Cryptography

Lecture 2 : Mathematics Background

Dr. Muhammad Hataba

Muhammad.Hataba@giu-uni.de

References and Legalities

These slides are in part based on:

- Understanding Cryptography, Christof Paar and Jan Pelzl
- Cryptography and Network Security Course, Swansea University,
- Information Security Course, German International University, Amr ElMougy
- Cryptography Course, German International University, *Alia El Bolock*

Outline of Today's Lecture

- Modular Arithmetic
- Groups, Rings, and Fields
- Prime and Extension Fields
- Arithmetic for Extension Fields

Modular Arithmetic

Prime Numbers

- Prime numbers only have divisors of 1 and self
  - they cannot be written as a product of other numbers
  - note: 1 is not prime, but is generally not of interest
- eg. 2, 3, 5, 7 are prime, 4, 6, 8, 9, 10 are not
- Prime numbers are central to number theory
- List of prime number less than 200 is:

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

Prime Factorization

- To **factor** a number n is to write it as a product of other numbers

  n=abc

- Note that factoring a number is relatively hard compared to multiplying the factors together to generate the number
- A **prime factorisation** of a number n is writing it as a product of primes
  - eg. $91 = 7 \times 13$; $3600 = 2^4 \times 3^2 \times 5^2$

$$a = \prod_{p \in \mathrm{P}} p^{a_p}$$

Divisibility

Definition: An integer n is divisible by a nonzero integer a if we can write it as $n = as$ for some integer s.

The following statements are equivalent:

- n is divisible by a
- a divides n
- a is a factor of n
- n is a multiple of a
- Mathematical notation: $a \mid n$

If an integer b does ***not*** divide n, we write $b \nmid n$

Example: A number n is even if and only if $2 \mid n$

Example: A number n is odd if and only if $2 \nmid n$

GCD and Relative Primality

- Two numbers (a,b) are **relatively prime** if they have no common divisors apart from 1
  - eg. 8 & 15 are relatively prime since
    - Factors of 8 are 1,2, 4, 8
    - Factors of 15 are 1,3, 5, 15
    - 1is the only common factor
- Determine the greatest common divisor by comparing their prime factorizations and using least powers

$$\text{e.g., } 300 = 2^1 \times 3^1 \times 5^2$$

$$18 = 2^1 \times 3^2 \times 5^0$$

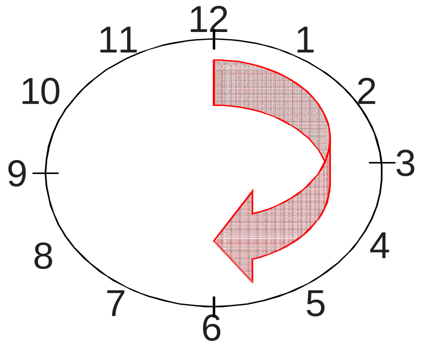
$$\Rightarrow \gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$$

Modulus

Generally speaking, most cryptosystems are based on **sets of numbers** that are

1. **discrete** (sets with integers are particularly useful)
2. **finite** (i.e., if we only compute with a finitely many numbers)

Seems too abstract? --- Let‘s look at a finite set with discrete numbers we are quite familiar with: a clock.



Interestingly, even though the numbers are incremented every hour we never leave the set of integers:

1, 2, 3, … 11, 12, 1, 2, 3, … 11, 12, 1, 2, 3, …:

Modulus

Definition 1.4.1 Modulo Operation

Let $a, r, m \in \mathbb{Z}$ *(where* $\mathbb{Z}$ *is a set of all integers) and* $m > 0$. *We write*

$$a \equiv r \bmod m$$

if m *divides* $a - r$.

