Discrete Structures (Monsoon 2021)

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/

Topic: **Ring and Field**

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 $a, b, c \in R$.

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 commutative ring, where $+$ and $\times$ denote the ordinary matrix addition and multiplication, respectively.

Ring and Field

- **Problem:** Let $(R, +, \times)$ be a ring with identity, R is the set of real numbers. Using its elements, let us define another structure $(R', \oslash, \otimes)$, where $R' = R$ and for $a, b \in R$, $a \oslash b = a + b + 1$ and $a \otimes b = a \times b + a + b$.
  (i) Prove that $(R', \oslash, \otimes)$ is a ring.
  (ii) Is R' is a ring with identity? If so, which one is the multiplicative identity (under $\otimes$)?

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

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:** $\forall a \in F$, $\exists 1 \in F$ such that $1a = a1 = a$, 1 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 $aa^{-1} = a^{-1}a = 1$.

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

Theorem

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

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

Finding greatest common divisor (gcd)

Definition

Given two integers a and b, the greatest common divisor (gcd) of a and b is $d = \gcd(a, b)$ if the following conditions are satisfied:

1. $d|a$ and $d|b$
2. Any divisor c of a and b is also a divisor of d.

We have:

$$\begin{aligned}
\gcd(a, 0) &= a \\
\gcd(0, 0) &= \textit{undefined} \\
\gcd(a, -b) &= \gcd(-a, b) = \gcd(-a, -b) = \gcd(|a|, |b|)
\end{aligned}$$

Euclid's GCD Algorithm

Given integers $b, c > 0$, we make a repeated application of division algorithms to obtain a series of equations which yield $\gcd(b, c)$:

$$\begin{aligned}
b &= q_1 c + r_1, 0 \leq r_1 < c \\
c &= q_2 r_1 + r_2, 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, 0 \leq r_3 < r_2 \\
\vdots &= \vdots \\
r_{j-2} &= q_j r_{j-1} + r_j, 0 \leq r_j < r_{j-1} \\
r_{j-1} &= q_{j+1} r_j + \boxed{0}
\end{aligned}$$

It is worth noticing that

$$0 \leq r_j < r_{j-1} < r_{j-2} < \cdots < r_2 < r_1 < c$$

Therefore,

$$\gcd(b, c) = \gcd(c, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{j-1}, r_j) = r_j.$$

Euclid's GCD Algorithm

Algorithm: EUCLID(b, c)

To compute $\gcd(b, c)$

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

Complexity: If j is the total number of iterations or steps needed to compute $\gcd(b, c)$, then $j < \lfloor 3.\log_e(c) \rfloor$, where $c = \min\{b, c\}$.

Problem: Compute $\gcd(1970, 1066)$.

Using the Euclid's gcd algorithm, we have the following computations:

$$
\begin{aligned}
1970 &= 1 \times 1066 + 904 \\
1066 &= 1 \times 904 + 162 \\
904 &= 5 \times 162 + 94 \\
162 &= 1 \times 94 + 68 \\
94 &= 1 \times 68 + 26 \\
68 &= 2 \times 26 + 16 \\
26 &= 1 \times 16 + 10 \\
16 &= 1 \times 10 + 6 \\
10 &= 1 \times 6 + 4 \\
6 &= 1 \times 4 + 2 \\
4 &= 2 \times \boxed{2} + 0
\end{aligned}
$$

Therefore, $\gcd(1970, 1066) = 2$.
We see that $j =$ number of iterations needed to compute $\gcd(1970, 1066)$ $= 11$ and $j < \lfloor 3. \log_e(c) \rfloor = \lfloor 3. \log_e(1066) \rfloor = 20$

Finding greatest common divisor (gcd)

Lemma

If $d = \gcd(a, b)$, then there exist integers x and y such that $d = ax + by$, where x and y are called the multipliers of a and b, respectively.

Problem: Find the multipliers x, y and z such that $\gcd(170, 128, 217) = 170x + 128y + 217z$.

Solution: We know,

$$\gcd(170, 128, 217) = \gcd[\gcd(170, 128), 217]. \quad (1)$$

To compute $\gcd(170, 128)$, we proceed as follows:

$$\begin{aligned} 170 &= 1 \times 128 + 42 & (2) \\ 128 &= 3 \times 42 + 2 & (3) \\ 42 &= 21 \times 2 + 0. \end{aligned}$$

Finding greatest common divisor (gcd)

Therefore, we have:

$$\begin{aligned} 2 &= \gcd(170, 128) \\ &= 128 - 3 \times 42, \text{ using Eqn (3)} \\ &= 128 - 3 \times [170 - 1 \times 128] \text{ using Eqn (2)} \\ &= (-3) \times 170 + 4 \times 128. \end{aligned} \tag{4}$$

Now, to compute $\gcd(2, 217)$, we proceed as follows:

$$\begin{aligned} 217 &= 108 \times 2 + 1 \quad (5) \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

Finding greatest common divisor (gcd)

Then,

$$\begin{aligned}
1 &= \gcd(2, 217) \\
&= \gcd[\gcd(170, 128), 217] \\
&= \gcd(170, 128, 217) \\
&= 217 - 108 \times 2, \text{using Eqn (5)} \\
&= 217 - 108 \times [(-3) \times 170 + 4 \times 128], \text{using Eqn (4)} \\
&= 324 \times 170 + (-432) \times 128 + 1 \times 217.
\end{aligned}$$

Hence, we have: $x = 324, y = -432, z = 1$.

