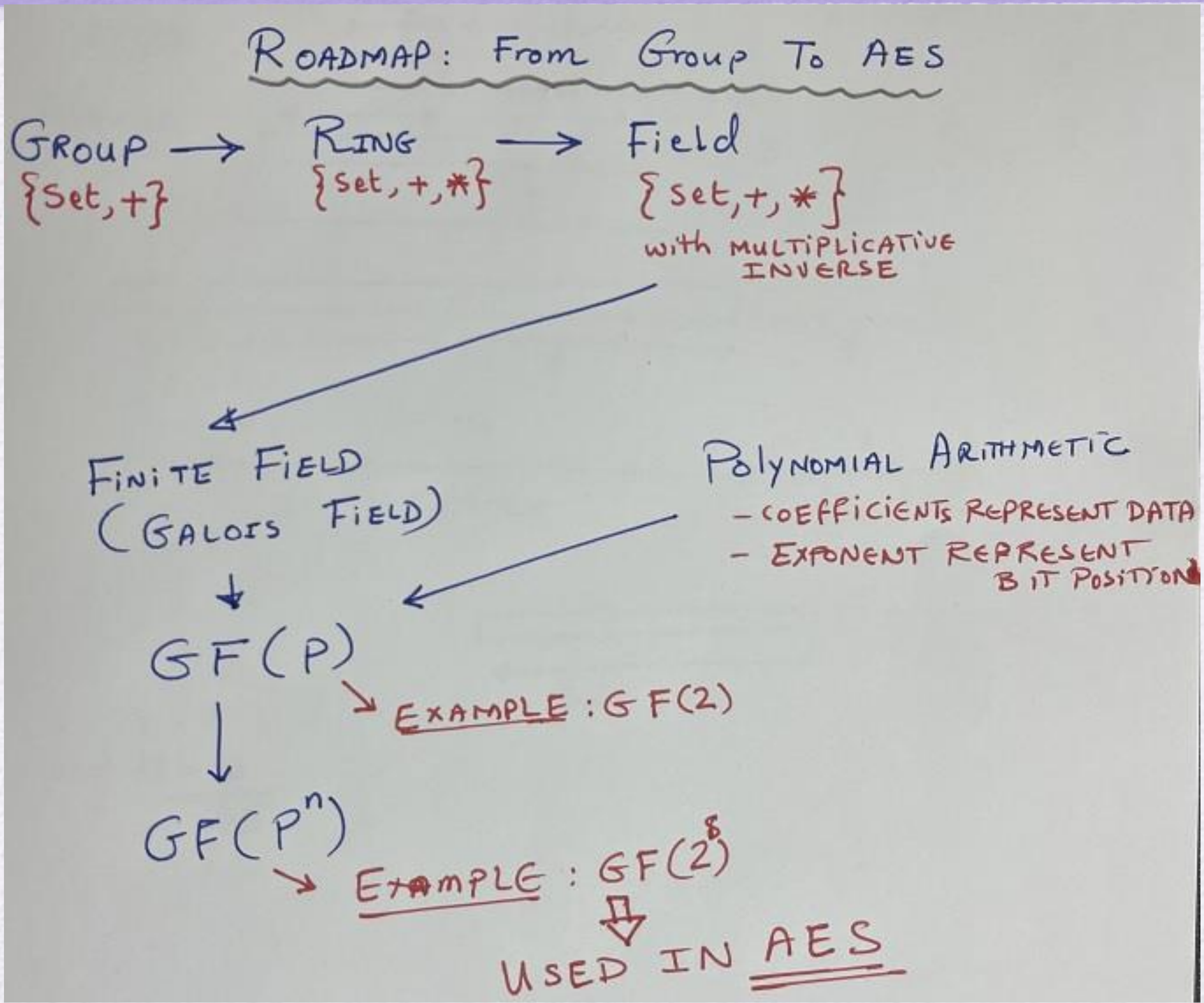
Chapter 5

Finite Fields

Roadmap To AES: Math Background



Abstract Algebra

- Groups, rings, and fields are fundamental **structures** of abstract algebra, or modern algebra.
- Example of Abstract Algebra: Boolean Algebra!
- Each **structure** in Abstract algebra consists of:
  - Sets of elements.
  - Operations:
    - Operations combine two elements of the set to obtain a third element of the set.
    - These operations are subject to specific rules, which define the nature of the set.
    - By convention, the notation for the two principal classes of operations on set elements is usually addition and multiplication.
  - In abstract algebra, we are not limited to ordinary arithmetical operations.