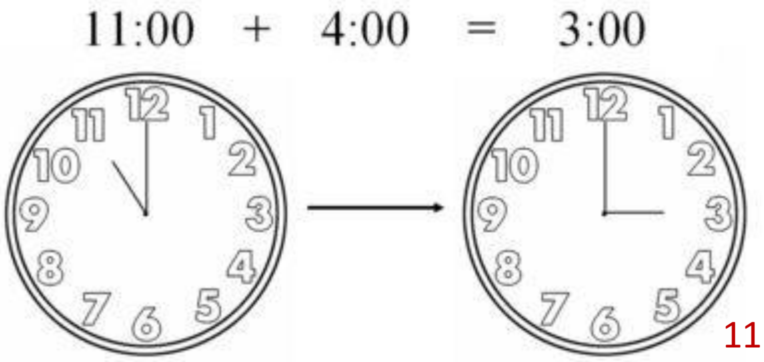
m *is called the* modulus *and* r *is called the* remainder.

Divisibility and Modular Arithmetic

In many applications, we only care about the remainder when an integer is divided by a specific positive integer.

- **Example 1:** On a 12-hour clock, what time is it when it is 52 hours after 11:00?
- **Answer 1:** 52 mod 12 = 4 ⇒ 11:00 + 4 hrs = 15:00
  ⇒ 15:00 mod 12 = 3:00

- **Example 2:** What day of the week will it be 100 days from today?
- **Answer 2:** 100 mod 7 = 2



Congruence

- We have already introduced *a mod m* to represent the remainder when *a* is divided by positive integer *m*
- We also will find it useful to say when two numbers *a* and *b* have the same remainder when divided by positive integer *m*.
- **Definition:** If *a* and *b* are integers and *m* is a positive integer, we say that *a* and *b* are **congruent modulo m** when (all of these are equivalent):
  - *a* and *b* have the same remainder when divided by *m*
  - $m \mid (a-b)$
  - **a mod m = b mod m**
  - $a \equiv b \pmod{m}$
- If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$

Equivalence Classes

- Consider equivalence classes *mod 3*

$$\begin{array}{ccc} [0] & [1] & [2] \\ 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \\ 9 & 10 & 11 \\ \vdots & \vdots & \vdots \end{array}$$

$[0] = \{\ldots -6,-3,0,3,6,9,\ldots\}$ and $[1] = \{\ldots -5,-2,1,4,7,10,\ldots\}$ and $[2] = \{\ldots -4,-1,2,5,8,11,\ldots\}$

Congruence Relationships

- We can also do arithmetic modulo a positive integer m
  (you already do this naturally mod 12 when you use a 12-hour clock)
- **Theorem:** Let m be a positive integer. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then

$$a + c \equiv b + d \bmod m \qquad \text{and} \qquad ac \equiv bd \bmod m$$

Congruence Relationships - Examples

- **Example:** If $7 \equiv 2 \bmod 5$ and $11 \equiv 1 \bmod 5$
  it follows that

  $$18 \equiv 3 \bmod 5$$

  and

  $$77 \equiv 2 \bmod 5$$

- **Question:** If $ac \equiv bc \bmod m$, is it true that $a \equiv b \bmod m$?
- **Answer:** No!
  Counterexample $a=2, b=4, c=6$ and $m=12$.
  We have:

  $$12 \equiv 24 \bmod 12 = 0 \qquad \text{but} \qquad 2 \not\equiv 4 \bmod 12$$

Modular Arithmetic

- We can also "distribute" the modulo operator
- **Theorem:** Let m be a positive integer and a, b are integers. Then…

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m \quad \text{and}$$

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

- **Fun/useful fact: We can "mod-out" before doing complicated arithmetic. (you might do this in your head already!)**
- **Example:** What is $81 \cdot 124 \bmod 11$?

$$\begin{aligned} 81 \cdot 124 \bmod 11 &= ((81 \bmod 11)(124 \bmod 11)) \bmod 11 \\ &= (4 \cdot 3) \bmod 11 \\ &= 12 \bmod 11 = 1 \end{aligned}$$

Modular Arithmetic - Example

Example: Compute $10^n \bmod 11$ for integer values of n

Solution:

$10^1 \bmod 11 = 10$ $\quad (10 = 11*0 + 10)$

$10^2 \bmod 11 = 100 \bmod 11 = 1$ $\quad (100 = 11*9 + 1)$

$10^3 \bmod 11 = 1000 \bmod 11 = 10$ $\quad (1000 = 11*90 + 10)$

…

$$
\begin{aligned}
10^4 \bmod 11 &= (10^3 \bmod 11)(10^1 \bmod 11) \bmod 11 \\
&= (10 \cdot 10) \bmod 11 \\
&= 100 \bmod 11 = 1
\end{aligned}
$$

…

$10^n \bmod 11 = 1$ if n is even, 10 if n is odd

Modular Additive Inverse

- The additive inverse b of a number a is defined such that:

$$a + b \equiv 0 \bmod m$$

- i.e., $b = n - a$
- Example: What is the inverse of $5 \bmod 9$?

