Software and Computer Security

SOFE4840U

Lecture 04

Finite Fields

Dr. Khalid A. Hafeez

Winter, 2024

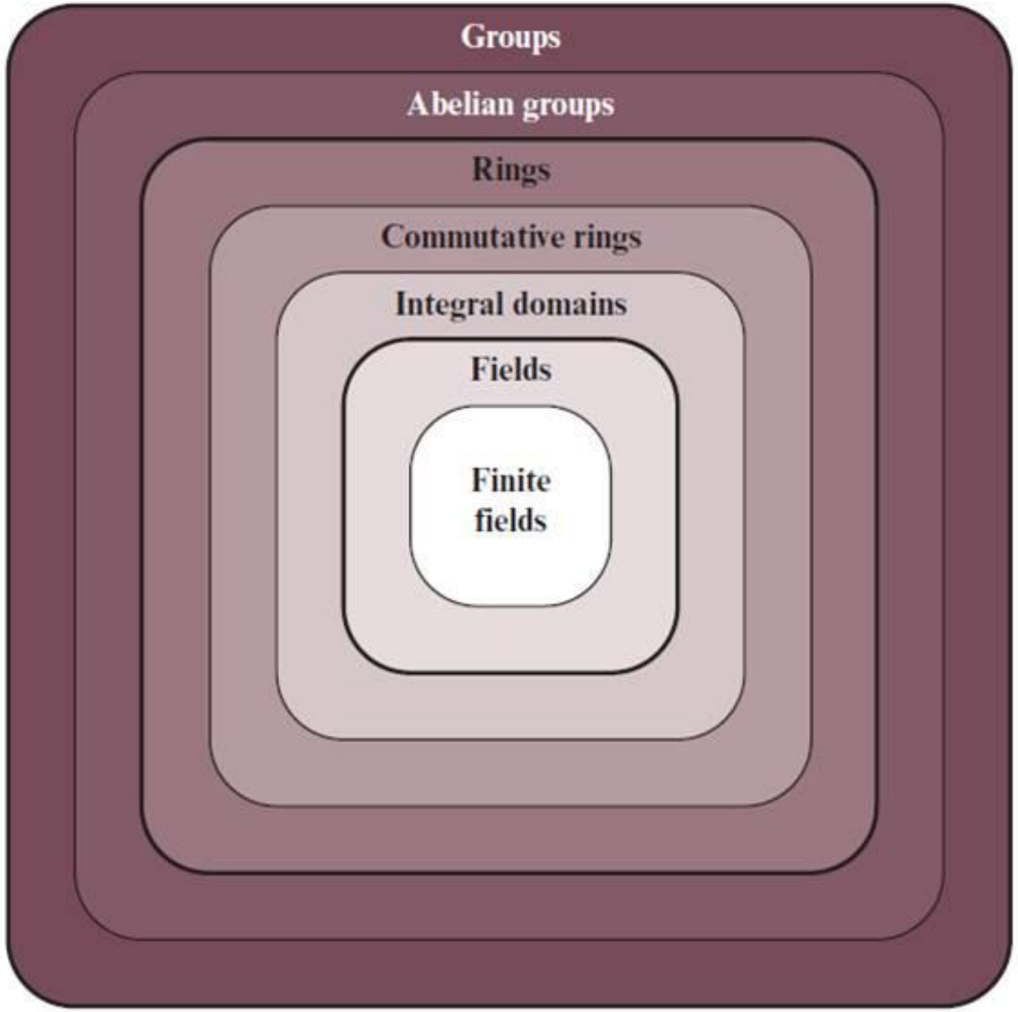
Lecture Outline

- **Group**
- **Ring**
- **Modulo Operation**
- **Euclidean Algorithm**
- **Finite Fields**
- **Extended Euclidean Algorithm**

Groups, Rings, and Fields

- Finite fields are used in cryptography.
  - Such as Advanced Encryption Standard (AES) and elliptic curve cryptography

- Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra.
- Concerned with sets: we can combine two elements of the set, perhaps in several ways, to obtain a third element of the set.



