Basic Number Theory and Finite Fields

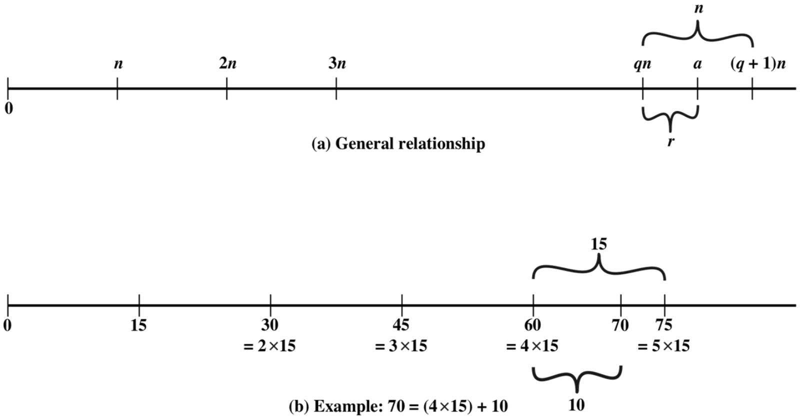
Yih-Kuen Tsay

Department of Information Management
National Taiwan University

Divisibility and Division

- We say a nonzero integer b divides another integer a, denoted as $b|a$, if $a = mb$ for some integer m.
- When an integer a is divided by a positive integer n, we get a unique integer quotient q and a unique integer remainder r such that
$$a = qn + r \quad 0 \leq r < n, q = \lfloor a/n \rfloor.$$
- The remainder r is also referred to as a *residue*.

Quotient and Remainder



(a) General relationship

(b) Example: 70 = (4×15) + 10

Source: Figure 4.1, Stallings 2014

Essence of the Euclidean Algorithm

IM NTU

- Given two integers a and b such that $a \geq b > 0$.
- Let $a = qb + r$, where $0 \leq r < b$.
- There are two cases:
  - If $r = 0$, then we know immediately $\gcd(a, b) = b$ and stop.
  - If $r \neq 0$, repeat the steps above with b as a and r as b.
- In both cases, the equality $\gcd(a, b) = \gcd(b, r)$ holds.
- We prove the equality by showing that $\gcd(b, r) \leq \gcd(a, b)$ and $\gcd(a, b) \leq \gcd(b, r)$.

Essence of the Euclidean Algorithm (cont.)

- We first show that $\gcd(b, r) \leq \gcd(a, b)$.
  - Consider $a = qb + r$.
  - Since $\gcd(b, r) | b$ and $\gcd(b, r) | r$, we have $\gcd(b, r) | a$.
  - Both $\gcd(b, r) | a$ and $\gcd(b, r) | b$; so, $\gcd(b, r) \leq \gcd(a, b)$.
- We next show that $\gcd(a, b) \leq \gcd(b, r)$.
  - Consider $r = a - qb$.
  - Since $\gcd(a, b) | a$, and $\gcd(a, b) | b$, we have $\gcd(a, b) | r$.
  - Both $\gcd(a, b) | b$ and $\gcd(a, b) | r$; so, $\gcd(a, b) \leq \gcd(b, r)$.

Modular Arithmetic

The remainder r from dividing a by n (> 0) is usually denoted by "$a \bmod n$".

$$a = qn + (a \bmod n) \qquad q = \lfloor a/n \rfloor.$$

$$11 \bmod 7 = 4 \text{ (because } 11 = 1 \times 7 + 4).$$

$$-11 \bmod 7 = 3 \text{ (because } -11 = -2 \times 7 + 3).$$

Congruence Modulo N

- Two integers a and b are *congruent modulo n* ($n > 0$), denoted as $a \equiv b \pmod{n}$, if $a \bmod n = b \bmod n$.
- The positive integer n is called the *modulus* of the congruence relation.
- If $a \equiv 0 \pmod{n}$, then $n|a$; and vice versa.
- If $a \equiv b \pmod{n}$, then $n|(a - b)$; and vice versa.