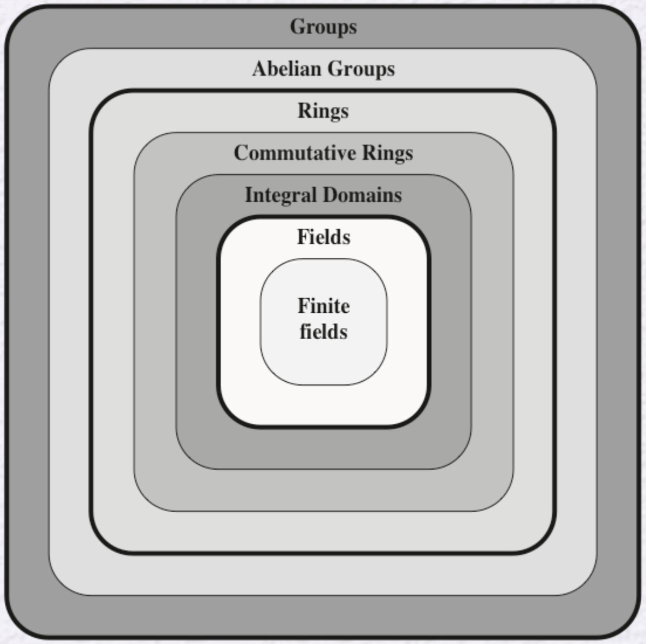


Figure 5.1 Groups, Rings, and Fields

Group, Ring and Field

- Rules for different structures in abstract algebra.
- Every field is a group.
- But, not every group is a field.

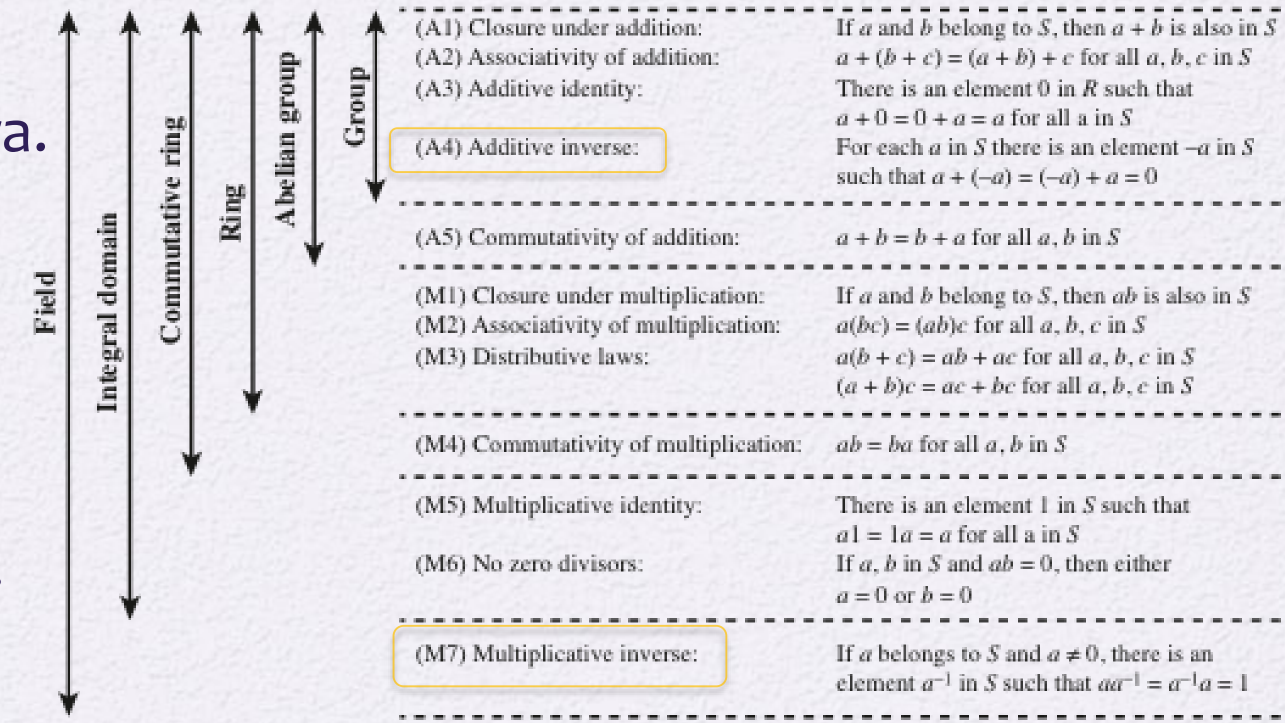


Figure 5.2 Properties of Groups, Rings, and Fields

Group: (set + operation+ axioms)

- A group (**G**) is a **set** of elements with a **binary operation** denoted by • that associates to each ordered pair (a,b) of elements in G an element $(a \bullet b)$ in G , such that the following **axioms** are obeyed:
- (A1) Closure:
  - If a and b belong to G, then $(a \bullet b)$ is also in G
- (A2) Associative:
  - $a \bullet (b \bullet c) = (a \bullet b) \bullet c$, for all a, b, c in G
- (A3) Identity element:
  - There is an element e in G such that: $a \bullet e = e \bullet a = a$, for all a in G
- (A4) Inverse element:
  - For each a in G, there is an element a^{1} in G such that $a \bullet a^{1} = a^{1} \bullet a = e$
- (A5) Commutative:
  - $a \bullet b = b \bullet a$ for all a, b in G