The inverse of $5 \bmod 9$ is 4 because $5 + 4 \equiv 0 \bmod 9$

Multiplicative Inverse (Modular Division)

- Rather than performing a division, we prefer to multiply by the inverse

$$b / a \equiv b \times a^{-1} \bmod m$$

- The inverse a^{-1} of a number a is defined such that:

$$a a^{-1} \equiv 1 \bmod m$$

- Example: What is $5 / 7 \bmod 9$?

The inverse of $7 \bmod 9$ is 4 since $7 \times 4 \equiv 28 \equiv 1 \bmod 9$, hence:

$$5 / 7 \equiv 5 \times 4 = 20 \equiv 2 \bmod 9$$

Computing the Inverse (mod m)

How is the inverse computed?

- The inverse of a number a mod m only exists if and only if a and m are coprime, i.e., :

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

  e.g., $\gcd(5, 9) = 1$, so that the inverse of 5 exists modulo 9)

- For now, the best way of computing the inverse is to use exhaustive search.

Excursion: Chapter 6 of Understanding Cryptography shows the Extended Euclidean Algorithm for computing an inverse for a given number and modulus.

Fermat's Theorem

Just FYI!

Fermat's Little Theorem

- $a^{p-1} = 1 (\bmod p)$
  - where p is prime and $gcd(a,p) = 1$
- Also: $a^p = a (\bmod p)$
- useful in public key and primality testing

Euler's Totient φ(n)

Just FYI!

For arithmetic modulo n

- **complete set of residues** is: 0..n-1
- **reduced set of residues** is those numbers (residues) which are relatively prime to n

  e.g., for n=10,

  – complete set of residues is {0,1,2,3,4,5,6,7,8,9}

  – reduced set of residues is {1,3,7,9}
- Number of elements in reduced set of residues is called the **Euler Totient Function φ**(n)

Euler's Totient $\varphi(n)$

Just FYI!

- To compute $\varphi(n)$ need to count number of residues to be excluded
- In general, this needs prime factorization, but
  - for p prime: $\varphi(p) = p - 1$
  - for p, q prime: $\varphi(pq) = (p - 1) x (q - 1)$

e.g.,

$\varphi(37) = 36$

$\varphi(21) = (3 - 1) x (7 - 1) = 2 x 6 = 12$

Euler's Theorem

Just FYI!

- Generalisation of Fermat's Theorem
- $a^{\varphi(n)} = 1 (\mathrm{mod}\ n)$
  - for any a, n where $\gcd(a, n) = 1$