Modular Arithmetic Operations

Properties:

$$
\begin{aligned}
((a \bmod n) + (b \bmod n)) \bmod n &= (a + b) \bmod n \\
((a \bmod n) - (b \bmod n)) \bmod n &= (a - b) \bmod n \\
((a \bmod n) \times (b \bmod n)) \bmod n &= (a \times b) \bmod n
\end{aligned}
$$

Applications:

$$
\begin{aligned}
& 11^7 \pmod{13} \\
\equiv\ & (11 \times 11^2 \times 11^4) \pmod{13} \\
\equiv\ & (11 \pmod{13}) \times (11^2 \pmod{13}) \times (11^4 \pmod{13}) \\
\equiv\ & (11 \pmod{13}) \times (4 \pmod{13}) \times (3 \pmod{13}) \\
\equiv\ & (11 \times 4 \times 3) \pmod{13} \\
\equiv\ & 2 \pmod{13}
\end{aligned}
$$

Arithmetic Modulo 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

Source: Table 4.2, Stallings 2014

Arithmetic Modulo 8 (cont.)

×	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

Source: Table 4.2, Stallings 2014

Arithmetic Modulo 8 (cont.)

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

Source: Table 4.2, Stallings 2014

Residue Classes

Let Z_n denote the set of nonnegative integers less than n:

$$Z_n = \{0, 1, 2, \cdots, (n-1)\}.$$

This is referred to as the set of residues, or *residue classes*, modulo n.

Each integer r in Z_n represents a residue class $[r]$, where

$$[r] = \{a : \ a \text{ is an integer}, a \equiv r \pmod{n}\}.$$

For example, if the modulus is 4, then

$$[1] = \{\cdots, -7, -3, 1, 5, 9, 13, \cdots\}.$$

Principles of Modular Arithmetic

If $(a+b) \equiv (a+c) \pmod{n}$, then $b \equiv c \pmod{n}$.

If $(a \times b) \equiv (a \times c) \pmod{n}$, then $b \equiv c \pmod{n}$, only when a is relatively prime to n.

Z_8	0	1	2	3	4	5	6	7
Multiplied by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

$(6 \times 3) \equiv (6 \times 7) \pmod{8}$, but $3 \not\equiv 7 \pmod{8}$.

Z_8	0	1	2	3	4	5	6	7
Multiplied by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

Modular Arithmetic in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Source: Table 4.3, Stallings 2014

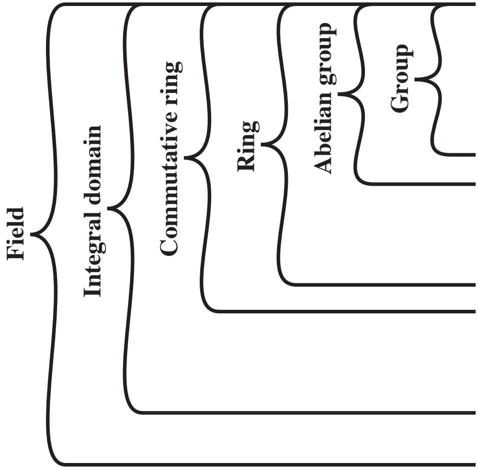
Finding the Multiplicative Inverse

$EXTENDED\ EUCLID(a, b):$

1. $(X_1, Y_1, R_1) \leftarrow (1, 0, a); (X_2, Y_2, R_2) \leftarrow (0, 1, b)$
2. if $R_2 = 0$ then return $R_1 = \gcd(a, b)$; no inverse
3. if $R_2 = 1$ then return $R_2 = \gcd(a, b)$; $Y_2 = b^{-1} \pmod a$
4. $Q = \lfloor R_1/R_2 \rfloor$
5. $(X, Y, R) \leftarrow (X_1 - QX_2, Y_1 - QY_2, R_1 - QR_2)$
6. $(X_1, Y_1, R_1) \leftarrow (X_2, Y_2, R_2)$
7. $(X_2, Y_2, R_2) \leftarrow (X, Y, R)$
8. goto 2

- Invariants: $aX_1 + bY_1 = R_1$ and $aX_2 + bY_2 = R_2$.
- If $\gcd(a, b) = 1$, then Y_2 equals the multiplicative inverse of b modulo a when the algorithm terminates.
  $aX_2 + bY_2 = R_2 = 1 \rightarrow bY_2 = 1 - aX_2 \rightarrow bY_2 \equiv 1 \bmod a$.