Cyclic Group

- Exponentiation is defined within a group as a repeated application of the group operator, so that $a^3 = a \bullet a \bullet a$
- We define $a^0 = \mathbf{e}$ as the identity element, and $a^{-n} = (a')^n$, where a' is the inverse element of a within the group
- A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$
- The element a is said to **generate** the group G or to be a **generator** of G
- A cyclic group is always abelian and may be finite or infinite
- Recall:
  - In Number theory lecture: **3** is a primitive root for **mod 7** multiplication.
  - This is because 3^k mod 7 generates numbers: 1 ..6
  - **We say: the group Z_n={1,2,3,4,5,6} is cyclic group under mod 7 multiplication, and 3 is a generator**

Ring : {R , + , * }

- A ring is a set in which we can do addition, subtraction $[a - b = a + (-b)]$, and multiplication without leaving the set.

- Formal definition: A **ring** R , sometimes denoted by {R , + , * }, is a **set** of elements **with two binary operations, called *addition* and *multiplication***, such that for all a , b , c in R the following **axioms** are obeyed:

  (A1–A5)

  ***R* is an abelian group** with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$

  (M1) Closure under multiplication:

  If a and b belong to 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

Rings (cont.)

- A ring is said to be commutative if it satisfies the following additional condition:

  (M4) Commutativity of multiplication:

  $ab = ba$ 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: {F, +,* }

- 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: $a/b = a(b^{-1})$

- A **field** F, sometimes denoted by {F, +,* }, is a **set** of elements with **two binary operations, called *addition* and *multiplication***, such that for all a, b, c in F the following axioms are obeyed:

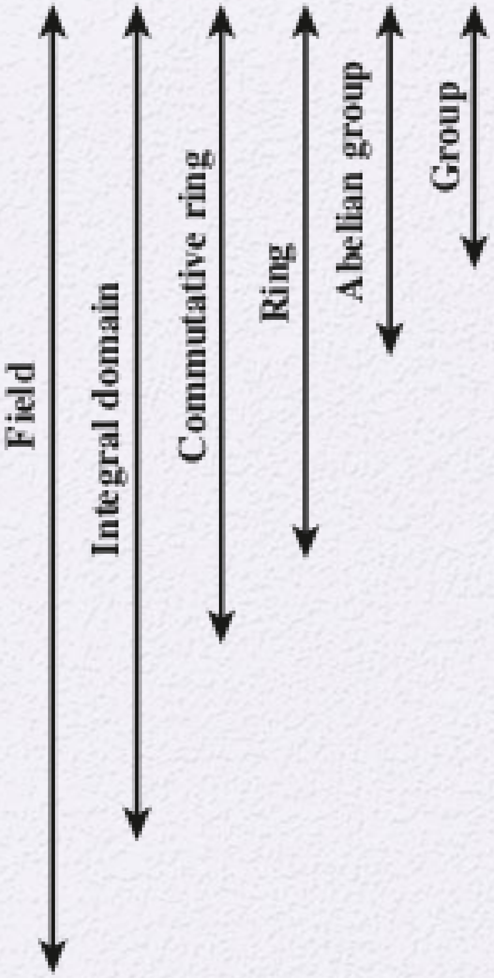
(A1–M6)

F is an **integral domain**; that is, F satisfies axioms A1 through A5 and M1 through M6

(M7) Multiplicative inverse:

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

> Familiar examples of fields are the rational numbers, the real numbers, and the complex numbers. Note that the set of all integers is not a field, because not every element of the set has a multiplicative inverse.