Group

- **Group**: a set of elements with an operation denoted by {G, *} that associates to each ordered pair (a, b) of elements in G an element ($a * b$) in G.
- ***Properties:***
  - **(A1) Closure:**
    - If a and $b \in G$, then $a * b = c \in G$
  - **(A2) Associative:**
    - $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$
  - **(A3) Identity element:**
    - There is an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$
  - **(A4) Inverse element:**
    - For each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = 1$
  - **(A5) Commutative: (** a group that satisfies this is called **abelian group)**
    - $a * b = b * a$ for all $a, b \in G$

- The set of integers (positive, negative, and 0) under addition is an abelian group.
- The set of nonzero real numbers under multiplication is an abelian group.

Rings

- A **ring** R, Denoted by {R , + , × }, is a set of elements with two operations, called *addition* and *multiplication*, such that for all a , b , $c \in$ R:
- **Properties:**
  - **(A1–A5)**
  - **(M1) Closure under multiplication:**

    If a and $b \in R$, then ab is also in R
  - **(M2) Associativity of multiplication:**

    $a(bc) = (ab)c$ for all a , b , $c \in R$
  - **(M3) Distributive laws:**

    $a(b + c) = ab + ac$ for all $a, b, c \in R$

    $(a + b)c = ac + bc$ for all $a, b, c \in R$

- *In essence, a ring is a set in which we can do addition, subtraction [a - b = a + (-b)], and multiplication without leaving the set*
- *With respect to addition and multiplication, the set of all n-square matrices over the real numbers is a ring.*

Rings

- A ring is said to be commutative if
  - **(M4) Commutativity of multiplication**: A ring is said to be commutative if

    $ab = ba$ for all $a, b \in R$

- *An integral domain is a commutative ring that obeys the following axioms.*
  - **(M5) Multiplicative identity**:

    There is an element 1 in R such that $a1 = 1a = a$ *for all* $a \in R$

  - ***(M6) No zero divisors:***

    If a, b *in R and* $ab = 0$, *then either* $a = 0$ *or* $b = 0$

Field

- **Field** is denoted by $\{F, +, \times, (\ )^{-1}\}$, is a set of elements with operations, called *addition, multiplication and inverse*, such that for all $a, b, c \in F$:
- Properties:
  - **(A1–M6)**
  - **(M7) Multiplicative inverse:**

    For each $a \in F$, except 0, there is an element $a^{-1} \in F$ such that $aa^{-1} = (a^{-1})a = 1$

- **Summary**: a Field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with the following rule: $a/b = a(b^{-1})$

- Examples of fields: rational numbers, real numbers, and complex numbers.
- The set of all integers is not a field, because not every element of the set has a multiplicative inverse.

