# Cryptography and Security

## Lecture 4

## Basic Concepts in Number Theory and Finite Fields

# Greatest Common Divisor

- A positive integer ***c*** is the greatest common divisor of ***a*** and ***b*** if
  - ***c*** is a divisor of ***a*** and ***b***.
  - Any divisor of ***a*** and ***b*** is a divisor of ***c***.
  - gcd(***a, b***) = max[***k***, such that ***k|a*** and ***k|b***]
- gcd (***a, b***) = gcd(|***a***|,|***b***|)
- gcd(***a,0***)=|***a***|.
- Two integers are relatively prime if their only common positive integer factor is 1. i.e, ***a*** and ***b*** are relatively prime if ***gcd(a,b)=1***.

# The Euclidean Algorithm

$$\left.\begin{array}{ll}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\quad\vdots & \quad\vdots \\
r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_{n+1} r_n + 0 & \\
d = \gcd(a, b) = r_n &
\end{array}\right\}$$

- gcd(10,63):

63=10.6+3

10=3.3+1

3=3.1+0

- gcd(1701,3768):

3768=1701.2+366

1701=366.4+237

366=237.1+129

237=129.1+108

129=108.1+21

108=21.5+3→gcd(1701,3768)

21=3.7+0

# Modular Arithmetic

- For an integer $a$ and $n$ is a positive integer, $a \bmod n$ is the remainder when $a$ is divided by $n$. The integer $n$ is called the modulus.

  $a = qn + r \Rightarrow a = \text{floor}(a/n) \times n + a \bmod n$

- Two integer $a$ and $b$ are said to be **congruent modulo** $n$, if $(a \bmod n) = (b \bmod n) \rightarrow a \equiv b \pmod{n}$

# Modular Arithmetic Operations

- Arithmetic operation on the set of integers [0, 1, 2, 3, …, (n-1)].

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

$11 \bmod 8 = 3; 15 \bmod 8 = 7$
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$
$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$
$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$
$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

# Modular Arithmetic Operations

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

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

**Modulo 8 Addition**

| + | 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 |

# Properties of Modular Arithmetic

- ***Z*** = Set of all integers = ***{…, -2, -1, 0, 1, 2, …***}
- $Z_n$ = Set of all non-negative integers less than ***n*** = {***0, 1, 2, …, (n-1)***}
- $Z_2 = \{0, 1\}$
- $Z_8 = \{ 0, 1, 2, 3, 4, 5, 6, 7\}$
- $Z_n$ = set of residues or residue classes (mod n)
- ***Residue class [r]=[a:a is an integer, aΞr (mod n)***

The residue classes (mod 4) are

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

# Properties of Modular Arithmetic in $Z_n$

| Property | Expression |
|---|---|
| Commutative Laws | $(w + x) \bmod n = (x + w) \bmod n$<br>$(w \times x) \bmod n = (x + w) \bmod n$ |
| 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 $a\ z$ such that $w + z = 0 \bmod n$ |

# Properties of Modular Arithmetic

- **Additive Inverse**

if $(a + b) \equiv (a + c) \pmod{n}$ then $b \equiv c \pmod{n}$

$$\boxed{(5 + 23) \equiv (5 + 7)(\bmod 8);\ 23 \equiv 7(\bmod 8)}$$

$$((-a) + a + b) \equiv ((-a) + a + c)(\bmod n)$$
$$b \equiv c \ (\bmod n)$$

- **Multiplicative Inverse**

if $(a \times b) \equiv (a \times c)(\bmod n)$ then $b \equiv c \ (\bmod n)$ if $a$ is relatively prime to $n$

$$6 \times 3 = 18 \equiv 2(\bmod 8)$$
$$6 \times 7 = 42 \equiv 2(\bmod 8)$$

Yet $3 \not\equiv 7 \ (\bmod 8)$.

If ***a*** and ***n*** have common factor, for a modulus ***n*** and a multiplier ***a*** fails to produce a complete set of residues.

# Properties of Modular Arithmetic

With $a = 6$ and $n = 8$,

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $Z_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Multiply by 6 | 0 | 6 | 12 | 18 | 24 | 30 | 36 | 42 |
| Residues | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |

Because we do not have a complete set of residues when multiplying by 6, more than one integer in $Z_8$ maps into the same residue. Specifically, $6 \times 0 \bmod 8 = 6 \times 4 \bmod 8$; $6 \times 1 \bmod 8 = 6 \times 5 \bmod 8$; and so on. Because this is a many-to-one mapping, there is not a unique inverse to the multiply operation.