(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 $aa^{-1} = a^{-1}a = 1$

Figure 5.2 Properties of Groups, Rings, and Fields

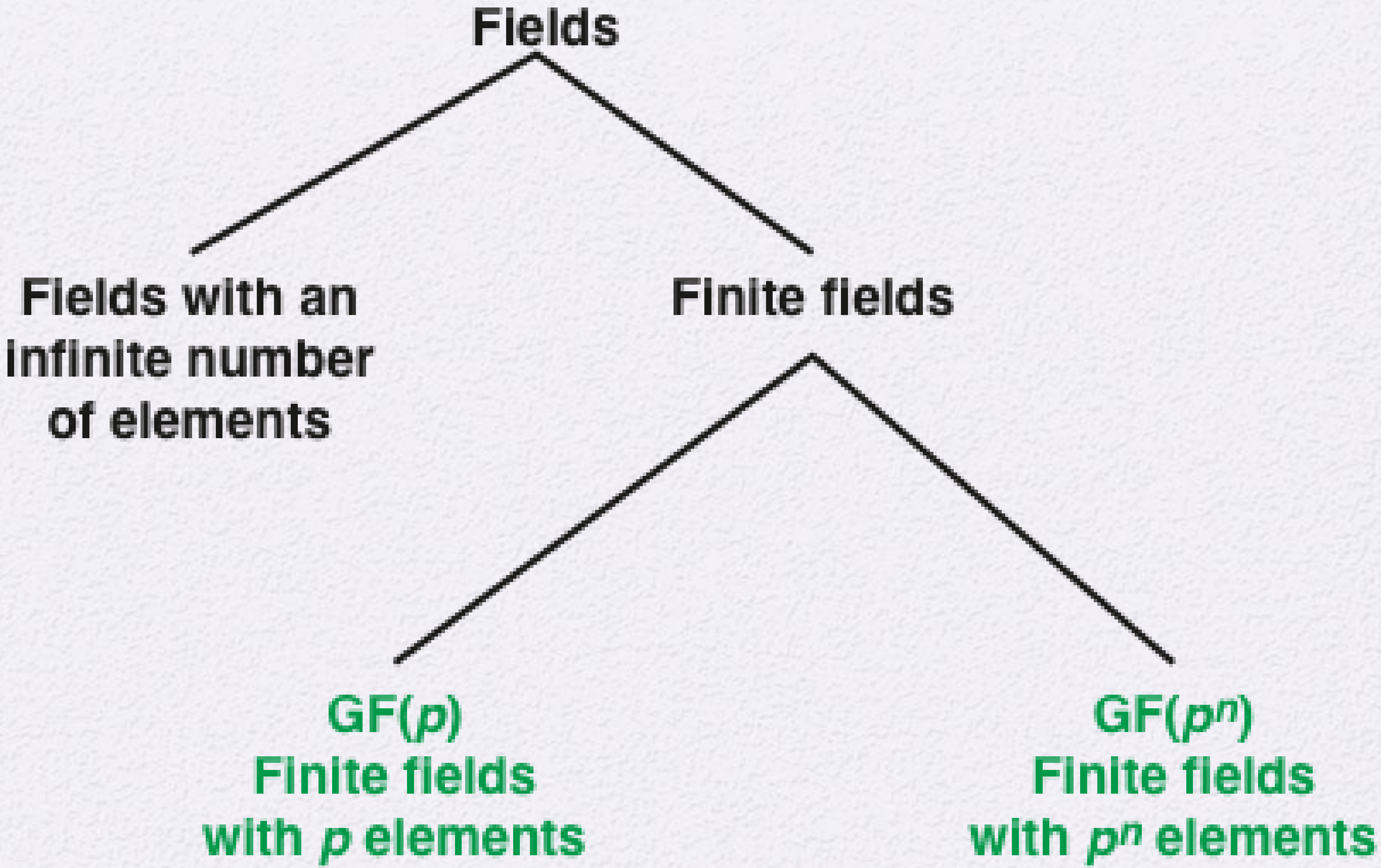


Figure 5.3 Types of Fields

Finite Fields of the Form GF(p^n)

- Finite fields play a crucial role in many cryptographic algorithms.
- GF stands for Galois field, in honor of the mathematician Galois (pronounced GALWA) who first studied finite fields
- The order of a finite field is the number of elements in the field.
  - The order must be of a power of prime (p^n), where n is a positive integer, p is a prime number.
  - The finite field of order p^n is generally written GF(p^n)

Special Cases of GF(p^n)

- We are interested in special cases of GF(p^n):
  - GF(p): n=1, and p is a prime
    - Finite filed of order p
  - GF(2): n=1, and p=2
    - represents 1-bit binary operations
  - GF(2^n): n>1, p=2
    - represents n-bit binary operations

GF(p): Finite field of order *p*, **where *p* is prime**

- GF(p) is defined with the following properties
  - 1. p is a prime
  - 2. GF(p) consists of p elements= $\{0, 1, \ldots, p - 1\}$
  - 3. The binary operations + and * are defined over the set.
    - operations are addition and multiplication **mod *p***
    - Addition, subtraction, multiplication, and division can be performed without leaving the set.
    - Each element of the set other than 0 has a **multiplicative inverse.**
  - In the next slides, will demonstrate that :
    - Example of : mod (non-prime number) is not a field.
    - Example of : *mod (p)* is a field

Modulu 8 : Not a field

+	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

×	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

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

Modulus 7: Finite Field

+	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

×	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

GF(7):
Operations are based on (mod 7)

2×4 (mod 7) $\equiv 1$
Hence:

- $\frac{1}{2} = 2^{-1}$ (mod 7) $\equiv 4$
- $\frac{1}{4} = 4^{-1}$ (mod 7) $\equiv 2$