e.g.,

$a = 3;\ n = 10;\ \boldsymbol{\varphi}(10) = 4;$

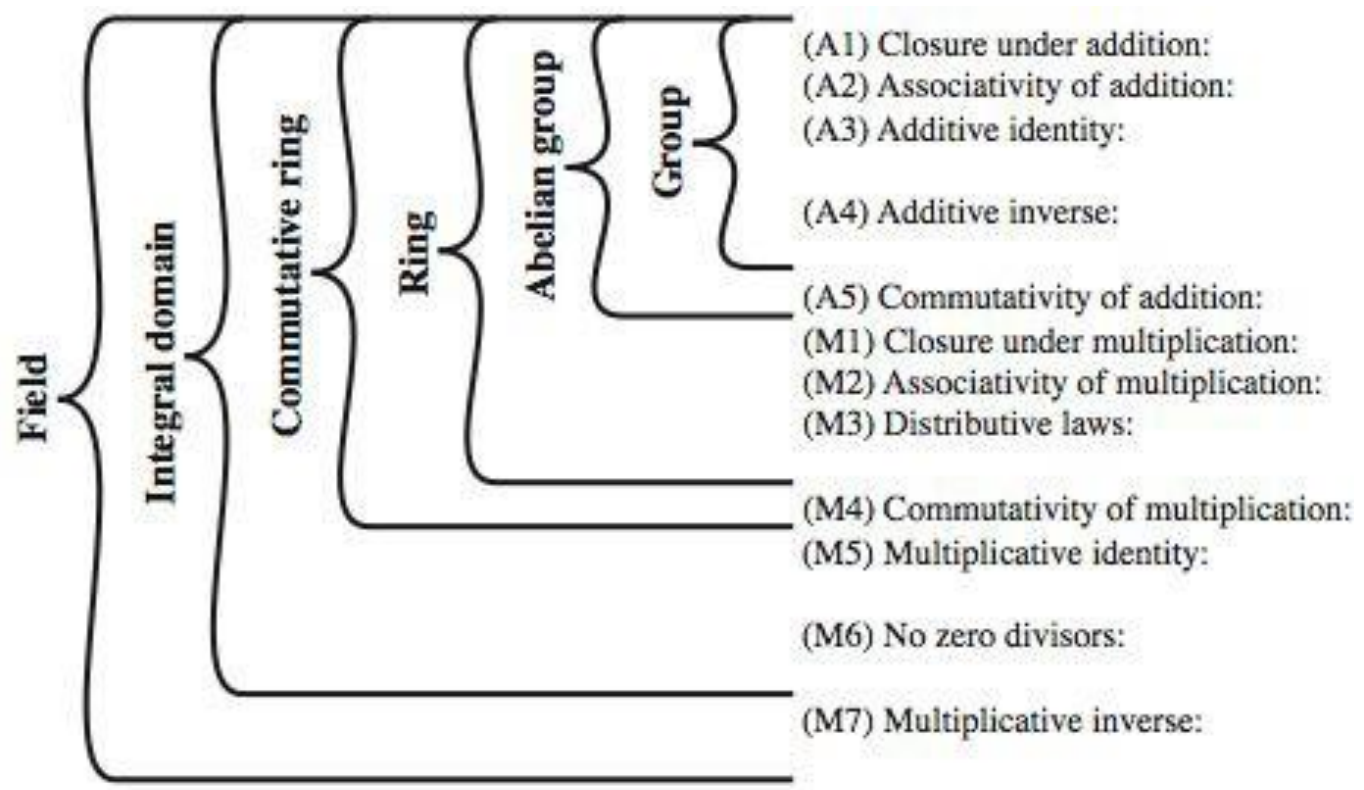
hence $3^4 = 81 = 1 \bmod 10$

$a = 2;\ n = 11;\ \boldsymbol{\varphi}(11) = 10;$

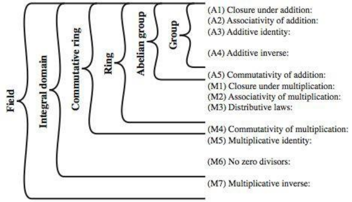
hence $2^{10} = 1024 = 1 \bmod 11$

Groups, Rings, and Fields

Mathematical Objects



Groups



Definition 4.3.1 Group

A group *is a set of elements G together with an operation $\circ$ which combines two elements of G. A group has the following properties:*

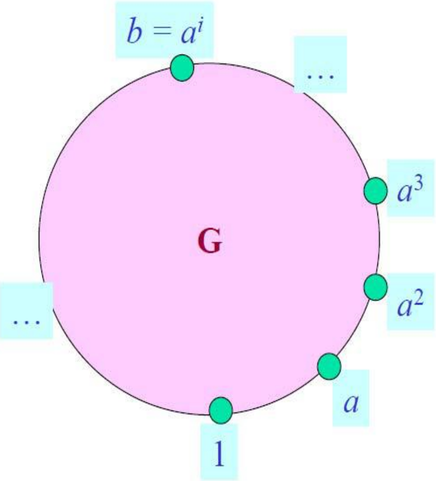
1. *The group operation $\circ$ is* closed. *That is, for all $a, b, \in G$, it holds that $a \circ b = c \in G$.*
2. *The group operation is* associative. *That is, $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$.*
3. *There is an element $1 \in G$, called the* neutral element *(or* identity element*), such that $a \circ 1 = 1 \circ a = a$ for all $a \in G$.*
4. *For each $a \in G$ there exists an element $a^{-1} \in G$, called the* inverse *of a, such that $a \circ a^{-1} = a^{-1} \circ a = 1$.*
5. *A group G is* abelian (or commutative) *if, furthermore, $a \circ b = b \circ a$ for all $a, b \in G$.*

