# Elementary Number Theory
# (Finite Fields, GCD and Modular Arithmetics)

Presented by: Er. Kobid Karkee
Himalaya College of Engineering

# Chapter Overview

- In order to understand some of the cryptographic algorithms dealt with throughout this course, it is necessary to have some background in two areas of mathematics
- Number Theory.
- Abstract Algebra.
- New Advanced Encryption Standard (AES) relies on the subject of finite fields which forms a part of abstract algebra.

# Number Theory

- Number theory deals with the theory of numbers and is probably one of the oldest branches of mathematics.
- It is divided into several areas including elementary, analytic and algebraic number theory.
- These are distinguished more by the methods used in each than the type of problems posed.
- Relevant ideas discussed here and include:
  - The greatest common divisor,
  - The modulus operator,
  - The modular inverse,
  - Euclidean and Extended Euclidean algorithms,
  - Finite fields

# The Divides Operator

- New notation: $3 \mid 12$
  - To specify when an integer evenly divides another integer
  - Read as "3 divides 12" or "3 is the divisor of 12"

- The not-divides operator: $5 \nmid 12$
  - To specify when an integer does *not* evenly divide another integer
  - Read as "5 does not divide 12" or "5 is not the divisor of 12"

# Divides, Factors and Multiples

- Let $a,b \in \mathbf{Z}$ with $a \neq 0$.

- **Def.:** $a|b$ $\equiv$ "*a divides b*" $:\equiv$ $(\exists\, c \in \mathbf{Z}\!: b = ac)$
- "There is an integer *c* such that *c* times *a* equals *b*."
  - Example: $3|-12 \Leftrightarrow$ **True**, but $3|7 \Leftrightarrow$ **False**.

- Iff (if and only if) *a* divides *b*, then we say *a* is a *factor* or a *divisor* of *b*, and *b* is a *multiple* of *a*.

- Ex.: "*b* is even" $:\equiv 2|b$. Is 0 even? Is $-4$?

# Results on the divides operator

- If a | b and a | c, then a | (b+c)
  - Example: if 5 | 25 and 5 | 30, then 5 | (25+30)
- If a | b, then a | bc for all integers c
  - Example: if 5 | 25, then 5 | 25*c for all ints c
- If a | b and b | c, then a | c
  - Example: if 5 | 25 and 25 | 100, then 5 | 100

# The Division “Algorithm”

- Theorem:
- Division Algorithm --- Let ‘$a$’ be an integer and ‘$d$’ a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq+r$.
- It’s really just a theorem, not an algorithm…
  - Only called an “algorithm” for historical reasons.
    - *q* is called the **quotient**
    - *r* is called the **remainder**
    - *d* is called the **divisor**
    - *a* is called the **dividend**

# The Division "Algorithm"

- What are the quotient and remainder when 101 is divided by 11?

$$\begin{array}{l} \ \ a \qquad\quad d \qquad q \quad r \\ 101 = 11 \times 9 + 2 \\ \text{We write:} \\ q = 9 = 101 \ \mathbf{div} \ 11 \\ r = 2 = \ 101 \ \mathbf{mod} \ 11 \end{array}$$

- If $a$ = 7 and $d$ = 3, then $q$ = 2 and $r$ = 1, since 7 = (2)(3) + 1.

  So: given positive **a** and (positive) **d**, in order to get **r** we repeatedly subtract **d** from **a**, as many times as needed so that what remains, **r**, is less than **d**.

- If $a$ = −7 and $d$ = 3, then $q$ = −3 and $r$ = 2, since −7 = (−3)(3) + 2.

  Given negative **a** and (positive) **d**, in order to get **r** we repeatedly add **d** to **a**, as many times as needed so that what remains, **r**, is positive (or zero) and less than **d**.

