Introduction to Information Security (Spring 2023)

Ashok Kumar Das

Associate Professor
IEEE Senior Member
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad (IIIT Hyderabad)

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

Mathematical Preliminaries for Advanced Encryption Standard (AES): Modular Arithmetic and Finite Fields

Group

Definition

A group $(G, \circ)$ is a set of elements with a binary operation $\circ$ that associates to each ordered pair (a, b) of elements of G to an element $a \circ b$ in G, such that the following axioms are obeyed:

- **(A1) Closure:** If $a, b \in G$, then $a \circ b \in G$.
- **(A2) Associativity:** If $a, b, c \in G$, then $a \circ (b \circ c) = (a \circ b) \circ c$.
- **(A3) Identity Element:** $\forall a \in G, \exists e \in G$ such that $e \circ a = a \circ e = a$.
  $e \in G$ is called the identity (left as well as right) of G.
- **(A4) Inverse Element:** For each $a \in G$, there exists an $a^{-1} \in G$, such that $a^{-1} \circ a = a \circ a^{-1} = e$.
  a^{-1} is called the inverse (left as well as right inverse) element in G.

Group

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Definition

A group $(G, \circ)$ is said to be an *abelian* (or commutative) if it satisfies the additional condition:

- **(A5) Commutative:** $a \circ b = b \circ a, \forall a, b \in G$.

Ring and Field

Definition (Ring)

A ring R, sometimes denoted by $(R, \circ, *)$ is a set of elements with two binary operations, $\circ$ (e.g., ordinary addition) and $*$ (e.g., ordinary multiplication), such that for all $a, b, c \in R$ the following axioms are obeyed:

- **(A1-A5)** R is an abelian group under $\circ$.
- **(M1) Closure under $*$:** If $a, b \in R$, then $a * b \in R$.
- **(M2) Associativity of $*$:** $a * (b * c) = (a * b) * c$, for all $a, b, c \in R$.
- **(M3) Distributive Laws:**
  (i) Left Distributive Law: $a * (b \circ c) = (a * b) \circ (a * c)$, for all $a, b, c \in R$.
  (i) Right Distributive Law: $(a \circ b) * c = (a * c) \circ (b * c)$, for all $a, b, c \in R$.

Ring and Field

Definition (Commutative Ring)

A ring $(R, \circ, *)$ is said to be *commutative* if it satisfies the following additional condition:

- **(M4) Commutative of $*$:** $a * b = b * a$, for all $a, b \in R$.

Ring and Field

Example

Let E denote the set of even integers, that is, $E = \{0, \pm 2, \pm 4, \pm 6, \cdots, \}$. Then, $(E, +, \times)$ is a commutative ring.

Example

Let M_n denote the set of all n-square $(n \times n)$ matrices over the real numbers. Then, $(M_n, +, \times)$ is a ring, where $+$ and $\times$ denote the ordinary matrix addition and multiplication, respectively.

Ring and Field

Definition (Field)

A field F, sometimes denoted by $(F, +, \times)$, is a set of elements with two binary operations, say addition and multiplication (note that these operations may be any binary operations), such that for all $a, b, c \in F$, the following axioms are obeyed:

- $(F, +, \times)$ is an *integral domain*, that is,
  - **(A1-M4)** hold
  - **(M5) Multiplicative identity:** $\forall a \in F$, $\exists e_m \in F$ such that $e_m a = a e_m = a$, e_m is called the multiplicative identity in F.
  - **(M6) No zero divisors:** If $a, b \in F$ and $ab = 0$, then either $a = 0$ or $b = 0$.
- **(M7) Multiplicative inverse:** For each $a \in F$, except 0, there is an element a^{-1} in F such that $aa^{-1} = a^{-1}a = e_m$.

Ring and Field

Example

The set of real numbers is a field under addition and multiplication.