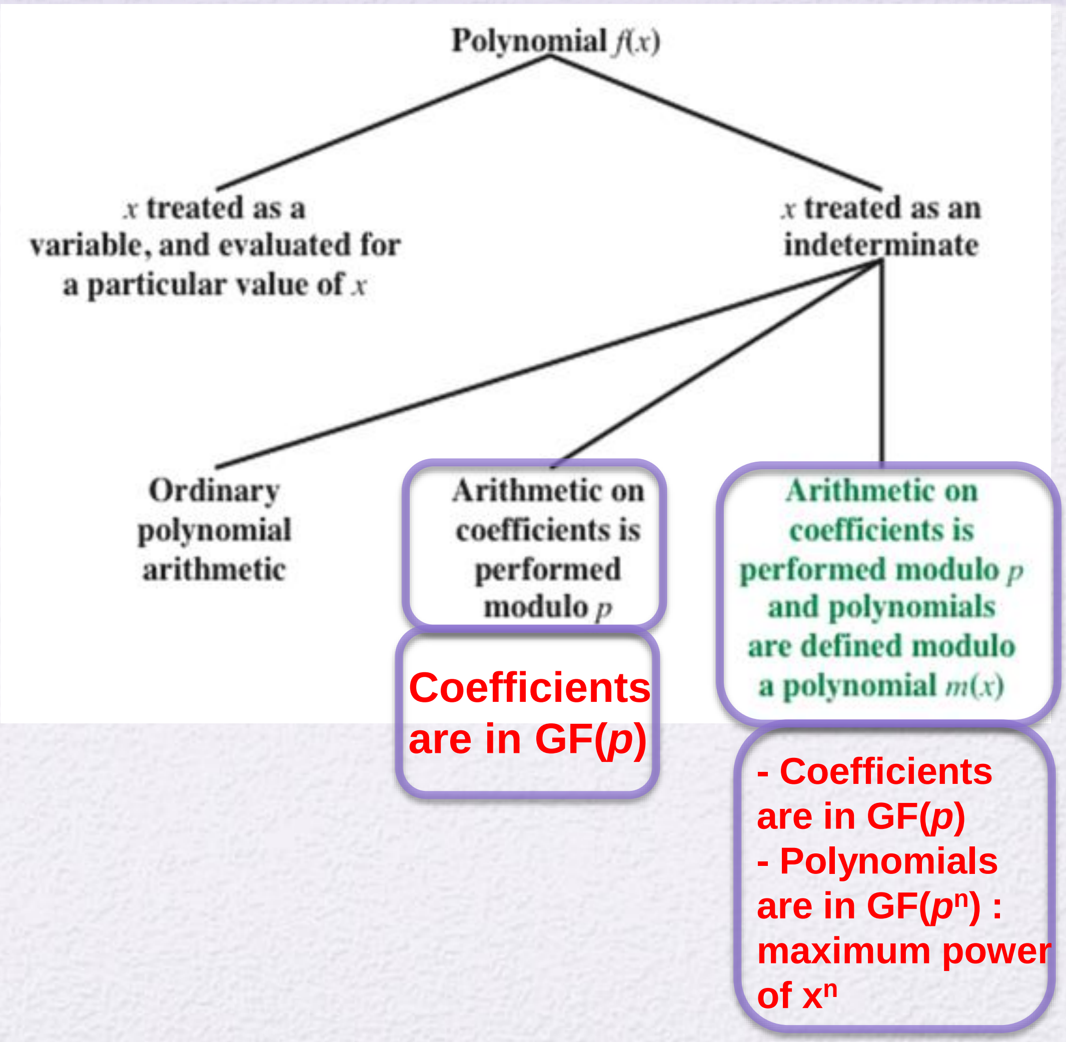
Compute $\frac{5}{2}$ (mod 7)?
$= \frac{5}{2}$ (mod 7)
$\equiv 5 \times 2^{-1}$ (mod 7)
$\equiv 5 \times 4$ (mod 7)
$\equiv 6$

Compute $2\times\frac{5}{2}$ (mod 7)?
$= 2\times\frac{5}{2}$ (mod 7)
$\equiv 2\times6$ (mod 7)
$\equiv 5$

Polynomial Arithmetic

- We are interested with polynomials in a single variable x, where x is treated as indeterminate. This means we are interested in the coefficients and power of variable x.
- We can distinguish three classes of polynomial arithmetic.

1. Ordinary polynomial arithmetic, using the basic rules of algebra.
2. Polynomial arithmetic in which the arithmetic on the coefficients is performed (mod p) ; that is, the coefficients are in GF(p).
3. Polynomial arithmetic in which:
    - the coefficients are in GF(p)
    - the polynomials are in GF(p^n): polynomial is defined modulo a polynomial m (x) whose highest power is some integer n .



GF(p) and GF(p^n)

- GF(p) means that polynomial coefficients are mod(p).
  - GF (2) means that polynomial coefficients are mod (2): 0 or 1
- GP (p^n) means that polynomials have maximum power of x^n. If polynomial has x^n or higher terms, then power is reduced by applying modulus operation using prime polynomial.
  - GP (2^n) means that polynomials have maximum power of x^{n-1}, and polynomial maps to n-bit binary number. If polynomial has 2^n or higher terms, then width is reduced by applying modulus operation using prime polynomial.