Properties of Groups, Rings, and Fields

Field
Integral domain
Commutative ring
Ring
Abelian group
Group

(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Modulo Operation

Modular Addition $(x + y) = (x + y) \text{ Mod } p$

Addition modulo 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

Modular Multiplication $(x \times y) = (x \times y) \text{ Mod } p$

Multiplication 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

Additive and multiplicative inverses modulo 7

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

Additive Inverse, $(x + i) \text{ Mod } p = 0$

Multiplicative Inverse, $(x \times i) \text{ Mod } p = 1$

Euclidean Algorithm and Modular Reduction

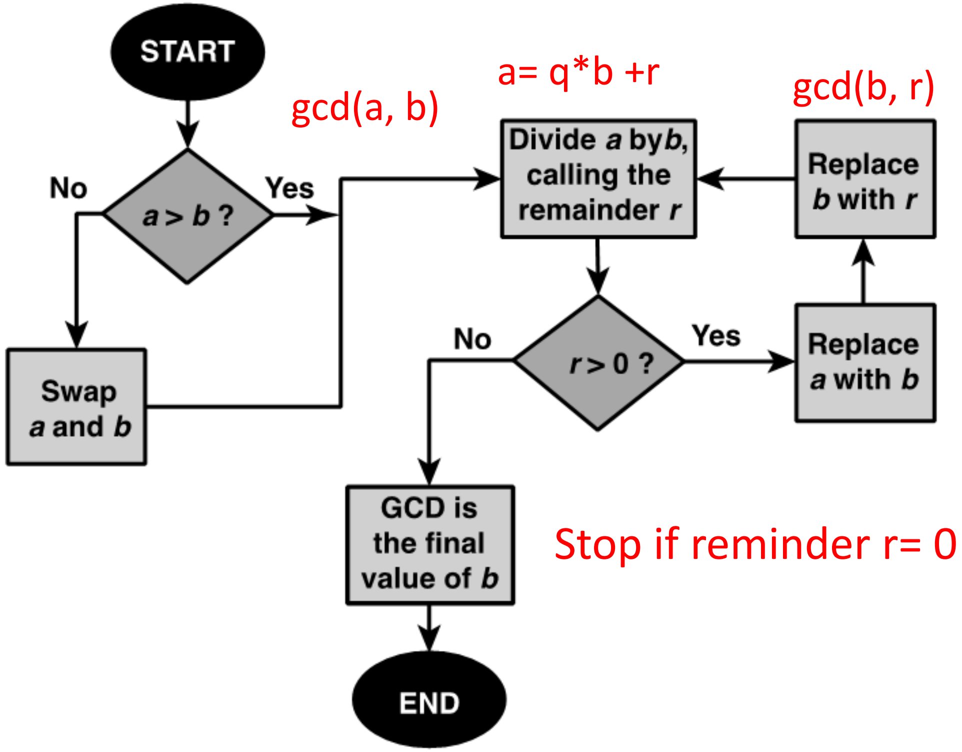
- Procedure for determining the greatest common divisor (gcd) of two positive integers
- The greatest common divisor of a and b is the largest integer that divides both a and b
- We can use the notation gcd(a,b) to mean the greatest common divisor of a and b
  - We also define gcd(0,0) = 0
- Positive integer c is said to be the gcd of a and b if:
  - c is a divisor of a and b
  - Any divisor of a and b is a divisor of c
- An equivalent definition is:
  - gcd(a,b) = max[k, such that k | a and k | b]
- Because we require that the greatest common divisor be positive,
  - gcd(a,b) = gcd(a,-b) = gcd(-a,b) = gcd(-a,-b)

- We stated that two integers a and b are relatively prime if their only common positive integer factor is 1;
  - this is equivalent to saying that a and b are relatively prime if **gcd(a,b) = 1**

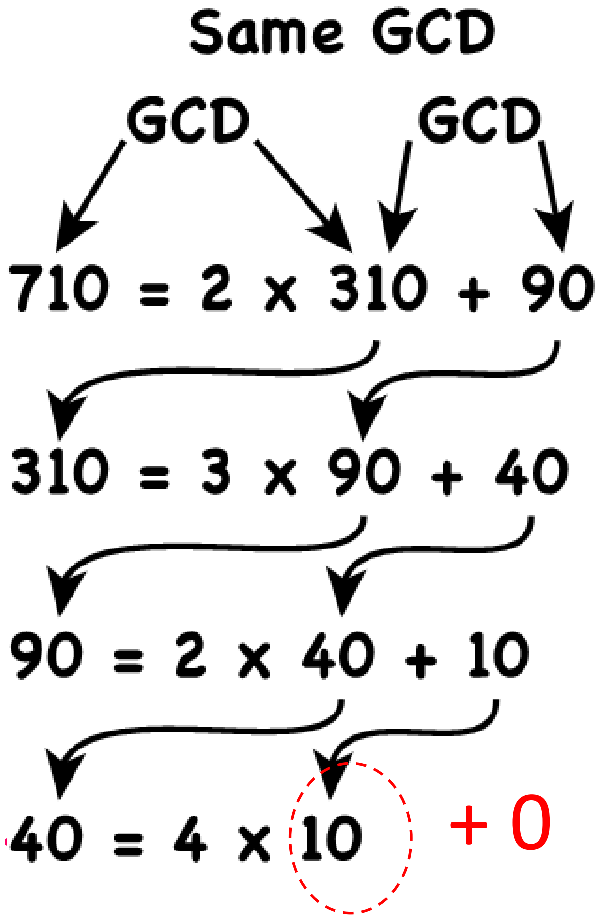
Euclidean Algorithm and Modular Reduction

- An algorithm credited to Euclid for easy finding the greatest common divisor of two integers
  - gcd(a, b) = gcd(b, a mod b)
  - Repeat until mod = 0

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



gcd(710, 310)=10



Euclidean Algorithm and Modular Reduction - Example

- **Example:**
  - gcd(1160718174 , 316258250) = gcd(b, a mod b)
  - Stop, reminder = 0