# Modular Arithmetic

- If $a$ and $b$ are integers and $m$ is a positive integer, then

  ***"a is congruent to b modulo m"*** **if** ***m* divides *a-b***

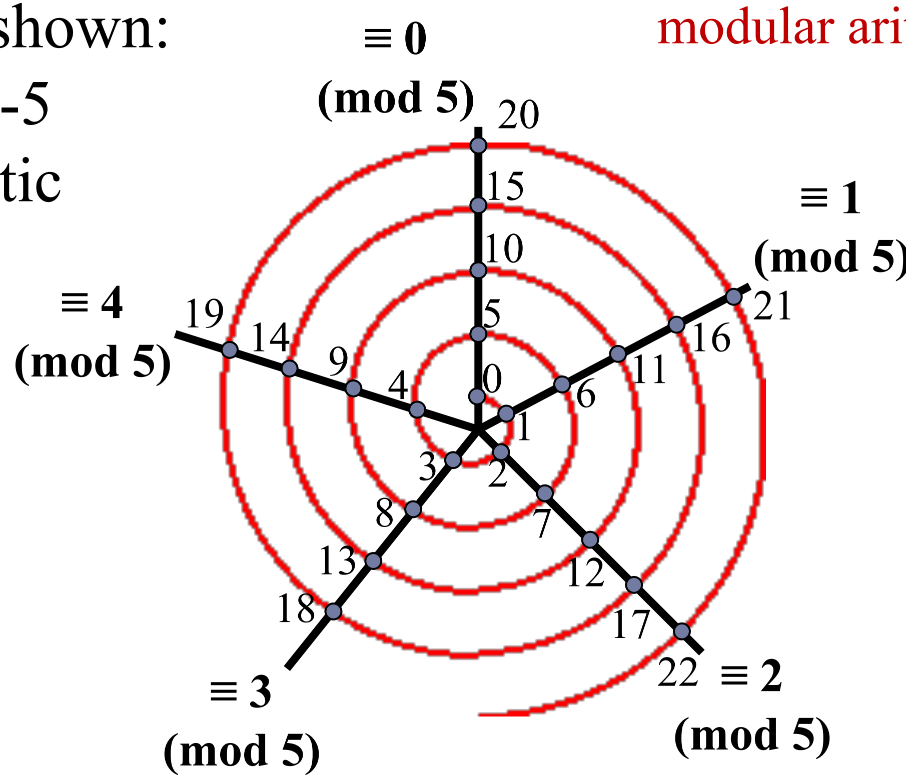
  - Notation: $a \equiv b \pmod{m}$
  - Rephrased: $m \mid a\text{-}b$
  - **Rephrased: $a \bmod m = b \bmod m$**
  - If they are not congruent: $a \not\equiv b \pmod{m}$
- Example: Is 17 congruent to 5 modulo 6?
  - Rephrased: $17 \equiv 5 \pmod{6}$
  - As 6 divides 17-5, they are congruent
- Example: Is 24 congruent to 14 modulo 6?
  - Rephrased: $24 \equiv 14 \pmod{6}$
  - As 6 does not divide 24-14 = 10, they are not congruent

Note: this is a different use of "≡" than the meaning "is defined as" used before.

# Spiral visualization of mod

- Example shown:
  modulo-5
  arithmetic

The spiral/circular view is useful to keep in mind when doing modular arithmetic!




**Congruence classes modulo 5.**

So, e.g., 19 is congruent to 9 modulo 5.

# Properties of Congruence

- Let *a*, *b* and *c* be integers, and let *m* be a positive integer. Then
  - $a \equiv b \pmod{m}$ if and only if $a$ **mod** $m = b$ **mod** $m$
  - $a \equiv b \pmod{m}$ if and only if there is an integer k such that a = b + k*m

    Example: 17 and 5 are congruent modulo 6, so

    17 = 5 + 2*6

    5 = 17 - 2*6
  - If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

    $a+c \equiv (b+d) \pmod{m}$ and $ac \equiv bd \pmod{m}$

    Example

    We know that $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$

    Thus, $7+11 \equiv (2+1) \pmod{5}$, or $18 \equiv 3 \pmod{5}$

    Thus, $7*11 \equiv 2*1 \pmod{5}$, or $77 \equiv 2 \pmod{5}$

# More properties

- If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for any positive integer $n$

Suppose we are asked to find the remainder when $9^{342}$ is divided by 10. Notice that $9^{342}$ is a very big number, so it is not easy to expand this number and then do the division.
So how do we determine the remainder?
Properties of congruence come to our rescue.
From congruence property, we know $9^2 = 1 \pmod{10}$. Then

$$9^{342} = (9^2)^{171} \equiv (1)^{171} \pmod{10} \text{ ,i.e., } 9^{342} \equiv 1 \pmod{10}$$

Exponentiation is performed by repeated multiplication:

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$
$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$
$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

# Modular Arithmetic Operations

- (mod n) operator maps all integers in to {0, 1, 2, …(n-1)}
- Hence, we can perform mathematical operations within the confines of the above set

Modular arithmetic properties:

1. [(a mod n) + (b mod n)] mod n = (a + b) mod n
2. [(a mod n) – (b mod n)] mod n = (a – b) mod n
3. [(a mod n) x (b mod n)] mod n = (a x b) mod n

e.g.