However, if we take $a = 5$ and $n = 8$, whose only common factor is 1,

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $Z_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Multiply by 5 | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 |
| Residues | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |

The line of residues contains all the integers in $Z_8$, in a different order.

# Euclidean Algorithm Revisited

- For any integer ***a>=0*** and ***b>=0***, gcd(***a, b***) = gcd(***b, a mod b***)
- gcd (55, 22) = gcd(22, 55 mod 22) = gcd (22,11)=11.
- gcd(18,12)=gcd(12, 6)=gcd(6,0)=6.

  - gcd(1701,3768):

| | |
|---|---|
| 3768=1701.2+366 | gcd(1701,366) |
| 1701=366.4+237 | gcd(366,237) |
| 366=237.1+129 | gcd(237,129) |
| 237=129.1+108 | gcd(129,108) |
| 129=108.1+21 | gcd(108,21) |
| 108=21.5+3 | gcd(21,3) |
| 21=3.7+0 | gcd(3,0) $\rightarrow$gcd(1701,3768) |

# The Extended Euclidean Algorithm

- Get not only GCD but $\boldsymbol{x}$ and $\boldsymbol{y}$ such that $\boldsymbol{ax + by} = \boldsymbol{d} =$ GCD($\boldsymbol{a,b}$)
- useful for latter crypto computations
- follow sequence of divisions for GCD but at each step i, keep track of $\boldsymbol{x}$ and $\boldsymbol{y}$ such that $\boldsymbol{r = ax + by}$
- at the end find GCD value and also $\boldsymbol{x}$ and $\boldsymbol{y}$

# The Extended Euclidean Algorithm--Example

- gcd(888,54)=6 $\longrightarrow$ 6 = 54. (33)+ 888 (-2)

  888 = 54.16+24 $\longrightarrow$ 6 = 54 + ( 888 + 54(-16)) (-2)

  54= 24. 2+ 6 $\longrightarrow$ 6= 54+24 (-2)

  24=6. 4 + 0
- gcd(888,54) = 6 = 888***x***+ 54***y*** where ***x*** = -2 and ***y***=33
- Try gcd(56,15) in class; result 15.15+56.(-4)=1

# Multiplicative Inverse using Extended Euclidean Algorithm

- Used to find a multiplicative inverse in $Z_n$ for any $n$.
- If extended euclidean algorithm is applied to $nx+by=d$ and the algorithm yields $d=1$, then $y=b^{-1}$ in $Z_n$.
- ***Example:***

  Gcd(56,15) =1 $\longrightarrow$ 15.15+56.(-4)=1

  i.e, $a$=56, $x$=-4, $b$=15 and $y$=15.

  $b^{-1}$=$y$=15 in $Z_{56}$ $\longrightarrow$ 15×15 mod 56 = 1.

# Group

- **Group**:

A set of elements that is closed with respect to a binary operation denoted by {G, •}.

- Closed ⇒ The result of the operation is also in the set.
- The operation obeys:
  - Closure: if ***a*** and ***b*** belong to G, then ***a.b*** is also in G.
  - Associative law: ***(a.b).c = a.(b.c)***
  - Identity element: Has identity ***e***: ***e.a = a.e = a***
  - Inverse element: Has inverses $\boldsymbol{a^{-1}}$: $\boldsymbol{a.a^{-1} = e}$

- **Abelian Group:**
  - commutative a.b = b.a
  - Example: $Z_8$, + modular addition, identity =0
  - Order of a finite group is the number of elements in that group.

# Cyclic Group

- **Exponentiation:**

  Repeated application of operator

  example: $a^3 = a.a.a$

- **Cyclic Group:**
  - Every element is a power of some fixed element,i.e, $b = a^k$ for some ***a*** and every ***b*** in group.
  - ***a*** is said to be a generator of the group
  - Example: {1, 2, 4, 8} with mod 12 multiplication, the generator is 2.
  - $2^0=1$, $2^1=2$, $2^2=4$, $2^3=8$, $2^4=4$, $2^5=8$
  - A cyclic group is always abelian and may be finite or infinite.
  - The additive group of integers is an infinite cyclic group generated by 1.