Example

Let Q denote the set of rational numbers, that is, $Q = \{\frac{a}{b} | \ a, b$ are reals, with $b \neq 0$ and $\gcd(a, b) = 1\}$. Then, $(Q, +, \times)$ is a field.

Example

Let C be the set of complex numbers. Then, $(C, +, \times)$ is also a field.

Example

The set Z of integers is NOT a field. Note that not every element of Z has a multiplicative inverse; in fact, only the elements 1 and -1 have the multiplicative inverses in the integers.

Ring and Field

Problem: Consider the addition and multiplication arithmetic modulo 8 in the finite set $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Construct the following composition table (addition modulo 8):

$+_8$	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

The additive identity is 0.

Ring and Field

Construct the following composition table (multiplication modulo 8):

$\times_8$	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

Ring and Field

Construct the following table of additive and multiplicative inverses:

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

- $-w$ is the additive inverse of w
- w^{-1} is the multiplicative inverse of w
- Z_8 **is NOT a field (only a commutative ring with identity 1)**

Ring and Field

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Theorem

Let $Z_n = \{0, 1, 2, \ldots, n-1\}$.

- *(i)* $\langle Z_n, +_n, .n \rangle$ *is a ring, for all* $n \in N$.
- *(ii)* $\langle Z_n, +_n, .n \rangle$ *has a multiplicative identity* 1.
- *(iii)* $\langle Z_n, +_n, .n \rangle$ *is an integral domain.*

Ring and Field

Theorem

Let $Z_n = \{0, 1, 2, \ldots, n-1\}$. *Then,*
$\langle Z_n, +_n, .n \rangle$ *is a field if and only if n is prime.*

Remark: $\langle Z_p, +_p, .p \rangle$ is known as **Galois field** or finite field, when p is a prime.
It is defined as $GF(p) = \langle Z_p, +_p, .p \rangle$; p being a prime.

Ring and Field

Definition (Irreducible Polynomial)

A polynomial $f(x)$ of degree $n > 0$ over the field K is *irreducible* over K if and only if there do not exist polynomials $g(x)$ and $h(x)$ of degree > 0 over K such that

$$f(x) = g(x).h(x),$$

where multiplication is ordinary polynomial multiplication with coefficients operations in K.

- In other words, a polynomial $f(x)$ is said to be irreducible if it can not be factored into non-trivial polynomials over the same field K. 1 and $f(x)$ are trivial factors of $f(x)$.
- A polynomial $f(x)$ is irreducible over K if and only if there does not exist a polynomial $d(x)$, $0 < deg.d(x) < deg.f(x)$, where $deg.f(x)$ means the degree of the polynomial $f(x)$, such that $d(x)|f(x)$ over K.

Ring and Field

Lemma

A polynomial $p(x)$ is irreducible over a field K if and only if $k.p(x)$ is also irreducible over K, $\forall k \in K$.

Ring and Field

Modular Polynomial Arithmetic

- Consider the set S of all polynomials of degree $n-1$ or less over a finite field (Galois field) $Z_p = GF(p)$.
- Each polynomial has the following form:

$$\begin{aligned} f(x) &= a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \\ &= \sum_{i-0}^{n-1} a_i x^i, \end{aligned}$$

  where $a_i \in Z_p = \{0, 1, 2, \cdots, p-1\}$.
- There are a total of p^n different polynomials is S.

Problem: Find all polynomials in the field $GF(3^2)$

Here, we have the extended Galois field $GF(p^n)$, where $p = 3$ and $n = 2$.

Then, $S = \{f(x) | f(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{1} a_i x^i = a_1 x + a_0\}$ where $a_i \in Z_p = Z_3 = \{0, 1, 2\}$.