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

(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

$$
\begin{array}{r|l}
\multicolumn{1}{r}{} & \quad x + 2 \\
\cline{2-2}
x^2 - x + 1 & x^3 + x^2 \phantom{{}+x} + 2 \\
& x^3 - x^2 + x \\
\cline{2-2}
& \quad 2x^2 - x + 2 \\
& \quad 2x^2 - 2x + 2 \\
\cline{2-2}
& \quad\quad\quad x
\end{array}
$$

(d) Division

Figure 5.5 Examples of Polynomial Arithmetic

Polynomial Arithmetic With Coefficient Set in Z_p

- If each distinct polynomial is considered to be an element of the set, then that set is a ring
- When polynomial arithmetic is performed on polynomials over a field, then division is possible
  - Note: this does not mean that *exact division* is possible
- If we attempt to perform polynomial division over a coefficient set that is not a field, we find that division is not always defined
  - Even if the coefficient set is a field, polynomial division is not necessarily exact
  - With the understanding that remainders are allowed, we can say that polynomial division is possible if the coefficient set is a field

Polynomial Division

- We can write any polynomial in the form:

  $$f(x) = q(x)\, g(x) + r(x)$$

  - $r(x)$ can be interpreted as being a remainder

  ➔ $r(x) = f(x) \bmod g(x)$

- If there is no remainder we can say $g(x)$ **divides** $f(x)$
  - Written as $g(x) \mid f(x)$
  - We can say that $g(x)$ is a **factor** of $f(x)$
  - *Or* $g(x)$ is a **divisor** of $f(x)$

- A **prime polynomial (or irreducible polynomial) is** a polynomial $f(x)$ over a field F which cannot be expressed as a product of two polynomials.

Example of Polynomial Arithmetic Over GF(2)

- Addition of variable coefficients is bitwise XOR
- Multiplication of variable coefficients is bitwise AND
- Addition Example:

$$\begin{array}{rrr} & x & +\ 1 \\ x^2 & +\ x & \\ \hline x^2 & + & +\ 1 \end{array}$$

- Multiplication Example:

$$\begin{array}{rrrr} & x^2 & +\ x & +\ 1 \\ & & x & +\ 1 \\ \hline & x^2 & +\ x & +\ 1 \\ x^3 & +\ x^2 & +\ x & \\ \hline x^3 & & & +\ 1 \end{array}$$

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Figure 5.6 Examples of Polynomial Arithmetic over GF(2)

Polynomial GCD

- Polynomial GCD is the same as integer GCD.
  - We replace integers with polynomials

- The polynomial $c(x)$ is said to be the greatest common divisor of $a(x)$ and $b(x)$ if the following are true:
  - $c(x)$ divides both $a(x)$ and $b(x)$
  - Any divisor of $a(x)$ and $b(x)$ is a divisor of $c(x)$

- An equivalent definition is:
  - $c(x)=\gcd[a(x), b(x)]$ is the polynomial of maximum degree that divides both $a(x)$ and $b(x)$

- The Euclidean algorithm can be extended to find the greatest common divisor of two polynomials whose coefficients are elements of a field

Euclidean algorithm to compute the greatest common divisor of two polynomials

- Recall computing GCD for integers using mod operation. Will use same approach for polynomial

GCD (710, 310)=10

a	b	r= a mod b
710	310	90
310	90	40
90	40	10
40	10	0

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

Euclidean algorithm to compute the greatest common divisor of two polynomials using GP(2)

GCD (710, 310)=10

a	b	r= a mod b
710	310	90
310	90	40
90	40	10
40	10	0

GCD ($x^6+x^5+x^4+x^3+x^2+x+1$, x^4+x^2+x+1) = x^3+x^2+1

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 $b(x)$:

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

This yields $r_1(x) = x^3 + x^2 + 1$ and $q_1(x) = x^2 + x$.

Then, we divide $b(x)$ by $r_1(x)$.

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

This yields $r_2(x) = 0$ and $q_2(x) = x + 1$.

Therefore, $\gcd[a(x), b(x)] = r_1(x) = x^3 + x^2 + 1$.

GF(2^8) For AES

GF(2^8) operations maps to unsigned 8-bit XOR and AND operations.

In the following example, we demonstrate computation in:

- **GF(2^8) and**
- **Binary operations.**

In the example, the functions maps to the following values:

m(x)= 1 0 0 0 1 1 0 1 1

f(x) = 0 1 0 1 0 1 1 1

g(x) = 1 0 0 0 0 0 1 1

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

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

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

$$\begin{array}{r|l} & x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \hline & x^{11} + x^4 + x^3 \\ & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \hline & x^7 + x^6 + 1 \end{array}$$

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

GF(2^8) For AES

Addition:

GF(2^8) maps to unsigned 8-bit XOR and AND operations:

m(x)= 1 0001 1011

f(x) = 0 1 0 1 0 1 1 1

g(x) = 1 0 0 0 0 0 1 1

----

f+g = 1 1 0 1 0 1 0 0

The binary result maps to: $x^7 + x^6 + x^4 + x^2$

The largest power in the result is x^7 which less than x^8. So, no further action is required.