**[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = (11 + 15) mod 8 = 26 mod 8 = 2**

**[(11 mod 8) – (15 mod 8)] mod 8 = –4 mod 8 = (11 – 15) mod 8 = –4 mod 8 = 4**

**[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = (11 x 15) mod 8 = 165 mod 8 = 5**

# Modulo 8 Addition Example

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

# Modulo 8 Multiplication

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

# Modulo 8 Additive and Multiplicative Inverse

The negative of an integer x is the integer y such that
(x + y) mod 8 = 0.

In modular arithmetic mod 8, the multiplicative inverse of x is the integer y such that
(x * y) mod 8 = 1 mod 8

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 7 | 1 |
| 2 | 6 | — |
| 3 | 5 | 3 |
| 4 | 4 | — |
| 5 | 3 | 5 |
| 6 | 2 | — |
| 7 | 1 | 7 |

# Modular Arithmetic Properties

Define the set $Z_n$ as the set of nonnegative integers less than $n$:

$$Z_n = \{0, 1, \ldots, (n - 1)\}$$

This is referred to as the **set of residues**, or **residue classes** (mod $n$). To be more precise, each integer in $Z_n$ represents a residue class. We can label the residue classes (mod $n$) as $[0], [1], [2], \ldots, [n - 1]$, where

$$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$$

The residue classes (mod 4) are

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

Of all the integers in a residue class, the smallest nonnegative integer is the one used to represent the residue class. Finding the smallest nonnegative integer to which $k$ is congruent modulo $n$ is called **reducing $k$ modulo $n$**.

# Modular Arithmetic Properties

Set of residues is defined as Z*n* = {0, 1, Á , (*n* - 1)}

| Property | Expression |
|---|---|
| Commutative Laws | $(w + x) \bmod n = (x + w) \bmod n$<br>$(w \times x) \bmod n = (x \times w) \bmod n$ |
| Associative Laws | $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$<br>$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$ |
| Distributive Law | $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ |
| Identities | $(0 + w) \bmod n = w \bmod n$<br>$(1 \times w) \bmod n = w \bmod n$ |
| Additive Inverse $(-w)$ | For each $w \in Z_n$, there exists a $z$ such that $w + z \equiv 0 \bmod n$ |

# Greatest Common Divisor

- The greatest common divisor of two integers *a* and *b* is the largest integer *d* such that *d* | a and *d* | b
  - Denoted by gcd(a,b)

- Examples
  - gcd (24, 36) = 12
  - gcd (17, 22) = 1
  - gcd (100, 17) = 1

# Relative Primes/Co-primes

- Two numbers are *relatively prime or co-primes* if they don't have any common factors (other than 1)
  - Rephrased: *a* and *b* are relatively prime if gcd (a,b) = 1

- gcd (25, 16) = 1, so 25 and 16 are relatively prime

# Pairwise relatively prime

- A set of integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if, for all pairs of numbers, they are relatively prime
  - Formally: The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- Example: are 10, 17, and 21 pairwise relatively prime?
  - gcd(10,17) = 1, gcd (17, 21) = 1, and gcd (21, 10) = 1
  - Thus, they are pairwise relatively prime
- Example: are 10, 19, and 24 pairwise relatively prime?
  - Since gcd(10,24) ≠ 1, they are not

# More on GCD

- Given two numbers *a* and *b*, rewrite them as:
  - Example: gcd (120, 500)
    - $120 = 2^3 * 3 * 5 = 2^3 * 3^1 * 5^1$
    - $500 = 2^2 * 5^3 = 2^2 * 3^0 * 5^3$
- Then compute the gcd by the following formula:

$$\boxed{\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}}$$

  - Example: $\gcd(120,500) = 2^{\min(3,2)}\, 3^{\min(1,0)}\, 5^{\min(1,3)} = 2^2\, 3^0\, 5^1 = 20$

# Euclid's Algorithm for GCD

- Finding GCDs by comparing prime factorizations can be difficult when the prime factors are not known! And, no fast alg. for factoring is known. (except on quantum computer!)
- **Euclid discovered:** For all ints. $a$, $b$,

$$\mathbf{gcd}(a, b) = \mathbf{gcd}((a \bmod b), b).$$

- Sort $a$,$b$ so that $a>b$, and then (given $b>1$) ($a$ mod $b$) < $a$, so problem is simplified.

Euclid of Alexandria 325-265 B.C.