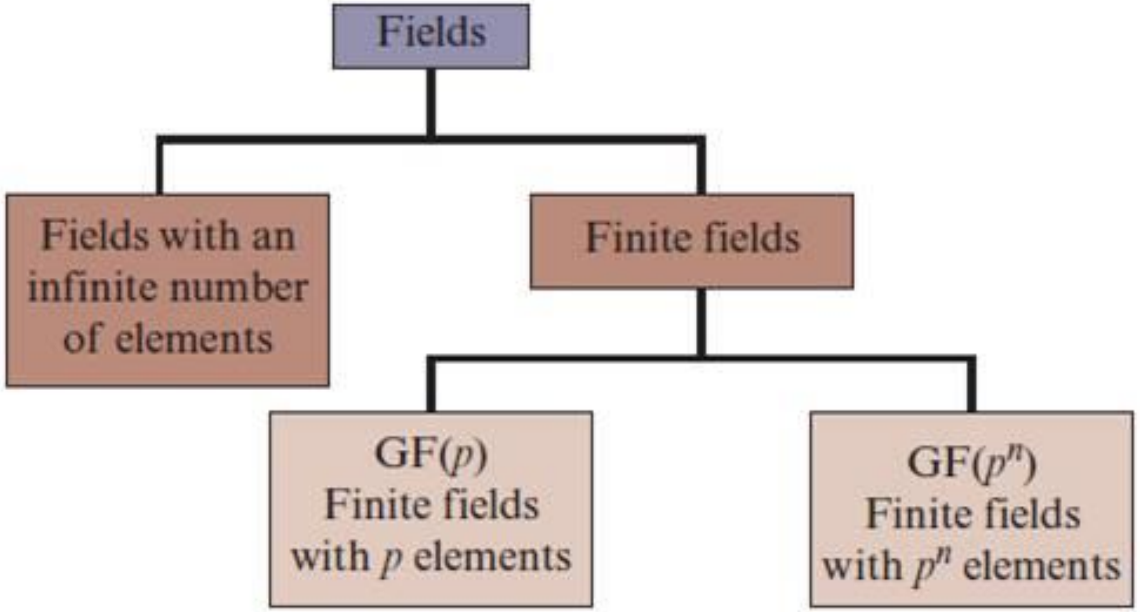
To find $d = \gcd(a, b) = \gcd(1160718174, 316258250)$		
$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2156 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

Euclidean Algorithm and Modular Reduction

- Example:
  - Calculate GCD(84, 30) using Euclidean Algorithm and Modular Reduction

Types of Fields

- Finite fields play a crucial role in many cryptographic algorithms
- It can be shown that the order of a finite field (number of elements in the field) must be a power of a prime p^n, where n is a positive integer
  - The finite field of order p^n is generally written GF(p^n)
  - GF stands for Galois field, in honor of the mathematician who first studied finite fields
  - For n = 1, we have the finite field GF(p); this finite field has a different structure than that for finite fields with n > 1
  - GF(2^n) is an important field in cryptography



Prime Fields - GF(p)

1. GF(p) consists of p elements. Where p is a prime number.
2. Elements of GF(p) are the integers $\{0, 1, . . . , p - 1\}$
3. The operations $+$ and $\times$ are defined over the set.
4. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set.
5. Addition and multiplication are done modulo p
6. Additive Inverse (-x), $(x + i) = 0 \ (\text{Mod } p)$
7. Multiplicative Inverse (x^{-1}), $(x \times i) = 1 \ (\text{Mod } p)$
8. Each element of the set other than 0 has a multiplicative inverse

Prime Fields - GF(7) - Operations

Addition

+	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

Multiplication

×	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

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

Additive inverse and

Multiplicative inverse

Prime Fields - GF(8) - Operations

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

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

Additive inverse

x	0	1	2	3	4	5	6	7
-x	0	7	6	5	4	3	2	1

Multiplicative inverse

x	0	1	2	3	4	5	6	7
X^{-1}	—	1	—	3	—	5	—	7

Prime Fields - GF(2) - 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.

