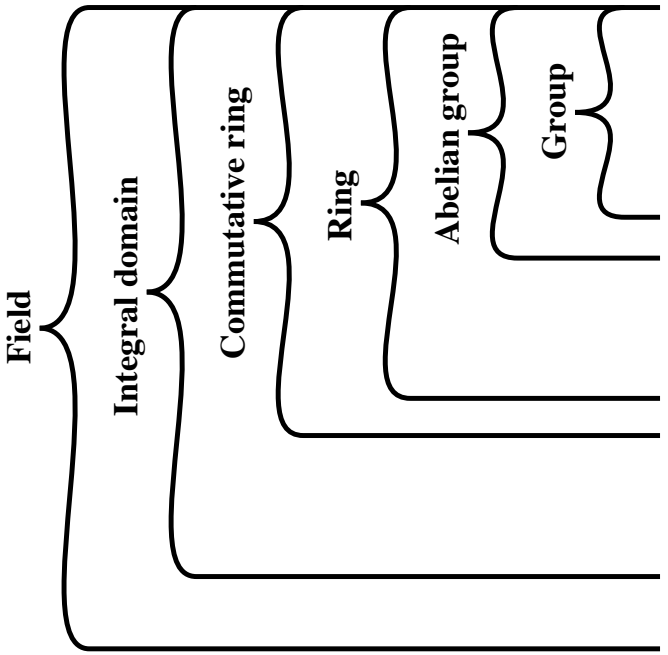
Finite Fields

Tsay, Yih-Kuen

Dept. of Information Management

National Taiwan University

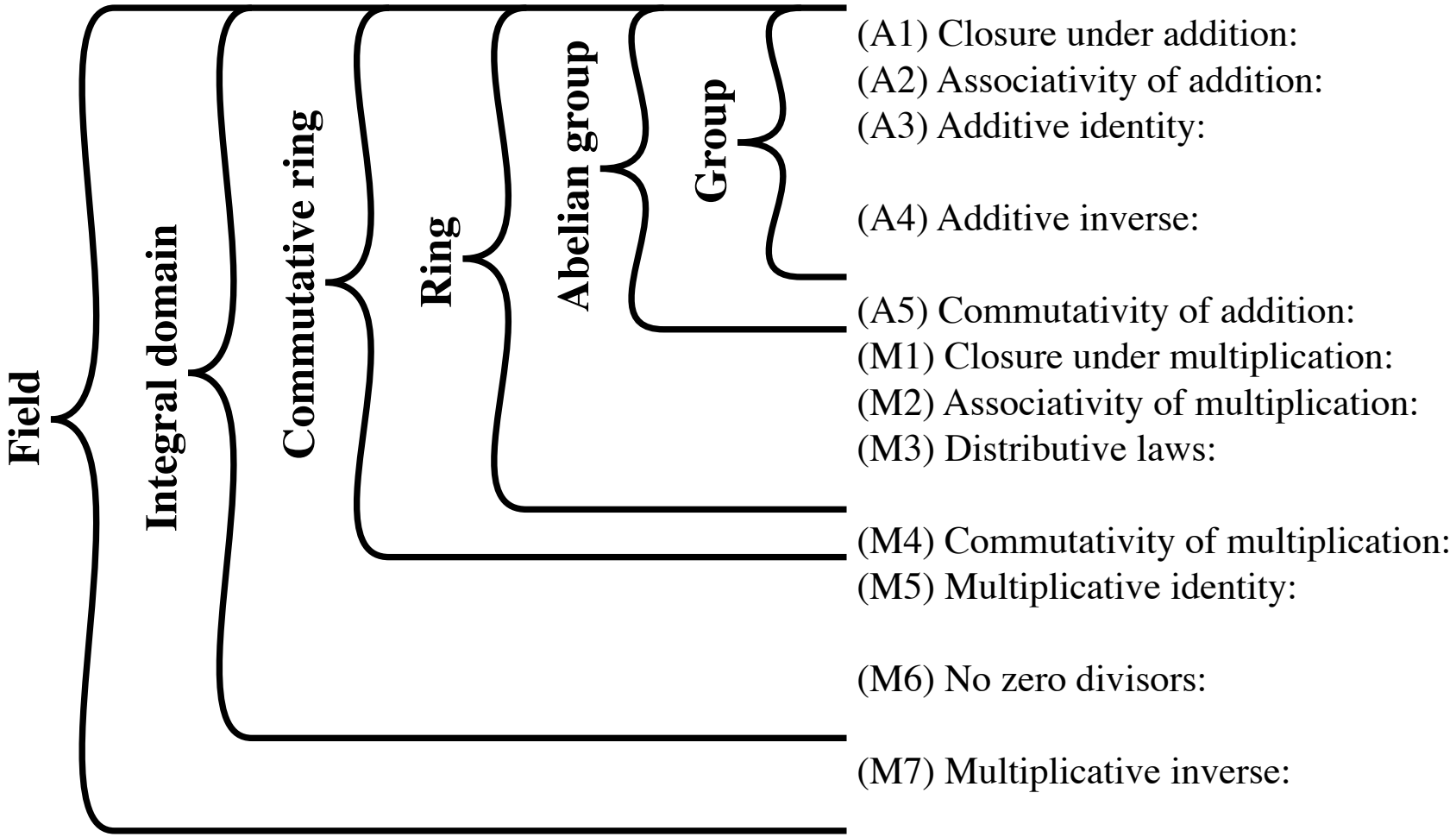
Groups, Rings, and Fields



(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 4.1, Stallings 2006

Groups, Rings, and Fields (cont.)



Source: Figure 4.1, Stallings 2006

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 4.1, Stallings 2006

Modular Arithmetic

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

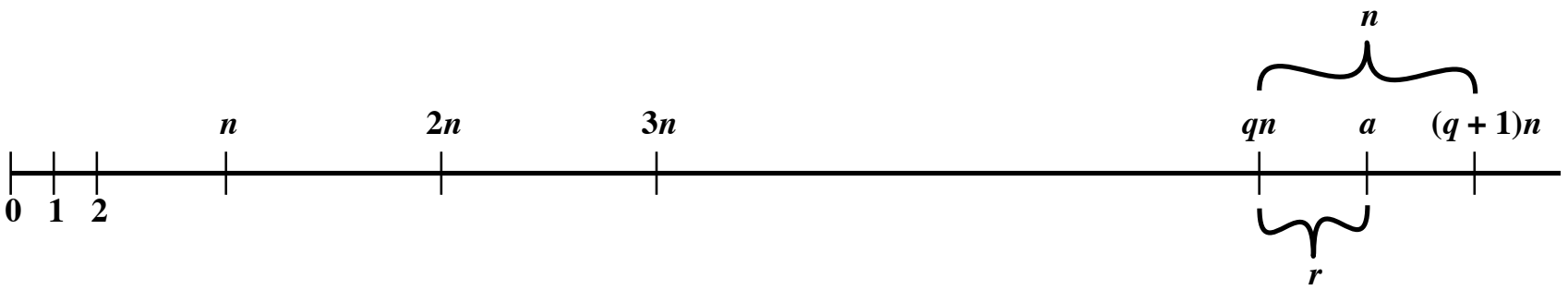
$$a = qn + r \quad 0 \leq r < n, q = \lfloor a/n \rfloor.$$

The remainder r is also referred to as the *residue* and is usually denoted by "$a \bmod n$".

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

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

Quotient and Remainder



Source: Figure 4.2, Stallings 2006

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.
- We say a nonzero integer b divides another integer a, denoted as $b|a$, if $a = mb$ for some integer m.
- 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

$$((a \bmod n) + (b \bmod n)) \bmod n = (a + b) \bmod n$$
$$((a \bmod n) - (b \bmod n)) \bmod n = (a - b) \bmod n$$