# Euclid's Algorithm

- For any integers a, b, with $a \geq b \geq 0$,
  - `GCD(a,b)= GCD(b, a mod b)` `//also known as diophantine equation`
- Euclidean Algorithm to compute GCD(a,b) is:

```
Euclid(a,b)  //recursive function
  if(b=0),then return a;
  else return Euclid(b,a mod b);
```

$$\gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$$
$$\gcd(11, 10) = \gcd(10, 1) = \gcd(1, 0) = 1$$

# Euclid's Algorithm Example

<u>Calculate the GCD of 372 and 164</u>

$\gcd(372,164) = \gcd(164, 372 \bmod 164)$.

$372 \bmod 164 = 372-164\lfloor 372/164 \rfloor = 372-164 \cdot 2 = 372-328 = 44$.

$\gcd(164,44) = \gcd(44, 164 \bmod 44)$.

$164 \bmod 44 = 164-44\lfloor 164/44 \rfloor = 164-44 \cdot 3 = 164-132 = 32$.

$\gcd(44,32) = \gcd(32, 44 \bmod 32)$

$= \gcd(32,12) = \gcd(12, 32 \bmod 12)$

$= \gcd(12,8) = \gcd(8, 12 \bmod 8)$

$= \gcd(8,4) = \gcd(4, 8 \bmod 4)$

$= \gcd(4,0) = 4$.

- So, we repeatedly swap the numbers. Largest first. "mod" reduces them quickly!
- ***Complexity: O(log b) divisions. Linear in #digits of b!***

# Extended Euclidean Algorithm

- For given integers a and b, the extended Euclidean algorithm not only calculate the greatest common divisor d but also two additional integers x and y that satisfy the following equation:

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

- It should be clear that x and y will have opposite signs.
- Useful for later crypto calculations
- Follow sequence for division of gcd but assume at each step i, we can find x & y:

$$r_i = ax + by$$

- If GCD(a,b) = 1, these values are inverses.

# Extended Euclidean Algorithm

| Extended Euclidean Algorithm | | | |
|---|---|---|---|
| **Calculate** | **Which satisfies** | **Calculate** | **Which satisfies** |
| $r_{-1} = a$ | | $x_{-1} = 1; y_{-1} = 0$ | $a = ax_{-1} + by_{-1}$ |
| $r_0 = b$ | | $x_0 = 0; y_0 = 1$ | $b = ax_0 + by_0$ |
| $r_1 = a \bmod b$<br>$q_1 = \lfloor a/b \rfloor$ | $a = q_1 b + r_1$ | $x_1 = x_{-1} - q_1 x_0 = 1$<br>$y_1 = y_{-1} - q_1 y_0 = -q_1$ | $r_1 = ax_1 + by_1$ |
| $r_2 = b \bmod r_1$<br>$q_2 = \lfloor b/r_1 \rfloor$ | $b = q_2 r_1 + r_2$ | $x_2 = x_0 - q_2 x_1$<br>$y_2 = y_0 - q_2 y_1$ | $r_2 = ax_2 + by_2$ |
| $r_3 = r_1 \bmod r_2$<br>$q_3 = \lfloor r_1/r_2 \rfloor$ | $r_1 = q_3 r_2 + r_3$ | $x_3 = x_1 - q_3 x_2$<br>$y_3 = y_1 - q_3 y_2$ | $r_3 = ax_3 + by_3$ |
| •<br>•<br>• | •<br>•<br>• | •<br>•<br>• | •<br>•<br>• |
| $r_n = r_{n-2} \bmod r_{n-1}$<br>$q_n = \lfloor r_{n-2}/r_{n-1} \rfloor$ | $r_{n-2} = q_n r_{n-1} + r_n$ | $x_n = x_{n-2} - q_n x_{n-1}$<br>$y_n = y_{n-2} - q_n y_{n-1}$ | $r_n = ax_n + by_n$ |
| $r_{n+1} = r_{n-1} \bmod r_n = 0$<br>$q_{n+1} = \lfloor r_{n-1}/r_n \rfloor$ | $r_{n-1} = q_{n+1} r_n + 0$ | | $d = \gcd(a, b) = r_n$<br>$x = x_n; y = y_n$ |