Finite Field $GF(p^n) = GF(2^n)$ Arithmetic

- The order of a finite field must be of the form p^n, where p is a prime and n is a positive integer.
  - For the case n=1 then GF(p) using modular arithmetic satisfies all of the axioms for a field
  - For the case p=2, then $GF(2^n)$ does not satisfy all axioms of a field
  - But most encryption algorithms, both symmetric and asymmetric, involve arithmetic operations on integers. If one of the operations that is used in the algorithm is division, then we need to work in arithmetic defined over a field
  - And also for efficiency, we need to use all possible elements of the n-bits range (2^n)
  - That is why we need to find a way to make $GF(2^n)$ finite field over addition, multiplication, and division
    1. Convert every binary number to a polynomial
    2. Arithmetic follows the ordinary rules of polynomial arithmetic using the basic rules of algebra, with the following two refinements.
       a) Arithmetic on the coefficients is performed modulo $p=2$.
       b) If multiplication results in a polynomial of degree greater than $n - 1$, then the polynomial is reduced modulo some irreducible polynomial $m(x)$ of degree n. That is, we divide by $m(x)$ and keep the remainder.
          - For a polynomial $f(x)$, the remainder is expressed as $r(x) = f(x) \bmod m(x)$.

Finite Field GF(p^n) = GF(2^n) Arithmetic

The elements of GF(2^n) are polynomials :

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 = \sum_{i=0}^{n-1} a_i x^i$$

$a_i \in \{0, 1\} \in GF(2)$

Ex: GF (2^3)

binary	***polynomial***
000	*0*
001	*1*
010	x
011	$x + 1$
100	x^2
101	$x^2 + 1$
110	$x^2 + x$
111	$x^2 + x + 1$

Finite Field GF(2^n) Arithmetic - Operations

Addition and Subtraction in GF(2^n) : the two operations are the same

Let A(x), B(x) ∈ GF(2^n)

$$C(x) = A(x) + B(x) = \sum_{i=0}^{n-1} c_i x^i, \quad c_i \equiv a_i + b_i \bmod 2$$

$$C(x) = A(x) - B(x) = \sum_{i=0}^{n-1} c_i x^i, \quad c_i \equiv a_i - b_i \equiv a_i + b_i \bmod 2.$$

Example:

$(x^2 + 1) + (x^2 + x + 1) = x$

$$\begin{array}{l} 101 \\ \underline{111} \\ 010 \end{array} \qquad \begin{array}{l} x^2 + 0 + 1 \\ \underline{x^2 + x + 1} \\ 0 + x + 0 = x \end{array}$$

Finite Field GF(2^n) Arithmetic - Operations

Addition in GF(2^3)

Let A(x), B(x) ∈ GF(2^3)

		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+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

Finite Field GF(2^n) Arithmetic - Operations

Multiplication in GF(2^n)

Let A(x), B(x) ∈ GF(2^n)

C(x) = A(x).B(x) mod P(x), where p(x) is an irreducible polynomial in GF(2^n)

Irreducible polynomial:

GF(2^3) : $p(x) = x^3 + x + 1$

GF(2^4) : $p(x) = x^4 + x + 1$

GF(2^8) : $p(x) = x^8 + x^4 + x^3 + x + 1$

Finite Field GF(2^n) Arithmetic - Operations

Multiplication in GF(2^3)

Use the Irreducible polynomial: GF(2^3) : $p(x) = x^3 + x + 1$

		000	001	010	011	100	101	110	111
	$\times$	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+x	x^2	$x+1$

Example:

$(x+1)(x^2+x) \bmod (x^3+x+1) = ?\ 1$

$(x^3+x^2+x^2+x) \bmod (x^3+x+1) = ?\ 1$

$(x^3+x) \bmod (x^3+x+1) = ?\ 1$

1

$x^3+x+1 \,\big)\, x^3+x$

$\underline{x^3+x+1}$

$0+0+1 = 1$

Finite Field GF(2^n) Arithmetic - Operations

Multiplicative Inverse in GF(2^n)

The Multiplicative inverse of A(x) = $A^{-1}(x)$ of an element A(x) ϵ GF(2^n) must satisfy **A(x). A^{-1}(x) = 1 [mod p(x)]**

GF(2^4) : $\boldsymbol{p(x) = x^4 + x + 1}$

Inverse pairs:

$0 \leftrightarrow 0$	$1 \leftrightarrow 1$
$x \leftrightarrow x^3 + 1$	$x + 1 \leftrightarrow x^3 + x^2 + x$
$x^2 \leftrightarrow x^3 + x^2 + 1$	$x^2 + 1 \leftrightarrow x^3 + x + 1$
$x^2 + x \leftrightarrow x^2 + x + 1$	$x^2 + x + 1 \leftrightarrow x^2 + x$
$x^3 \leftrightarrow x^3 + x^2 + x + 1$	$x^3 + 1 \leftrightarrow x$
$x^3 + x \leftrightarrow x^3 + x^2$	$x^3 + x + 1 \leftrightarrow x^2 + 1$
$x^3 + x^2 \leftrightarrow x^3 + x$	$x^3 + x^2 + 1 \leftrightarrow x^2$
$x^3 + x^2 + x \leftrightarrow x + 1$	$x^3 + x^2 + x + 1 \leftrightarrow x^3$

But how to find Multiplicative inverse **A^{-1}(x) ?**

Extended Euclidean Algorithm

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

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

- Where x and y will have opposite signs
- Example: when *a* = 42 and *b* = 30, gcd(42, 30) = 6.

y \ *x*	−3	−2	−1	0	1	2	3
−3	−216	−174	−132	−90	−48	−6	36
−2	−186	−144	−102	−60	−18	24	66
−1	−156	−114	−72	−30	12	54	96
0	−126	−84	−42	0	42	84	126
1	−96	−54	−12	30	72	114	156
2	−66	−24	18	60	102	144	186
3	−36	6	48	90	132	174	216

- So x=-2 and y=3, then x × y = gcd(42, 30) = 6 :

  observation: 30 × 3 mod 42 = gcd(42, 30) = 6

Note: If a and b are relatively prime then gcd(a, b) = 1 then y is the multiplicative inverse of b

Extended Euclidean Algorithm for Polynomials

- The algorithm will find the multiplicative inverse of $b(x)$ modulo $a(x)$ if the degree of $b(x)$ is less than the degree of $a(x)$ and gcd$[a(x), b(x)] = 1$.
- If $a(x)$ is an irreducible polynomial, then it has no factor other than itself or 1, so that gcd$[a(x), b(x)] = 1$.
- We wish to solve the following equation for the values $v(x)$, $w(x)$, and $d(x)$,

  where $d(x) = \gcd[a(x), b(x)]$:

  $$a(x)v(x) + b(x)w(x) = d(x)$$

- If $d(x) = 1$, then $w(x)$ is the **multiplicative inverse** of $b(x)$ modulo $a(x)$.

- The calculations are as follows:

Extended Euclidean Algorithm for Polynomials

Calculate	Which satisfies	Calculate	Which satisfies
$r_{-1}(x) = a(x)$		$v_{-1}(x) = 1;\ w_{-1}(x) = 0$	$a(x) = a(x)v_{-1}(x) + bw_{-1}(x)$
$r_0(x) = b(x)$		$v_0(x) = 0;\ w_0(x) = 1$	$b(x) = a(x)v_0(x) + b(x)w_0(x)$
$r_1(x) = a(x) \bmod b(x)$ $q_1(x) =$ quotient of $a(x)/b(x)$	$a(x) = q_1(x)b(x) + r_1(x)$	$v_1(x) = v_{-1}(x) - q_1(x)v_0(x) = 1$ $w_1(x) = w_{-1}(x) - q_1(x)w_0(x) = -q_1(x)$	$r_1(x) = a(x)v_1(x) + b(x)w_1(x)$
$r_2(x) = b(x) \bmod r_1(x)$ $q_2(x) =$ quotient of $b(x)/r_1(x)$	$b(x) = q_2(x)r_1(x) + r_2(x)$	$v_2(x) = v_0(x) - q_2(x)v_1(x)$ $w_2(x) = w_0(x) - q_2(x)w_1(x)$	$r_2(x) = a(x)v_2(x) + b(x)w_2(x)$
$r_3(x) = r_1(x) \bmod r_2(x)$ $q_3(x) =$ quotient of $r_1(x)/r_2(x)$	$r_1(x) = q_3(x)r_2(x) + r_3(x)$	$v_3(x) = v_1(x) - q_3(x)v_2(x)$ $w_3(x) = w_1(x) - q_3(x)w_2(x)$	$r_3(x) = a(x)v_3(x) + b(x)w_3(x)$
• • •	• • •	• • ⋮	• • •
$r_n(x) = r_{n-2}(x) \bmod r_{n-1}(x)$ $q_n(x) =$ quotient of $r_{n-2}(x)/r_{n-2}(x)$	$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x)$	$v_n(x) = v_{n-2}(x) - q_n(x)v_{n-1}(x)$ $w_n(x) = w_{n-2}(x) - q_n(x)w_{n-1}(x)$	$r_n(x) = a(x)v_n(x) + b(x)w_n(x)$
$r_{n+1}(x) = r_{n-1}(x) \bmod r_n(x) = 0$ $q_{n+1}(x) =$ quotient of $r_{n-1}(x)/r_n(x)$	$r_{n-1}(x) = q_{n+1}(x)r_n(x) + 0$		$d(x) = \gcd(a(x), b(x)) = r_n(x)$ $v(x) = v_n(x);\ w(x) = w_n(x)$

