AES Arithmetic

- **Finite Field:** A field with finite number of elements, also known as **Galois Field**.
- The number of elements is always a power of a prime number, denoted as $GF(p^n)$.
- $GF(p)$ is the set of integers $\{0, 1, \ldots, p-1\}$ with arithmetic operations modulo prime p.
- Addition, subtraction, multiplication, and division can be done without leaving the field $GF(p)$.
  E.g. $GF(2)$ = mod 2 arithmetic and $GF(8)$ = mod 8 arithmetic.
- AES uses arithmetic in the finite field $GF(2^8)$ with irreducible (prime) polynomial.
  $m(x) = x^8 + x^4 + x^3 + x + 1$ which is (1 0001 1011) in binary or {11B} in Hex-decimal
- **Irreducible polynomial** is a polynomial that is not a product of two other polynomials.

- **Example: Find arithmetic multiplication in $GF(2^8)$ for the following:**

1- {02} • {87} mod {11B} = (0000 0010)(1000 0111) mod (1 0001 1011)

$$= x\,(x^7 + x^2 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$= (x^8 + x^3 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$= x^4 + x^2 + 1 = (0001\ 0101)$$

2- {03} •{6E} mod {11B} = (11)(110 1110) mod (1 0001 1011)

$$= (x + 1)\,(x^6 + x^5 + x^3 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$= (x^7 + x^6 + x^4 + x^3 + x^2 + x^6 + x^5 + x^3 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$= x^7 + x^5 + x^4 + x = \{1011\ 0010\}$$

Polynomial Arithmetic

❑ Polynomial arithmetic operations:

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

Then,

(**Addition**) f(x) + g(x) = $x^3 + x + 1$

(**Multiplication**) f(x) × g(x) = $x^5 + x^2$

$$
\begin{array}{ccccccccc}
(x^2 & + & x & + & 1) & \times & (x^3 + x^2) \\
\hline
x^5 & + & x^4 & + & x^3 & & \\
 & + & x^4 & + & x^3 & + & x^2 \\
\hline
x^5 & + & & & & + & x^2
\end{array}
$$

Polynomial Division: f(x) = q(x) g(x) + r(x) where q(x) is quotient, g(x) is divisor, r(x) is remainder

Let f(x) = $x^3 + x + 1$, and g(x) = x + 1,

(Division) r(x) = remainder = f(x) mod g(x)

q(x) = $x^2 + x$ (quotient) , g(x) = x + 1 (modular polynomial),

r(x) = 1

then f(x) / g(x) is computed as

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

Polynomial Arithmetic

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

(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	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

(b) Multiplication

		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	$x+1$

When (A + B) mod n = 0, then B is called additive inverse mod n of A
e.g. from the table (a), additive inverse of ($x^2 + x$) is ($x^2 + x$)
When (A × B) mod n = 1, then B is called multiplicative inverse mod n of A
e.g. from the table (b), multiplicative inverse of (x) is ($x^2 + 1$)

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

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 $b(x)$:

$$
\begin{array}{r@{\,}l}
 & x^2 + x \\
x^4 + x^2 + x + 1 \big) & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & \underline{x^6 \phantom{{}+x^5} + x^4 + x^3 + x^2} \\
 & \phantom{x^6+{}} x^5 \phantom{{}+x^4+x^3+x^2} + x + 1 \\
 & \phantom{x^6+{}} \underline{x^5 \phantom{{}+x^4} + x^3 + x^2 + x \phantom{{}+1}} \\
 & \phantom{x^6+x^5+x^4+{}} x^3 + x^2 \phantom{{}+x} + 1
\end{array}
$$

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

$$
\begin{array}{r@{\,}l}
 & x + 1 \\
x^3 + x^2 + 1 \big) & x^4 \phantom{{}+x^3} + x^2 + x + 1 \\
 & \underline{x^4 + x^3 \phantom{{}+x^2} + x} \\
 & \phantom{x^4+{}} x^3 + x^2 \phantom{{}+x} + 1 \\
 & \phantom{x^4+{}} \underline{x^3 + x^2 \phantom{{}+x} + 1}
\end{array}
$$

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