Finding the multiplicative inverse in $GF(p)$

If $\gcd(m, b) = 1$, then b has a multiplicative inverse modulo n. In other words, for positive integer $b < m$, there exists $b^{-1} < m$ such that $b.b^{-1} = 1 \pmod{m}$, where 1 is the multiplicative identity in $GF(p)$.

Algorithm: EXTENDED EUCLID(m, b)

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

Ring and Field

Problem: Find the multiplicative inverse of 550 in $GF(1759)$.

Here, $m = 1759$ and $b = 550$. We need to find $b^{-1} \pmod{m}$, i.e., $550^{-1} \pmod{1759}$.
Applying the extended Euclid's gcd algorithm, we have the following table.

Q	$A1$	$A2$	$A3$	$B1$	$B2$	$B3$	$T1$	$T2$	$T3$
–	1	0	1759	0	1	550	–	–	–
3	0	1	550	1	-3	109	1	-3	109
5	1	-3	109	-5	16	5	-5	16	5
21	-5	16	5	106	-339	4	106	-339	4
1	106	-339	4	-111	355	$\boxed{1}$	-111	355	1

Since $B3 = 1$, so $\gcd(m, b) = B3 = 1$ and multiplicative inverse will be $b^{-1} \pmod{m} = B2 = 355$.
Verification: $b.b^{-1} \pmod{m} = 550.355 \pmod{1759} = 1$.

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

Problem: Determine which of the following are reducible over the Galois (finite) field $GF(2)$:

1. $f(x) = x^4 + 1$
2. $f(x) = x^3 + x + 1$
3. $f(x) = x^3 + 1$
4. $f(x) = x^3 + x^2 + 1$

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, $\forall k \in K$.

Proof.

$(\Rightarrow)$: Given that $p(x)$ is irreducible over K.
RTP: $k.p(x)$ is irreducible over K, $\forall k \in K$.
If possible, let $k.p(x)$ be reducible over K.
Then, there exist $f(x), g(x) \in \mathcal{P}_K^n$, the set of all polynomials of degree $< n$ over the field K, such that

$$k.p(x) = f(x).g(x).$$

Since $k^{-1} \in K$ exists, we have:

$$p(x) = (k^{-1}.f(x)).g(x) = f'(x).g(x),$$

where $f'(x) = k^{-1}.f(x) \in \mathcal{P}_K^n$.

Ring and Field

This shows that $p(x)$ is is reducible polynomial. Hence, it is a contradiction. Consequently, $k.p(x)$ must be irreducible over K.
$(\Leftarrow)$: Given $k.p(x)$ is irreducible, $\forall k \in K$.
RTP: $p(x)$ is irreducible.
If possible, assume that $p(x)$ is reducible one.
Then, there exist $f(x), g(x) \in \mathcal{P}_K^n$, the set of all polynomials of degree $< n$ over the field K, such that

$$p(x) = f(x).g(x).$$

Now,

$$k.p(x) = k.f(x).g(x) = f'(x).g(x),$$

where $f'(x) = k.f(x) \in \mathcal{P}_K^n$.
It shows that $k.p(x)$ is reducible polynomial over the finite field K. But, it is a contradiction from the given condition. Hence, $p(x)$ must be irreducible polynomial over 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

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

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:**

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

Ring and Field

- **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:**

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

Ring and Field

- **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 $GF(2^n)$, $f(x) = a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ $= \sum_{i=0}^{n-1} a_i x^i$,
  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 $(a_7a_6a_5a_4a_3a_2a_1a_0)$, 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

$$
\begin{aligned}
f(x) \times g(x) &= x^7 \times g(x) \oplus x^5 \times g(x) \\
&\quad \oplus x^2 \times g(x) \pmod{m(x)} && (6)\\
x \times g(x) &= 1110\,1010, \text{ since } b_7 = 0 && (7)\\
x^2 \times g(x) &= 1101\,0100 \oplus 0001\,1011, \text{ since } b_7 = 1 \\
&= 1100\,1111 && (8)\\
x^3 \times g(x) &= 1000\,0101 && (9)\\
x^4 \times g(x) &= 0001\,0001 && (10)\\
x^5 \times g(x) &= 0010\,0010 && (11)
\end{aligned}
$$

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

Solution (Continued...):

- We have,

$$x^6 \times g(x) = 0100\,0100 \quad (12)$$
$$x^7 \times g(x) = 1000\,1000 \quad (13)$$

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

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

Thank you!