Groups, Rings, and Fields



(A1) Closure under addition:
(A2) Associativity of addition:
(A3) Additive identity:
(A4) Additive inverse:
(A5) Commutativity of addition:
(M1) Closure under multiplication:
(M2) Associativity of multiplication:
(M3) Distributive laws:
(M4) Commutativity of multiplication:
(M5) Multiplicative identity:
(M6) No zero divisors:
(M7) Multiplicative inverse:

Source: Figure 4.2, Stallings 2010

Groups, Rings, and Fields (cont.)

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

Source: Figure 4.2, Stallings 2010

Z_p

- Consider $Z_p = \{0, 1, 2, \cdots, (p-1)\}$ where p is a prime.
- For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod{p}$.
- The element z is called the *multiplicative inverse* of w.
- For any prime p, $(Z_p, +, \times)$ is a finite field of order p, denoted $GF(p)$.

Arithmetic in $GF(7)$

+	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

Source: Table 4.5, Stallings 2014

Arithmetic in $GF(7)$ (cont.)

×	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

Source: Table 4.5, Stallings 2014

Arithmetic in $GF(7)$ (cont.)

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

Source: Table 4.5, Stallings 2014

Polynomial Arithmetic

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

(a) Addition

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

(b) Subtraction

$$
\begin{array}{r}
x^3 + x^2 \qquad\quad + 2 \\
\times \;(x^2 - x + 1) \\
\hline
x^3 + x^2 \qquad\quad + 2 \\
- x^4 - x^3 \qquad\quad - 2x \qquad\qquad \\
x^5 + x^4 \qquad\quad + 2x^2 \qquad\qquad\qquad\quad \\
\hline
x^5 \qquad\qquad\qquad + 3x^2 - 2x + 2
\end{array}
$$

(c) Multiplication

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

(d) Division

Source: Figure 4.3, Stallings 2014

Polynomial Arithmetic over $GF(2)$

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

(a) Addition

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

(b) Subtraction

Source: Figure 4.4, Stallings 2014

Polynomial Arithmetic over $GF(2)$ (cont.)

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

(c) Multiplication

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

(d) Division

Source: Figure 4.4, Stallings 2014

Arithmetic in $GF(2^3)$

		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

Source: Table 4.6, Stallings 2014

Arithmetic in $GF(2^3)$ (cont.)

		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

Source: Table 4.6, Stallings 2014

Arithmetic in $GF(2^3)$ (cont.)

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

Source: Table 4.6, Stallings 2014

Modular Polynomial Arithmetic

- Let S denote the set of all polynomials of degree $n-1$ or less over the field Z_p with the form

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

  where each a_i takes on a value in Z_p. Arithmetic on the coefficients is performed modulo p.
- If multiplication results in a polynomial of degree greater than $n-1$, then the polynomial is reduced modulo some irreducible polynomial of degree n.
- Each such S is a finite field; every nonzero element a in S has a multiplicative inverse a^{-1} such that $a \times a^{-1} = 1$.
- Such an S is denoted as GF(2^n) when $p = 2$.

Irreducible Polynomials

- A polynomial $f(x)$ is *irreducible* if $f(x)$ cannot be expressed as a product of two polynomials with degrees lower than that of $f(x)$.
- Irreducible polynomials play a role analogous to that of primes.
- The AES algorithm uses the finite field $\mathrm{GF}(2^8)$ with the following irreducible polynomial modulus

$$x^8 + x^4 + x^3 + x + 1.$$

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

		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

Source: Table 4.7, Stallings 2014

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

		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	$x+1$

Source: Table 4.7, Stallings 2014

Extended Euclid's Algorithm for GF(p^n)

$EXTENDED\ EUCLID(a(x), b(x))$:

1. $[V_1(x), W_1(x), R_1(x)] \leftarrow [1, 0, a(x)]; [V_2(x), W_2(x), R_2(x)] \leftarrow [0, 1, b(x)]$
2. if $R_2(x) = 0$ then return $R_1(x) = \gcd(a(x), b(x))$; no inverse
3. if $R_2(x) = 1$ then return $R_2(x) = \gcd(a(x), b(x)); W_2(x) = b^{-1}(x) \pmod{a(x)}$
4. $Q(x) =$ the quotient of $R_1(x)/R_2(x)$
5. $[V(x), W(x), R(x)]$
   $\leftarrow [V_1(x) - Q(x)V_2(x), W_1(x) - Q(x)W_2(x), R_1(x) - Q(x)R_2(x)]$
6. $[V_1(x), W_1(x), R_1(x)] \leftarrow [V_2(x), W_2(x), R_2(x)]$
7. $[V_2(x), W_2(x), R_2(x)] \leftarrow [V(x), W(x), R(x)]$
8. goto 2

- Invariants: $a(x)V_1(x) + b(x)W_1(x) = R_1(x)$ and $a(x)V_2(x) + b(x)W_2(x) = R_2(x)$.
- If $\gcd(a(x), b(x)) = 1$, then $W_2(x)$ equals the multiplicative inverse of $b(x)$ modulo $a(x)$ when the algorithm terminates.

A Run of Extended Euclid

The following run finds the multiplicative inverse of $x^7 + x + 1$ in GF(2^8) with $x^8 + x^4 + x^3 + x + 1$ as the irreducible polynomial modulus; the result is x^7.

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	$q_4(x) = x$; $r_4(x) = 0$ $v_4(x) = x^7 + x + 1$; $w_4(x) = x^8 + x^4 + x^3 + x + 1$
Result	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $w(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

Source: Table 4.8, Stallings 2014

Bytes and Polynomials in GF(2^8)

- In the AES algorithm, the basic unit for processing is a byte.
- A byte $b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$ is interpreted as an element of the finite field GF(2^8) using the polynomial representation:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^{7} b_i x^i .$$

- For example, 01100011 identifies $x^6 + x^5 + x + 1$.

Addition in GF(2^8)

IM NTU

- The addition of two polynomials in the finite field GF(2^8) is achieved by adding (modulo 2) the coefficients of the corresponding powers.

polnomial representation:

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

binary representation:

$$01010111 \oplus 10000011 = 11010100$$

hexadecimal representation:

$$\{57\} \oplus \{83\} = \{D4\}$$

Multiplication in $\mathbf{GF}(2^8)$

- Let $f(x)$ be $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$.
- Multiply $f(x)$ by x, we have

$$
\begin{aligned}
& f(x) \times x \\
= \; & b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \\
& \bmod m(x)
\end{aligned}
$$

  Again, for the AES algorithm,

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

- When $b_7 = 0$, the result is already in the reduced form.

Multiplication in GF(2^8) (cont.)

- When $b_7 = 1$:

$$
\begin{array}{rll}
& f(x) \times x & \\
= & (x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0) \times x & \mod m(x) \\
= & x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x & \mod m(x) \\
= & (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + & \\
& (x^4 + x^3 + x + 1) & \mod m(x)
\end{array}
$$

Note: $x^8 \mod m(x) = m(x) - x^8 = x^4 + x^3 + x + 1$.

- To summarize in binary representation,

$$
f(x) \times x = \begin{cases} (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) & \text{if } b_7 = 0 \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus (00011011) & \text{if } b_7 = 1 \end{cases}
$$

- Repeat the above to get multiplications by x^2, x^3, etc.

Cyclic Groups

- Let a^n denote $a \cdot a \cdot \cdots \cdot a$ with n (≥ 0) occurrences of a. Formally,

$$a^n = \begin{cases} e & \text{if } n = 0 \\ a \cdot a^{n-1} & \text{if } n > 0 \end{cases}$$

- A group G is *cyclic* if, for every b in G, $b = a^n$ for a fixed a in G and some integer $n \geq 0$.
- The fixed element a is said to *generate* G and is called the *generator* of G.

Generators for Finite Fields

A generator for GF(2^3) using $f(x) = x^3 + x + 1$ (irreducible):

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

Source: Table 4.9, Stallings 2014

Note: $f(g) = g^3 + g + 1 = 0$, $g^3 = -g - 1 = g + 1$,
$g^4 = g(g^3) = g(g+1) = g^2 + g$, etc.

GF(2^3) Arithmetic Using a Generator

		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

Source: Table 4.10, Stallings 2014

GF(2^3) Arithmetic Using a Generator (cont.)

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

Source: Table 4.10, Stallings 2014