# Extended Euclidean Algorithm

- As an example, let us use a = 1759 and b = 550 and solve for 1759x + 550y = gcd(1759, 550).
- The results are shown in the table.
- Thus, we have
- 1759 * (-111) + 550 * 355= -195249 + 195250 = 1

| $i$ | $r_i$ | $q_i$ | $x_i$ | $y_i$ |
|---|---|---|---|---|
| −1 | 1759 | | 1 | 0 |
| 0 | 550 | | 0 | 1 |
| 1 | 109 | 3 | 1 | −3 |
| 2 | 5 | 5 | −5 | 16 |
| 3 | 4 | 21 | 106 | −339 |
| 4 | 1 | 1 | −111 | 355 |
| 5 | 0 | 4 | | |

Result: $d = 1; x = -111; y = 355$

# Groups, Rings and Fields

- Groups, Rings and Fields are fundamental elements of modern or abstract algebra
- In abstract algebra, we operate algebraically on a set of elements
- We can combine two elements of the set, in several ways, to obtain a third element of the set.
- These operations are subject to specific rules
- In abstract algebra, we are not limited to ordinary arithmetical operations.

# Group

- a Group G is a set of elements or "numbers"
  - may be finite or infinite
- with a binary operation '.' denoted {G,.}
- Obeys the following axioms:
  - Closure: if $a, b \in G$, then $a.b \in G$
  - Associative law: $(a.b).c = a.(b.c)$
  - has Identity $e$: $e.a = a.e = a$
  - has inverses $a^{-1}$: $a.a^{-1} = a^{-1}.a = e$
- if commutative $a.b = b.a$
  - then forms an **abelian group**

# Abelian Group

- In mathematics, 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, the group operation is commutative.

# Cyclic Group

- We define exponentiation as repeated application of operator
  - example: $a^3 = a.a.a$
- Identity element defined as: $e = a^0$
- $a^{-n} = (a')^n$ where $a'$ is the inverse element of $a$ in the group
- a group is **cyclic** if every element is a power of some fixed element $a$
  - i.e., $b = a^k$ for some $a$ and every $b$ in group
- $a$ is said to be a generator of the group
- cyclic group is always abelian

# Ring

- Denoted by {R,+, .} is a set of "numbers" with two binary operations (addition and multiplication) which obeys the following axioms:
  - an abelian group with addition operation
  - Closure under multiplication: If $a$ and $b \in R$ then $ab \in R$
  - Associative under multiplication: $a(bc) = (ab)c$ for all $a$, $b$, $c$ in $R$
  - distributive over addition: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- if multiplication operation is commutative ab = $ba$, it forms a **commutative ring**
- Ring is a set in which we can do addition, subtraction [$a - b = a + (-b)$], and multiplication without leaving the set

# Field

- A Field F, denoted by {$F$, +, x } is a set of elements with two operations called addition and multiplication (ignoring 0)
- Division is defined by $a/b = a\,(b^{-1})$.
- Examples of field: rational numbers, real numbers, complex numbers
- have hierarchy with more axioms/laws
  - group -> ring -> field

# Example of Boolean field

**Definition 2.1.1** A **field** is a set $F$ which has two binary operations, denoted $+$ and $\cdot$, satisfying the following properties. For all $a, b, c \in F$, we have

1. $a+b=b+a$, (``addition is commutative")
2. $a \cdot b = b \cdot a$, (``multiplication is commutative")
3. $(a+b)+c=a+(b+c)$, (``addition is associative")
4. $(a \cdot b)c = a(b \cdot c)$, (``multiplication is associative")
5. $(a+b) \cdot c = a \cdot c + b \cdot c$, (``distributive")
6. there is an element $1 \in F$ such that $a \cdot 1 = a$, (`` $1$ is a multiplicative identity")
7. there is an element $0 \in F$ such that $a+0=a$ (``0 is a additive identity"),
8. if $a \neq 0$ then there is an element, denoted $a^{-1}$, such that $a \cdot a^{-1} = 1$ (``the inverse of any non-zero element exists").