Groups - Example

- The set of integers $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ and **addition modulo m** form a group with the neutral element 0.
- Every element a has an inverse $-a$ such that $a + (-a) = 0 \bmod m$.
- **Note**: this set does not form a group with **multiplication** because most elements a do not have an inverse such that $a a^{-1} = 1 \bmod m$.

Cyclic Groups

Definition 2 A multiplicative group G is said to be *cyclic* if there is an element $a \in G$ such that for any $b \in G$ there is some integer i with $b = a^i$. Such an element a is called a *generator* of the cyclic group, and we write $G = \langle a \rangle$.



Examples

- $(Z_6, +, 0)$, cyclic group with generators 1 and 5.

- $(Z_3^*, \times, 1)$, cyclic group with generator 2.

  $Z_3^* = \{1, 2\} = \langle 2 \rangle = \{2^0 = 1, 2\}$, $2^2 = 1 \bmod 3$.

- $(Z_7^*, \times, 1)$, cyclic group, 3 is a generator:

  $3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1 \bmod 7$

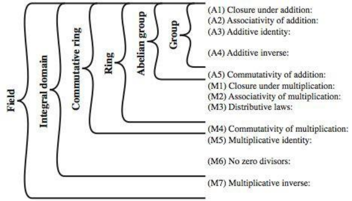
  However, $2^3 = 1 \bmod 7$. Thus 2 is not a generator of Z_7^*.

- $(Z_5^*, \times, 1)$, cyclic group, 2 is a generator.

  $2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1 \bmod 5$, thus $Z_5^* = \langle 2 \rangle$.

  i.e., every element in Z_5^* can be written into a power of 2.

Rings



Definition 1.4.2 Ring

The integer ring $\mathbb{Z}_m$ consists of:

1. *The set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$*
2. *Two operations "$+$" and "$\times$" for all $a, b \in \mathbb{Z}_m$ such that:*
   1. $a + b \equiv c \mod m$, $(c \in \mathbb{Z}_m)$
   2. $a \times b \equiv d \mod m$, $(d \in \mathbb{Z}_m)$

Rings - Example

- Let m=9, i.e., we are dealing with the ring $\mathbb{Z}_9 = \{0,1,2,3,4,5,6,7,8\}$.
- Let's look at a few simple arithmetic operations:

$$6+8=14 \equiv 5 \bmod 9$$

$$6 \times 8 = 48 \equiv 3 \bmod 9$$

Rings - Some Properties

- Closed under addition and multiplication
- Addition and multiplication are associative
  e.g., $a + (b + c) = (a + b) + c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,b,c \in \mathbb{Z}_m$
- There is the neutral element 0 with respect to addition,
  i.e., for every element $a \in \mathbb{Z}_m$ it holds that $a + 0 \equiv a \bmod m$
- For any element a in the ring, there is always the negative element $-a$ such that $a + (-a) \equiv 0 \bmod m$, i.e., the additive inverse always exists
- There is the neutral element 1with respect to multiplication,
  i.e., for every element $a \in \mathbb{Z}_m$ it holds that $a \times 1 \equiv a \bmod m$
- The multiplicative inverse exists only for some, but not for all, elements
  - Let $a \in \mathbb{Z}$, the inverse a^{-1} is defined such that $a \cdot a^{-1} \equiv 1 \bmod m$
  - If an inverse exists for a, we can divide by this element since $b/a \equiv b \cdot a^{-1} \bmod m$
  - It is computationally hard to find the inverse
  - However, its existence can be checked: An element $a \in \mathbb{Z}$ has a multiplicative inverse a^{-1} if and only if $\gcd(a,m) = 1$