# Ring

- **Ring**:
  - A set with two operations: addition and multiplication, denoted by {R, +, ×}
  - Abelian group with respect to addition: ***a+b = b+a***
  - Closed under multiplication. → for ***a, b ϵ R***, ***a.b*** is also in ***R***.
  - Associativity of multiplication. → ***a.(b.c)=(a.b).c***
  - Multiplication distributes over addition→ ***a.(b+c)=a.b+a.c and (a+b).c = a.c + b.c***
- **Commutative Ring:**

  Multiplication is commutative → ***a.b = b.a***
- **Example:**

  $Z_8$, +, × is a commutative ring.

# Ring

- **Integral Domain:**

  multiplication operation has an identity and no zero divisors

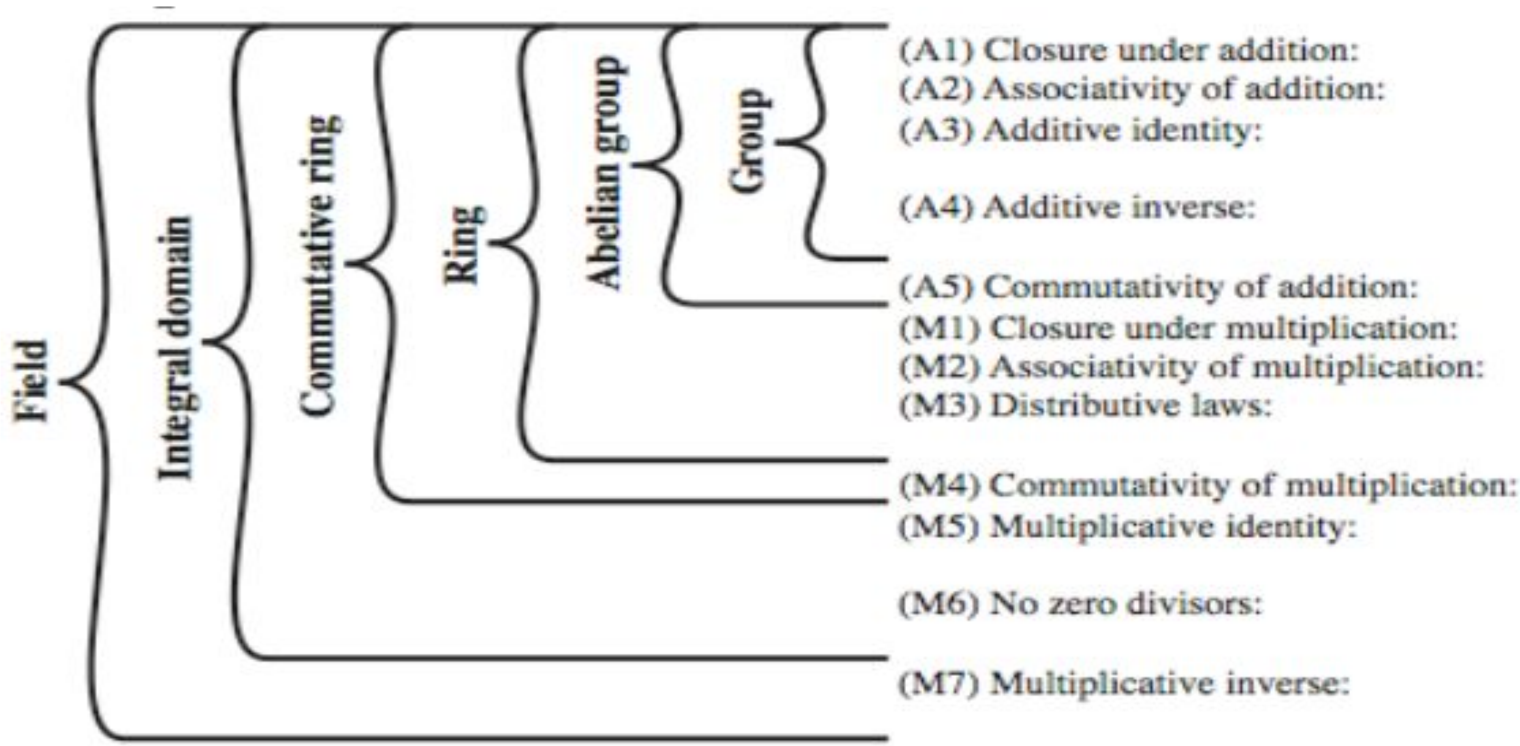
  - There is an element 1 such that a1 = 1a =a for all a R.
  - If ***a, b ϵ R*** and ***ab=0***, then either ***a=0*** or ***b=0***.