Therefore, there are a total of $3^2 = 9$ polynomials in the set S, which are given below.

a_1	a_0	$f(x) = a_1 x + a_0$
0	0	0
0	1	1
0	2	2
1	0	x
1	1	$x + 1$
1	2	$x + 2$
2	0	$2x$
2	1	$2x + 1$
2	2	$2x + 2$

Problem: Find all polynomials in the field $GF(2^3)$

Here, we have the extended Galois field $GF(p^n)$, where $p = 2$ and $n = 3$.
Then, $S = \{f(x) | f(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{2} a_i x^i = a_2 x^2 + a_1 x + a_0\}$ where $a_i \in Z_p = Z_2 = \{0, 1\}$. Therefore, there are a total of $2^3 = 8$ polynomials in the set S, which are given below.

a_2	a_1	a_0	$f(x) = a_2 x^2 + a_1 x + a_0$
0	0	0	0
0	0	1	1
0	1	0	x
0	1	1	$x + 1$
1	0	0	x^2
1	0	1	$x^2 + 1$
1	1	0	$x^2 + x$
1	1	1	$x^2 + x + 1$

Finding the Greatest Common Divisor (gcd)

The polynomial $c(x)$ is said to be the greatest common divisor of the polynomials $a(x)$ and $b(x)$ if

1. $c(x)$ divides both $a(x)$ and $b(x)$
2. any divisor of $a(x)$ and $b(x)$ is a divisor of $c(x)$, that is,

$$\gcd[a(x), b(x)] = \gcd[b(x), a(x) \bmod b(x)]$$

Algorithm: EUCLID$(a(x), b(x))$

1: Set $A(x) \leftarrow a(x)$; $B(x) \leftarrow b(x)$
2: **if** $B(x) = 0$ **then**
3: **return** $A(x) = \gcd[a(x), b(x)]$
4: **end if**
5: Compute $R(x) = A(x) \bmod B(x)$
6: Set $A(x) \leftarrow B(x)$
7: Set $B(x) \leftarrow R(x)$
8: goto Step 2

Finding the multiplicative inverse of a polynomial $b(x)$ modulo $m(x)$ in $GF(p^n)$

If $\gcd(m(x), b(x)) = 1$, then $b(x)$ has a multiplicative inverse $b(x)^{-1}$ modulo $m(x)$, where $m(x)$ is irreducible polynomial over $GF(p^n)$.

Algorithm: EXTENDED EUCLID$(m(x), b(x))$

1: Initialize: $(A1(x), A2(x), A3(x)) \leftarrow (1, 0, m(x))$ and $(B1(x), B2(x), B3(x)) \leftarrow (0, 1, b(x))$
2: **if** $B3(x) = 0$ **then**
3: **return** $A3(x) = \gcd[m(x), b(x)]$; no inverse
4: **end if**
5: **if** $B3 = 1$ **then**
6: **return** $B3(x) = \gcd[m(x), b(x)]$; $B2(x) = b(x)^{-1} \pmod{m(x)}$
7: **end if**
8: Set $Q(x) = \lfloor \frac{A3(x)}{B3(x)} \rfloor$, quotient when $A3(x)$ is divided by $B3(x)$
9: Set $[T1(x), T2(x), T3(x)] \leftarrow [A1(x) - Q(x).B1(x), A2(x) - Q(x).B2(x), A3(x) - Q(x).B3(x)]$
10: Set $[A1(x), A2(x), A3(x)] \leftarrow [B1(x), B2(x), B3(x)]$
11: Set $[B1(x), B2(x), B3(x)] \leftarrow [T1(x), T2(x), T3(x)]$
12: goto Step 2

Ring and Field

Problem: Find the multiplicative inverse of $(x^7 + x + 1)$ modulo an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ in $GF(2^8)$.