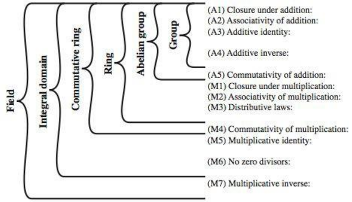
Integral Domain

An integral domain {R,+,×} is a commutative ring that obeys the following two additional properties:

- *ADDITIONAL PROPERTY 1:* The set R must include an identity element for the multiplicative operation. That is, it should be possible to symbolically designate an element of the set R as ’1’ so that for every element a of the set we can say a1 = 1a = a
- *ADDITIONAL PROPERTY 2:* Let 0 denote the identity element for the addition operation. If a multiplication of any two elements a and b of R results in 0, that is if ab = 0 then either a or b must be 0.

Examples of an integral domain: The set of all integers under the operations of arithmetic addition and multiplication.

Fields



Definition 4.3.2 Field

A field F *is a set of elements with the following properties:*

- *All elements of* F *form an additive group with the group operation "+" and the neutral element 0.*
- *All elements of* F *except 0 form a multiplicative group with the group operation "×" and the neutral element 1.*
- *When the two group operations are mixed, the distributivity law holds, i.e., for all* $a,b,c \in F$: $a(b+c) = (ab)+(ac)$.

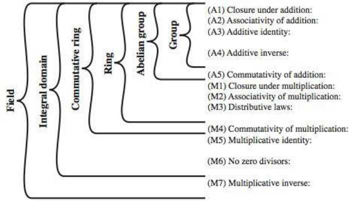
Fields - Example

The set $\mathbb{R}$ of real numbers is a field with the neutral element 0 for the **additive** group and the neutral element 1 for the **multiplicative** group.

Every real number a has an additive inverse, namely $-a$, and every nonzero element a has a multiplicative inverse 1/a.

- The set of all integers under the operations of arithmetic addition and multiplication is NOT a field.

Finite or Galois Fields



Theorem 4.3.1 *A field with order m only exists if m is a prime power, i.e., $m = p^n$, for some positive integer n and prime integer p. p is called the* characteristic *of the finite field.*

- **Order:** number of elements in the field (also called cardinality)

Thus, we can have finite fields with 11, 81 (= 3^4), or 256(= 2^8) elements.

However, not with 12 ($2^2 * 3$) elements.

Prime and Extension Fields

Fields

Field $GF(p^n)$

$n=1$

Prime Field

GF(p)

$n>1$

Extension Field

$GF(p^n)$

Prime Fields

Most intuitive fields: *n=1*$\Rightarrow$ Fields of Prime Order *GF(p)*

Theorem 4.3.2 *Let p be a prime. The integer ring* $\mathbb{Z}_p$ *is denoted as* $GF(p)$ *and is referred to as a* prime field, *or as a* Galois field *with a prime number of elements. All nonzero elements of* $GF(p)$ *have an inverse. Arithmetic in* $GF(p)$ *is done modulo p.*

Prime Fields - Example GF(5)

- Consider the finite field

  $$GF(5) = \{0,1,2,3,4\}$$

- Tables enable performing all calculations in this field without using modular reduction explicitly

addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

additive inverse

$-0 = 0$
$-1 = 4$
$-2 = 3$
$-3 = 2$
$-4 = 1$

multiplication

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

multiplicative inverse

0^{-1} does not exist
$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

Prime Fields - Example GF(2)

- Consider the finite field $GF(2) = \{0,1\}$ (Very important prime field. Why??)

addition

+	0	1
0	0	1
1	1	0

multiplication

×	0	1
0	0	0
1	0	1

- Addition is equivalent to XOR gate
- Multiplication is equivalent to AND gate

Extension Fields GF(2^m)

- Important for cryptography
- The Advanced Encryption Standard (AES) is based on a finite field consisting of 256 elements, denoted GF(2^8).
- Each field element represents one byte.
- GF(2^8) is not a prime field but an extension field (for $m>1$).
- Addition and multiplication cannot be represented by addition and multiplication of integers modulo 2^8.

