 + x^2 + x = 11110110_2 = \texttt{F6}_{16}.$$

Assignment 1

- Read textbook