- **Initialization:**

$$A1(x) = 1; A2(x) = 0; A3(x) = m(x) = x^8 + x^4 + x^3 + x + 1$$

$$B1(x) = 0; B2(x) = 1; B3(x) = x^7 + x + 1$$

- **Iteration 1:**

$$\begin{aligned} Q(x) &= \left\lfloor \frac{A3(x)}{B3(x)} \right\rfloor = x \\ T1(x) &= A1(x) - Q(x).B1(x) = 1 \\ T2(x) &= A2(x) - Q(x).B2(x) = -x = x \pmod 2 \\ T3(x) &= A3(x) - Q(x).B3(x) = x^4 + x^3 + x^2 + 1 \end{aligned}$$

- **Iteration 1 (Continued...):**

$$A1(x) = B1(x) = 0; A2(x) = B2(x) = 1;$$
$$A3(x) = B3(x) = x^7 + x + 1$$
$$B1(x) = T1(x) = 1; B2(x) = T2(x) = x;$$
$$B3(x) = T3(x) = x^4 + x^3 + x^2 + 1$$

- **Iteration 2:**

$$\begin{aligned} Q(x) &= \left\lfloor \frac{A3(x)}{B3(x)} \right\rfloor = x^3 + x^2 + 1 \\ T1(x) &= A1(x) - Q(x).B1(x) = x^3 + x^2 + 1 \\ T2(x) &= A2(x) - Q(x).B2(x) = x^4 + x^3 + x + 1 \\ T3(x) &= A3(x) - Q(x).B3(x) = x \end{aligned}$$

- **Iteration 2 (Continued...):**

$$\begin{aligned} A1(x) &= B1(x) = 1; A2(x) = B2(x) = x; \\ A3(x) &= B3(x) = x^4 + x^3 + x^2 + 1 \\ B1(x) &= T1(x) = x^3 + x^2 + 1; \\ B2(x) &= T2(x) = x^4 + x^3 + x + 1; \\ B3(x) &= T3(x) = x \end{aligned}$$

- **Iteration 3:**

$$\begin{aligned} Q(x) &= \left\lfloor \frac{A3(x)}{B3(x)} \right\rfloor = x^3 + x^2 + x \\ T1(x) &= A1(x) - Q(x).B1(x) = x^6 + x^2 + x + 1 \\ T2(x) &= A2(x) - Q(x).B2(x) = x^7 \\ T3(x) &= A3(x) - Q(x).B3(x) = 1 \end{aligned}$$

Ring and Field

- **Iteration 4:** Since $B3(x) = 1$, so

$$\gcd[m(x), b(x)] = B3(x) = 1$$

and

$$\begin{aligned} b(x)^{-1} \bmod m(x) &= B2(x) \\ &= (x^7 + x + 1)^{-1} \bmod x^8 + x^4 + x^3 + x + 1 \\ &= x^7. \end{aligned}$$

Finite field of the form $GF(2^n)$

Computational Considerations

- A polynomial $f(x)$ in $GF(2^n)$, $f(x) = a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$
  $= \sum_{i=0}^{n-1} a_i x^i$,
  where $a_i \in Z_2 = \{0, 1\}$,
  can be uniquely expressed by its n binary co-efficients
  $(a_{n-1}a_{n-2}\cdots a_1 a_0)$, since $a_i \in Z_2$.
- Thus, every polynomial in $GF(2^n)$ can be represented by an n-bit number.
- For example, every polynomial in $GF(2^8)$ can be represented by an 8-bit number $(a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$, which is a byte.
  If $f(x) = x^6 + x^4 + x^2 + x + 1$ in $GF(2^8)$, then we can express
  $f(x) = 0.x^7 + 1.x^6 + 0.x^5 + 1.x^4 + 0.x^3 + 1.x^2 + 1.x + 1$
  $= (0101\ 0111)$ (in binary)
  $= \{57\}$ (in hexadecimal).