Extended Euclidean Algorithm for Polynomials

Example:

GF(2^8) : $p(x) = a(x) = x^8 + x^4 + x^3 + x + 1$

$b(x) = x^7 + x + 1$

$a(x)v(x) + b(x)w(x) = d(x)$

Initialization	$a(x) = x^8 + x^4 + x^3 + x + 1$; $v_{-1}(x) = 1$; $w_{-1}(x) = 0$ $b(x) = x^7 + x + 1$; $v_0(x) = 0$; $w_0(x) = 1$
Iteration 1	$q_1(x) = x$; $r_1(x) = x^4 + x^3 + x^2 + 1$ $v_1(x) = 1$; $w_1(x) = x$ $a(x) mod\ b(x)$
Iteration 2	$q_2(x) = x^3 + x^2 + 1$; $r_2(x) = x$ $v_2(x) = x^3 + x^2 + 1$; $w_2(x) = x^4 + x^3 + x + 1$ $b(x) mod\ r_1(x)$
Iteration 3	$q_3(x) = x^3 + x^2 + x$; $r_3(x) = 1$ $v_3(x) = x^6 + x^2 + x + 1$; $w_3(x) = x^7$ $r_1(x) mod\ r_2(x)$
Iteration 4	$q_4(x) = x$; $r_4(x) = 0$ $v_4(x) = x^7 + x + 1$; $w_4(x) = x^8 + x^4 + x3 + x + 1$ $r_2(x) mod\ r_3(x)$
Result	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $w(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

$(x^8+x^4 + x^3 + x + 1)/(x^7 + x + 1)$

$v_1(x) = v_{-1}(x) - q_1(x)v_0(x) = 1$

$w_1(x) = w_{-1}(x) - q_1(x)w_0(x) = -q_1(x)$

$(x^7 + x + 1)/(x^4 + x^3 + x^2 + 1)$

$v_2(x) = v_0(x) - q_2(x)v_1(x)$

$w_2(x) = w_0(x) - q_2(x)w_1(x)$

$(x^4 + x^3 + x^2 + 1)/(x)$

$v_3(x) = v_1(x) - q_3(x)v_2(x)$

$w_3(x) = w_1(x) - q_3(x)w_2(x)$

$(x)/(1)$

$v_4(x) = v_2(x) - q_4(x)v_3(x)$

$w_4(x) = w_2(x) - q_4(x)w_3(x)$

Check:

$(x^7 + x + 1)(x^7) \bmod (x^8 + x^4 + x^3 + x + 1)=1$

Extended Euclidean Algorithm for Polynomials

Example: Prove that $f^{-1}(x) = x + 1$ is the multiplicative inverse of $f(x) = x^3 + x^2 + x$ for irreducible polynomial **GF(2^4) :** $\boldsymbol{p(x) = x^4 + x + 1}$

$$(x+1)(x^3+x^2+x) \bmod (\boldsymbol{x^4+x+1}) = 1$$

Extended Euclidean Algorithm for Polynomials

Example: Prove that $f^{-1}(x) = x^5 + x^3 + x^2 + x + 1$ is the multiplicative inverse of $f(x) = x^7 + x^6 + x$ for irreducible polynomial **GF(2^8) :** $\boldsymbol{p(x) = x^8 + x^4 + x^3 + x + 1}$

$$(x^5 + x^3 + x^2 + x + 1)(x^7 + x^6 + x) \bmod (\boldsymbol{x^8 + x^4 + x^3 + x + 1}) = 1$$