- **Example:**

The set of integers (positive, negative and 0) under the usual operation of addition and multiplication.

# Field

- An integral domain in which each element has a multiplicative inverse.




- The set of all real numbers under the operation of addition and multiplication is an example of field.
- In field we can do addition, subtraction, multiplication and division $\longrightarrow$ $a/b = a(b^{-1})$

# Finite Field or Galois Field

- **Finite Field**:
  - A field with finite number of elements.
  - Also known as Galois Field.
  - The number of elements is always a power (positive integer) of a prime number. Hence, denoted as ***GF($p^n$)***
  - ***GF(p)*** is the set of integers, $Z_p$ ={0,1, … , p-1} with arithmetic operations modulo prime p.
  - Can do addition, subtraction, multiplication, and division without leaving the field ***GF(p)***

# Finite Field or Galois Field

- Any integer in $Z_n$ has a multiplicative inverse if and only if that integer is relatively prime to ***n***.
- There exists a multiplicative inverse for all of the nonzero integers in $Z_p$.
- $Z_p$ is a field

| | |
|---|---|
| Multiplicative inverse ($w^{-1}$) | For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod{p}$ |

- For $Z_p$ the following equation holds.

$$\textbf{if } (a \times b) \equiv (a \times c) \pmod{p} \textbf{ then } b \equiv c \pmod{p}$$

When ***a*** is a relatively prime to ***p***.

# GF(2)

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

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

Addition

| × | 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)

Table 4.5 Arithmetic in GF(7)

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

(a) Addition modulo 7

| × | 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 |

(b) Multiplication modulo 7

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

(c) Additive and multiplicative inverses modulo 7

# Ordinary Polynomial Arithmetic

- A polynomial of degree n (n>=0) is an expression

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

  where, S = a set of coefficients and $a_n \neq 0$
- Ordinary polynomial arithmetic includes addition, subtraction and multiplication.
- Division operation requires S to be a **field**.
- Example:

  let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

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

  $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

# Ordinary Polynomial Arithmetic

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

# Polynomial Arithmetic with Coefficients in $Z_p$

- When polynomial arithmetic is performed on polynomials over a field, then division is possible.
- Example:
  - If coefficients are integers, then $(5x^2/3x) \rightarrow$ does not have solution.
  - If coefficients are from $Z_7$, then $(5x^2/3x) \rightarrow 4x$.
- Given polynomials $f(x)$ of degree $n$ and $g(x)$ of $m$ $(n>=m)$, we can write $f(x) = q(x)g(x)+r(x)$

where

$deg(f(x))=n$

$deg(g(x))=m$

$deg(q(x))=n-m$

$deg(r(x))<=m-1$

# Polynomial Arithmetic with Coefficients in $Z_p$

- A polynomial $f(x)$ over a field $F$ is irreducible if and only if $f(x)$ cannot be expressed as a product of two polynomials, both over $F$ and both of degree lower than that of $f(x)$.
- Example: [$F=GF(2)$]

  $f(x) = x^3+x+1$ is a irreducible polynomial.

# 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**

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\
\cline{2-2}
\end{array}
$$

# Polynomial GCD

- Polynomial c(x) is the greatest common divisor of a(x) and b(x) if :
  - c(x) divides both a(x) and b(x)
  - Any divisor of a(x) and b(x) is a divisor of c(x)
  - c(x) is the polynomial of maximum degree that divides both a(x) and b(x).

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 $b(x)$:

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

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

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

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

# Motivation for Finite Field of Form GF($2^n$)

- All encryption algorithm requires arithmetic operations on integers.
- Need integers in the range ***0*** through ***$2^n$-1***, which fit into an ***n***-bit word with no wasted bit patterns.

> Suppose we wish to define a conventional encryption algorithm that operates on data 8 bits at a time, and we wish to perform division. With 8 bits, we can represent integers in the range 0 through 255. However, 256 is not a prime number, so that if arithmetic is performed in $Z_{256}$ (arithmetic modulo 256), this set of integers will not be a field. The closest prime number less than 256 is 251. Thus, the set $Z_{251}$, using arithmetic modulo 251, is a field. However, in this case the 8-bit patterns representing the integers 251 through 255 would not be used, resulting in inefficient use of storage.

- The set of integers modulo ***$2^n$*** is not a field. Even if only addition and multiplication are required, the use of ***$Z_{2n}$*** is not good choice.