Finite field of the form $GF(2^n)$

Addition

- Addition of two polynomials in $GF(2^n)$ coprresponds to a bitwise XOR operation (modulo 2 operation).
- **Example.** Consider the two polynomials in $GF(2^8)$:
  $f(x) = x^6 + x^4 + x^2 + x + 1$, and
  $g(x) = x^7 + x + 1$.
  Note that $f(x) = (0101\ 0111) = \{57\}$, and
  $g(x) = (1000\ 0011) = \{83\}$.
  Then

$$\begin{aligned} f(x) + g(x) &= (0101\,0111) \oplus (1000\,0011) \\ &= (1101\,0100) \\ &= x^7 + x^6 + x^4 + x^2 \\ &= \{d4\}. \end{aligned}$$

Finite field of the form $GF(2^n)$

Multiplication

- In AES (Advanced Encryption Standard), $GF(2^8)$ has irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.
- The technique is based on the observation that
  $x^8 \pmod{m(x)} = [m(x) - x^8] \pmod{2}$
  $= x^4 + x^3 + x + 1$
  $= (0001\ 1011)$.
- In general, in $GF(2^n)$ with n^{th}-degree polynomial $p(x)$, we have
  $x^n \pmod{p(x)} = [p(x) - x^n]$.

Finite field of the form $GF(2^n)$

Multiplication

- In $GF(2^8)$, a polynomial is of the form $f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$, which is also a byte $(b_7b_6b_5b_4b_3b_2b_1b_0)_2$.
- Then $x \times f(x)$
  $= x \times (b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0)$
  $= b_7x^8 + (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x + 0)$.
- Thus,

$$x \times f(x) = \begin{cases} (b_6b_5b_4b_3b_2b_1b_00), & \text{if } b_7 = 0 \\ (b_6b_5b_4b_3b_2b_1b_00) \oplus (0001\ \ 1011), & \text{if } b_7 = 1. \end{cases}$$

Finite field of the form $GF(2^n)$

Multiplication

- $x^2 \times f(x) = x \times [x \times f(x)]$
- $x^3 \times f(x) = x \times [x^2 \times f(x)]$
- $x^4 \times f(x) = x \times [x^3 \times f(x)]$

  $\vdots$

- $x^n \times f(x) = x \times [x^{n-1} \times f(x)]$

Finite field of the form $GF(2^n)$

- **Problem:** Given an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ in the finite field $GF(2^8)$. Compute the product of two bytes $\{A4\}$ and $\{75\}$, where $\{\cdot\}$ represents a hexadecimal number as a 8-bit binary number, in $GF(2^8)$ with respect to $m(x)$.

Finite field of the form $GF(2^n)$

Solution:

- Let $f(x) = \{A4\} = (1010\ 0100) = x^7 + x^5 + x^2$,
  $g(x) = \{75\} = (0111\ 0101) = x^6 + x^5 + x^4 + x^2 + 1$.
- Then

$$
\begin{aligned}
f(x) \times g(x) &= x^7 \times g(x) \oplus x^5 \times g(x) \\
&\quad \oplus x^2 \times g(x) \pmod{m(x)} && (1)\\
x \times g(x) &= 1110\,1010, \text{ since } b_7 = 0 && (2)\\
x^2 \times g(x) &= 1101\,0100 \oplus 0001\,1011, \text{ since } b_7 = 1 \\
&= 1100\,1111 && (3)\\
x^3 \times g(x) &= 1000\,0101 && (4)\\
x^4 \times g(x) &= 0001\,0001 && (5)\\
x^5 \times g(x) &= 0010\,0010 && (6)
\end{aligned}
$$

Finite field of the form $GF(2^n)$

Solution (Continued...):

- We have,

$$x^6 \times g(x) = 0100\,0100 \quad (7)$$
$$x^7 \times g(x) = 1000\,1000 \quad (8)$$

- Finally, using Equations (8), (11) and (13), from Equation (6), we obtain:

$$\begin{aligned} f(x) \times g(x) \pmod{m(x)} &= 1100\,1111 \\ &\oplus\ 0010\,0010 \\ &\quad\ 1000\,1000 \\ \hline &= 0110\,0101 \\ &= \{65\} \\ &= x^6 + x^5 + x^2 + 1. \end{aligned}$$