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

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

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

$$\begin{array}{r|l} & x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \hline & x^{11} + x^4 + x^3 \\ & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \hline & x^7 + x^6 + 1 \end{array}$$

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

GF(2^8) For AES

Multiplicatrion:

```
f(x) =   0 1 0 1   0 1 1 1
g(x) =  1 0 0 0   0 0 1 1
-----------------------------------
                    0 1 0 1 0 1 1 1
                  0 1 0 1 0 1 1 1
      0 1 0 1 0 1 1 1
--------------------------------------------------
  0  0 1 0 1 0 1 1 0 1 1 1 1 0 0 1
```

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

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

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

$$\begin{array}{r|l} & x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 \quad + x^6 + x^5 + x^4 + x^3 + 1 \\ & x^{13} \quad + x^9 + x^8 \quad + x^6 + x^5 \\ \hline & x^{11} \quad + x^4 + x^3 \\ & x^{11} \quad + x^7 + x^6 \quad + x^4 + x^3 \\ \hline & x^7 + x^6 \quad + 1 \end{array}$$

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

f × g maps to: $x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$

The power of f × g is larger than n=8.

Hence, we should compute f × g mod m(x)

$m(x) = x^8+x^4+x^3+x+1$

m(x) maps to : 1 0001 1011

GF(2^8) For AES

Below, we compute f(x)xg(x) mod (x) using binary math.
The result = x^7+x^6+1

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

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

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

$$\begin{array}{r|l} & x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \hline & x^{11} + x^4 + x^3 \\ & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \hline & x^7 + x^6 + 1 \end{array}$$

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

```
                           0 0 1 0 1
                          ______________________________
1 0 0 0 1 1 0 1 1        / 0 0 1 0 1 0 1 1 0 1 1 1 1 0 0 1
                             1 0 0 0 1 1 0 1 1
                           ______________________________
                             0 0 1 0 0 0 0 0 0 1 1 0 0 1
                                 1 0 0 0 1 1 0 1 1
                                 ________________________
                                       1 1 0 0 0 0 0 1
```

Arithmetic in GF(2^3): Addition

GF(2^3) field is constructed using prime polynomial : (X^3 + X+ 1)
Prime polynomial maps to binary number: 1011

		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

X (010)
$X^2 + X + 1$ (111)

$X^2 + 1$ (101)

$X^2 + X$ (110)
$X^2 + X + 1$ (111)
----
1 (001)

Arithmetic in GF(2^3): Multiplication

GF(2^3) field is constructed using prime polynomial : (X^3 + X+ 1)

		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

X (010)
X^2+ X + 1 (111)

X^3 + X^2+ X (1110)

Since the result has power equal or greater than n=3, then we should compute remainder using the prime polynomial.

(X^3 + X^2+ X) mod (X^3 + X+ 1)
= (X^2 + 1) (101)

Arithmetic in GF(2^3) Using prime polynomial : ($X^3 + X + 1$)

Summary

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

Polynomial Arithmetic Modulo ($x^3 + x + 1$)

GF(2^3) field is constructed using prime polynomial : ($X^3 + X + 1$)

	+	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+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	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+x	x^2	$x+1$

(b) Multiplication

Extended Euclid (read)

- Just as the Euclidean algorithm is used to find the greatest common divisor of two polynomials, **the extended Euclidean algorithm is used to find the multiplicative inverse of a polynomial.**
- Algorithm computes multiplicative inverse of

  ***b*(*x*) modulo *a*(*x*)**

  if :

  - degree of b(x) is less than the degree of a(x) and
  - gcd[a(x), b(x)] = 1

Extended Euclid [$(x^8 + x^4 + x^3 + x + 1), (x^7 + x + 1)$]

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

Computational Considerations

- Since coefficients are 0 or 1, they can represent any such polynomial as a bit string
- Addition becomes XOR of these bit strings
- Multiplication is shift and XOR
  - cf long-hand multiplication
- Modulo reduction is done by repeatedly substituting highest power with remainder of irreducible polynomial (also shift and XOR)

Defining GF(2^n) using a **Generator**

- **Generator** is another way of defining GF(2^n).
- A **generator** g of a finite field *F* of order *q* (contains *q* elements) is:
  - an element whose first *q*-1 powers generate all the nonzero elements of F.
  - The elements of F consist of: $\{0, g^0, g^1, \ldots, g^{q-2}\}$; where: $g^0 = g^{q-1} = 1$
- Consider a field *F* defined by a polynomial *f(x):* an element ***b*** contained in F is called a **root** of the polynomial if *f(b)* = *0*
- Finally, it can be shown that a root **g** of an irreducible polynomial is a generator of the finite field defined on that polynomial

Generator Example for GF(2^3) using: $f(x)=x^3 + x + 1$

- Assume F is defined by the prime (irreducible) polynomial = $x^3 + x + 1$
- g= 010 ; which represents: x
- **g** *is a* root and computed by plugging **g** in $f(x)=x^3 + x + 1$
- Order of the field = number of elements = $q=7$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
g^0 (= g^7)	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

When exponent is 3 or more, them we determine answer by taking:
mod (g^3 + g + 1)
For example:
$g^3 = g^3$ **mod (g^3+ g+1)**
= g + 1

Generator Example for GF(2^3) using: $f(x)=x^3 + x + 1$

- $g^0 = 1$, which maps to 001
- $g^1 = g$, which maps to 010
- $g^2 = g.g$, which maps to 100
- g^3:
  - If **g** is a generator, then it must satisfy :

    $f(g)=g^3 + g + 1 = 0$

    $g^3 = -g - 1 = g + 1$

  Note: addition and subtraction are the same.
- $g^4 = g.g^3 = g(g+1) = g^2 + g$, which maps to 110
- …. .