# Motivation for Finite Field of Form $GF(2^n)$

| | | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|---|
| | + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 000 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 001 | 1 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| 010 | 2 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| 011 | 3 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| 100 | 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 101 | 5 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| 110 | 6 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| 111 | 7 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

(a) Addition

| | | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|---|
| | × | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 000 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 001 | 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 010 | 2 | 0 | 2 | 4 | 6 | 3 | 1 | 7 | 5 |
| 011 | 3 | 0 | 3 | 6 | 5 | 7 | 4 | 1 | 2 |
| 100 | 4 | 0 | 4 | 3 | 7 | 6 | 2 | 5 | 1 |
| 101 | 5 | 0 | 5 | 1 | 4 | 2 | 7 | 3 | 6 |
| 110 | 6 | 0 | 6 | 7 | 1 | 5 | 3 | 2 | 4 |
| 111 | 7 | 0 | 7 | 5 | 2 | 1 | 6 | 4 | 3 |

(b) Multiplication

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

(c) Additive and multiplicative inverses

| Integer | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Occurrences in $Z_8$ | 4 | 8 | 4 | 12 | 4 | 8 | 4 |
| Occurrences in $GF(2^3)$ | 7 | 7 | 7 | 7 | 7 | 7 | 7 |

# Modular Polynomial Arithmetic

- ***S*** = set of all polynomials of degree n-1 or less over $Z_p$ where coefficients are taken from {0,1,….,p-1}. There are a total of $p^n$ polynomials in ***S***.

For $p = 3$ and $n = 2$, the $3^2 = 9$ polynomials in the set are

| | | |
|---|---|---|
| $0$ | $x$ | $2x$ |
| $1$ | $x + 1$ | $2x + 1$ |
| $2$ | $x + 2$ | $2x + 2$ |

For $p = 2$ and $n = 3$, the $2^3 = 8$ polynomials in the set are

| | | |
|---|---|---|
| $0$ | $x + 1$ | $x^2 + x$ |
| $1$ | $x^2$ | $x^2 + x + 1$ |
| $x$ | $x^2 + 1$ | |

- ***S*** is a finite field, where
  - Arithmetic follows the ordinary rules of polynomial arithmetic.
  - Arithmetic on coefficients is performed modulo p.
  - If a polynomial of degree greater than n-1 is generated from multiplication, then the polynomial is reduced modulo some irreducible m(x) of degree n.

# Modular Polynomial Arithmetic

The Advanced Encryption Standard (AES) uses arithmetic in the finite field GF($2^8$), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$$\begin{aligned} f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\ &= x^7 + x^6 + x^4 + x^2 \end{aligned}$$

$$\begin{aligned} f(x) \times g(x) = {} & x^{13} + x^{11} + x^9 + x^8 + x^7 \\ & + x^7 + x^5 + x^3 + x^2 + x \\ & + x^6 + x^4 + x^2 + x + 1 \\ = {} & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{array}{r} x^5 + x^3 \\ x^8 + x^4 + x^3 + x + 1 \overline{\big)\, x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1} \\ \underline{x^{13} \qquad + x^9 + x^8 \qquad + x^6 + x^5} \qquad\qquad \\ x^{11} \qquad\qquad\qquad\qquad + x^4 + x^3 \quad \\ \underline{x^{11} \qquad\qquad + x^7 + x^6 \qquad + x^4 + x^3} \quad \\ x^7 + x^6 \qquad\qquad\qquad + 1 \end{array}$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

# Modular Polynomial Arithmetic

- The set of residues modulo ***m(x)***, an ***n***th degree polynomial, consists of $\boldsymbol{p^n}$ elements where each of the elements is represented by one of the $\boldsymbol{p^n}$ polynomials of degree ***m<n = S***.
- Example GF($2^3$)

**Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)**

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

**(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 and XOR
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift and XOR)
- eg. irreducible poly = $x^3 + x + 1$ **means** $x^3 = x + 1$ in the polynomial field

# 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
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x + x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101){<<}1 \text{ XOR } (101){<<}0 =$
    $1010 \text{ XOR } 0101 = 1111_2$
- polynomial modulo reduction (to get $q(x)$ & $r(x)$)
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$

- Basic concepts in number theory and finite fields from the book of William Stallings (Chapter 2 and Chapter 5).
- Also refer to various youtube clips on the discussed topic.