# Group,Ring and Field

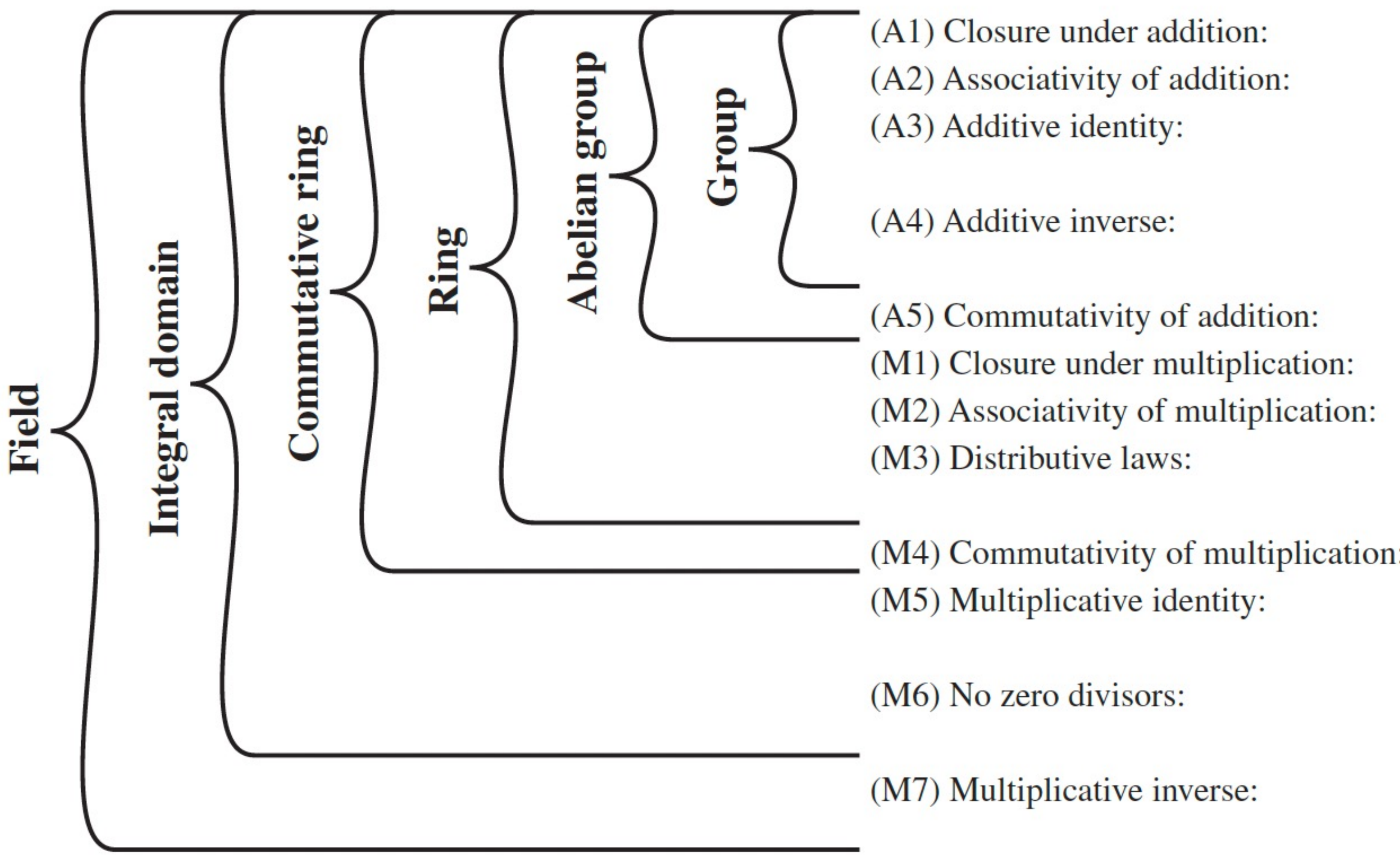



**Figure 4.2** Groups, Ring, and Field

# Finite (Galois) Fields

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime $p^n$ known as Galois fields, denoted GF($p^n$)
- in particular often use the fields:
  - GF(p)
  - GF($2^n$)

# Galois Fields GF(p)

- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- and can do addition, subtraction, multiplication, and division without leaving the field GF(p)
- GF(2) = Mod 2 arithmetic
- GF(8) = Mod 8 arithmetic
- AES uses arithmetic in the finite field GF($2^8$ ) with irreducible (prime) polynomial. $m(x) = x^8 + x^4 + x^3 + x + 1$ which is

  (1 0001 1011) in binary or {11B} in Hex-decimal
- Irreducible polynomial is a polynomial that is not a product of two other polynomials.

# GF(2) arithmetic operations

The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Addition

| $\times$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Multiplication

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 1 | 1 |

Inverses

In this case, addition is equivalent to the exclusive-OR (XOR) operation, and multiplication is equivalent to the logical AND operation.

# GF(7) Multiplication Example

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

# Polynomial Arithmetic

- can compute using polynomials *in a single variable x*

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$

- Three classes of polynomial arithmetic
  - ordinary polynomial arithmetic, using the basic rule of algebra
  - Polynomial arithmetic in which the arithmetic on the coefficients is performed modulo *p* ; that is, the coefficients are in GF(*p*).
  - Polynomial arithmetic in which the coefficients are in GF(*p*), and the polynomials are defined modulo *a* polynomial *m*(*x*) whose highest power is some integer *n*.

# Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg

$$
\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
+ \; (x^2 - x + 1) \\
\hline
x^3 + 2x^2 - x + 3
\end{array}
$$

**(a) Addition**

$$
\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
- \; (x^2 - x + 1) \\
\hline
x^3 \qquad + x + 1
\end{array}
$$

**(b) Subtraction**

$$
\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
\times \; (x^2 - x + 1) \\
\hline
x^3 + x^2 \qquad + 2 \\
-x^4 - x^3 \qquad - 2x \qquad \\
x^5 + x^4 \qquad + 2x^2 \qquad\qquad \\
\hline
x^5 \qquad\qquad + 3x^2 - 2x + 2
\end{array}
$$

**(c) Multiplication**

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

**(d) Division**

**Figure 4.3** Examples of Polynomial Arithmetic

# Polynomial Arithmetic with Modulo Coefficients

- when computing value of each coefficient do calculation modulo some value
  - forms a polynomial ring
- could be modulo any prime
- but we are most interested in mod 2
  - ie all coefficients are 0 or 1
  - eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$$f(x) + g(x) = x^3 + x + 1$$

$$f(x) \text{ x } g(x) = x^5 + x^2$$

# Polynomial arithmetic over GF(2)

$$\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
+ (x^3 + x + 1) \\ \hline
x^7 + x^5 + x^4
\end{array}$$

**(a) Addition**

$$\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
- (x^3 + x + 1) \\ \hline
x^7 + x^5 + x^4
\end{array}$$

**(b) Subtraction**

$$\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\times (x^3 + x + 1) \\ \hline
x^7 + x^5 + x^4 + x^3 + x + 1 \\
x^8 + x^6 + x^5 + x^4 + x^2 + x \\
x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 \\ \hline
x^{10} + x^4 + x^2 + 1
\end{array}$$

**(c) Multiplication**

$$\begin{array}{r|l}
 & x^4 + 1 \\ \hline
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\ \hline
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\ \hline
\end{array}$$

**(d) Division**

# Modular Polynomial Arithmetic

- can compute in field $GF(2^n)$
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- form a finite field
- can always find an inverse
  - can extend Euclid's Inverse algorithm to find

# Example GF($2^3$)

**Table 4.7** Polynomial Arithmetic Modulo $(x^3 + x + 1)$

| | + | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|---|
| | | $0$ | $1$ | $x$ | $x + 1$ | $x^2$ | $x^2 + 1$ | $x^2 + x$ | $x^2 + x + 1$ |
| 000 | $0$ | $0$ | $1$ | $x$ | $x + 1$ | $x^2$ | $x^2 + 1$ | $x^2 + 1$ | $x^2 + x + 1$ |
| 001 | $1$ | $1$ | $0$ | $x + 1$ | $x$ | $x^2 + 1$ | $x^2$ | $x^2 + x + 1$ | $x^2 + x$ |
| 010 | $x$ | $x$ | $x + 1$ | $0$ | $1$ | $x^2 + x$ | $x^2 + x + 1$ | $x^2$ | $x^2 + 1$ |
| 011 | $x + 1$ | $x + 1$ | $x$ | $1$ | $0$ | $x^2 + x + 1$ | $x^2 + x$ | $x^2 + 1$ | $x^2$ |
| 100 | $x^2$ | $x^2$ | $x^2 + 1$ | $x^2 + x$ | $x^2 + x + 1$ | $0$ | $1$ | $x$ | $x + 1$ |
| 101 | $x^2 + 1$ | $x^2 + 1$ | $x^2$ | $x^2 + x + 1$ | $x^2 + x$ | $1$ | $0$ | $x + 1$ | $x$ |
| 110 | $x^2 + x$ | $x^2 + x$ | $x^2 + x + 1$ | $x^2$ | $x^2 + 1$ | $x$ | $x + 1$ | $0$ | $1$ |
| 111 | $x^2 + x + 1$ | $x^2 + x + 1$ | $x^2 + x$ | $x^2 + 1$ | $x^2$ | $x + 1$ | $x$ | $1$ | $0$ |