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
g^0 (= g^7)	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Power representation Makes Math easy

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
g^0 (= g^7)	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Example: compute $g^4 \times g^6$:

- Easy way:
  - Power representation: $g^4 \times g^6 = g^{10 \bmod q} = g^{10 \bmod 7} = g^3 = g+1$
- Harder way:
  - $g^4 = g^2+g$
  - $g^6 = g^2+1$
  - $g^4 \times g^6 = g^4+g^3+g^2+1$
  - $(g^4+g^3+g^2+1) \bmod (g^3+g+1)$

  $= g+1$

$$
\begin{array}{r@{\,}l}
 & g \quad + 1 \\
g^3+g+1 \,\big) & \overline{g^4 + g^3 + g^2 + g} \\
 & \underline{g^4 \qquad\;\; + g^2 + g} \\
 & \qquad g^3 \\
 & \qquad \underline{g^3 + \qquad g + 1} \\
 & \qquad\qquad\quad\; g + 1
\end{array}
$$

GF(2^3) Arithmetic Using Generator for the Polynomial ($x^3 + x + 1$)

power representation

polynomial representation

		000	001	010	100	011	110	111	101
	+	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
001	1	1	0	$g+1$	g^2+1	g	g^2+g+1	g^2+g	g^2
010	g	g	$g+1$	0	g^2+g	1	g^2	g^2+1	g^2+g+1
100	g^2	g^2	g^2+1	g^2+g	0	g^2+g+1	g	$g+1$	1
011	g^3	$g+1$	g	1	g^2+g+1	0	g^2+1	g^2	g^2+g
110	g^4	g^2+g	g^2+g+1	g^2	g	g^2+1	0	1	$g+1$
111	g^5	g^2+g+1	g^2+g	g^2+1	$g+1$	g^2	1	0	g
101	g^6	g^2+1	g^2	g^2+g+1	1	g^2+g	$g+1$	g	0

(a) Addition

		000	001	010	100	011	110	111	101
	×	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
010	g	0	g	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1
100	g^2	0	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g
011	g^3	0	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g	g^2
110	g^4	0	g^2+g	g^2+g+1	g^2+1	1	g	g^2	$g+1$
111	g^5	0	g^2+g+1	g^2+1	1	g	g^2	$g+1$	g^2+g
101	g^6	0	g^2+1	1	g	g^2	$g+1$	g^2+g	g^2+g+1

(b) Multiplication

Multiplicative Inverse in GF(2^n)

- Consider the last example of GF(2^3) Arithmetic
- g^5 is the multiplicative inverse of g^2
  - g^5 corresponds to 111 (i.e. x^2+x+1)
  - g^2 corresponds to 100 (i.e. x^2)
  - This implies:
    - $(x^2+x+1) . (x^2)$ mod $(x^3 + x + 1) \equiv 1$
    - (111) . (100) mod $(x^3 + x + 1) \equiv 1$

		000	001	010	100	011	110	111	101
	×	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$
010	g	0	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1
100	g^2	0	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g
011	g^3	0	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2
110	g^4	0	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2	$g + 1$
111	g^5	0	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2	$g + 1$	$g^2 + g$
101	g^6	0	$g^2 + 1$	1	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$

Multiplicative Inverse in GF(2^8)

- Multiplicative inverse table in GF(2^8) for bytes xy **used within the AES S-Box**
  - Prime polynomial = $x^8+x^4+x^3+x+1$

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Multiplicative Inverse in GF(2^8)

Example . From Table , the inverse of

$$x^7 + x^6 + x = (11000010)_2 = (C2)_{hex} = (xy)$$

is given by the element in row C, column 2:

$$(2F)_{hex} = (00101111)_2 = x^5 + x^3 + x^2 + x + 1.$$

This can be verified by multiplication:

$$(x^7 + x^6 + x) \cdot (x^5 + x^3 + x^2 + x + 1) \equiv 1 \mod P(x)$$

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Summary

- Groups
  - Abelian group
  - Cyclic group
- Finite fields of the form GF(p)
  - Finite fields of Order p
  - Finding the multiplicative inverse in GF(p)
- Polynomial arithmetic
  - Ordinary polynomial arithmetic
  - Polynomial arithmetic with coefficients in Z_p
  - Finding the greatest common divisor

- Rings
- fields
- Finite fields of the form GF(2^n)
  - Motivation
  - Modular polynomial arithmetic
  - Finding the multiplicative inverse
  - Computational considerations
  - Using a generator