Notation for Extension Field Elements

- Elements of $GF(2^m)$ are represented as polynomials
- The polynomials have coefficients that are elements of GF(2)
- Maximum degree of polynomials is $m-1$, i.e., there are m coefficients per element.
- $A \in GF(2^8)$ is represented as:

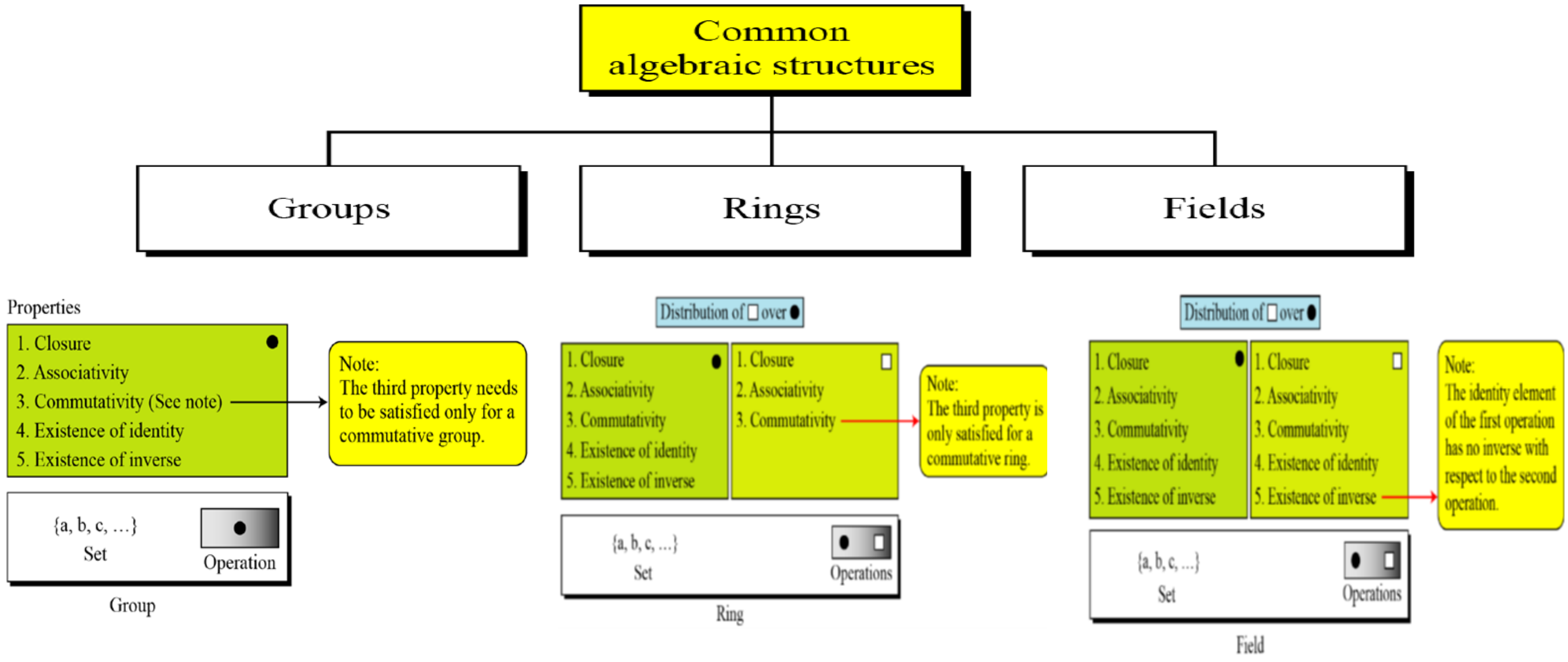
$$A(x) = a_7 x^7 + \cdots + a_1 x + a_0, \text{ where } a_i \in GF(2) = \{0,1\}$$

- There are exactly 256 such polynomials that make up the finite field of $GF(2^8)$
- Such polynomials can be stored as an 8-bit vector

$$A = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$$

Recall: A polynomial is an expression consisting of variables and coefficients, that involves only the
operations of +, -, x, and non-negative integer exponents of variables

To Summarize...



Thank you