**(a) Addition**

| | × | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|---|
| | | $0$ | $1$ | $x$ | $x + 1$ | $x^2$ | $x^2 + 1$ | $x^2 + x$ | $x^2 + x + 1$ |
| 000 | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| 001 | $1$ | $0$ | $1$ | $x$ | $x + 1$ | $x^2$ | $x^2 + 1$ | $x^2 + x$ | $x^2 + x + 1$ |
| 010 | $x$ | $0$ | $x$ | $x^2$ | $x^2 + x$ | $x + 1$ | $1$ | $x^2 + x + 1$ | $x^2 + 1$ |
| 011 | $x + 1$ | $0$ | $x + 1$ | $x^2 + x$ | $x^2 + 1$ | $x^2 + x + 1$ | $x^2$ | $1$ | $x$ |
| 100 | $x^2$ | $0$ | $x^2$ | $x + 1$ | $x^2 + x + 1$ | $x^2 + x$ | $x$ | $x^2 + 1$ | $1$ |
| 101 | $x^2 + 1$ | $0$ | $x^2 + 1$ | $1$ | $x^2$ | $x$ | $x^2 + x + 1$ | $x + 1$ | $x^2 + x$ |
| 110 | $x^2 + x$ | $0$ | $x^2 + x$ | $x^2 + x + 1$ | $1$ | $x^2 + 1$ | $x + 1$ | $x$ | $x^2$ |
| 111 | $x^2 + x + 1$ | $0$ | $x^2 + x + 1$ | $x^2 + 1$ | $x$ | $1$ | $x^2 + 1$ | $x^2$ | $x + 1$ |

**(b) Multiplication**

# Computational Considerations

- since coefficients are 0 or 1, can represent any such polynomial as a bit string
- addition becomes XOR of these bit strings
- multiplication is shift & XOR
  - cf long-hand multiplication
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift & XOR)

# Computational Example

- in $GF(2^3)$ have $(x^2+1)$ is $101_2$ & $(x^2+x+1)$ is $111_2$
- so addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- and multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$

    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101){<<}1 \text{ XOR } (101){<<}0 =$

    $1010 \text{ XOR } 101 = 1111_2$

# Computational Example (con't)

- in GF($2^3$) have ($x^2+1$) is $101_2$ & ($x^2+x+1$) is $111_2$
- polynomial modulo reduction (get q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$

# GCD of Polynomials

| Euclidean Algorithm for Polynomials | |
|---|---|
| **Calculate** | **Which satisfies** |
| $r_1(x) = a(x) \bmod b(x)$ | $a(x) = q_1(x)b(x) + r_1(x)$ |
| $r_2(x) = b(x) \bmod r_1(x)$ | $b(x) = q_2(x)r_1(x) + r_2(x)$ |
| $r_3(x) = r_1(x) \bmod r_2(x)$ | $r_1(x) = q_3(x)r_2(x) + r_3(x)$ |
| • <br> • <br> • | • <br> • <br> • |
| $r_n(x) = r_{n-2}(x) \bmod r_{n-1}(x)$ | $r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x)$ |
| $r_{n+1}(x) = r_{n-1}(x) \bmod r_n(x) = 0$ | $r_{n-1}(x) = q_{n+1}(x)r_n(x) + 0$ <br> $d(x) = \gcd(a(x), b(x)) = r_n(x)$ |

# GCD of Polynomials

Find $\gcd[a(x), b(x)]$ for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$. First, we divide $a(x)$ by $b(x)$:

$$
\begin{array}{r|l}
 & x^2 + x \\
\hline
x^4 + x^2 + x + 1 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & \underline{x^6 \qquad\; + x^4 + x^3 + x^2} \\
 & \qquad x^5 \qquad\qquad\qquad\quad + x + 1 \\
 & \qquad \underline{x^5 \qquad\; + x^3 + x^2 + x \quad\;\;} \\
 & \qquad\qquad\quad x^3 + x^2 \qquad + 1
\end{array}
$$

This yields $r_1(x) = x^3 + x^2 + 1$ and $q_1(x) = x^2 + x$.
Then, we divide $b(x)$ by $r_1(x)$.

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
x^3 + x^2 + 1 & x^4 \qquad\; + x^2 + x + 1 \\
 & \underline{x^4 + x^3 \qquad\; + x} \\
 & \qquad x^3 + x^2 \qquad + 1 \\
 & \qquad \underline{x^3 + x^2 \qquad + 1}
\end{array}
$$

This yields $r_2(x) = 0$ and $q_2(x) = x + 1$.
Therefore, $\gcd[a(x), b(x)] = r_1(x) = x^3 + x^2 + 1$.