$$((a \bmod n) \times (b \bmod n)) \bmod n = (a \times b) \bmod n$$

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

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

(a) Addition modulo 8

Source: Table 4.1, Stallings 2006

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

(b) Multiplication modulo 8

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

(c) Additive and multiplicative inverses modulo 8

Source: Table 4.1, Stallings 2006

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 4.2, Stallings 2006

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.

Finding the Multiplicative Inverse

$EXTENDED\ EUCLID(M, B)$:

1. $(A_1, A_2, A_3) \leftarrow (1, 0, m); (B_1, B_2, B_3) \leftarrow (0, 1, b)$
2. if $B_3 = 0$ then return $A_3 = \gcd(m, b)$; no inverse
3. if $B_3 = 1$ then return $B_3 = \gcd(m, b); B_2 = b^{-1} \pmod{m}$
4. $Q = \lfloor A_3/B_3 \rfloor$
5. $(T_1, T_2, T_3) \leftarrow (A_1 - QB_1, A_2 - QB_2, A_3 - QB_3)$
6. $(A_1, A_2, A_3) \leftarrow (B_1, B_2, B_3)$
7. $(B_1, B_2, B_3) \leftarrow (T_1, T_2, T_3)$
8. goto 2

Invariants: $mA_1 + bA_2 = A_3$ and $mB_1 + bB_2 = B_3$.

If $\gcd(m, b) = 1$, then B_2 equals the multiplicative inverse of b modulo m when the algorithm terminates.

$mB_1 + bB_2 = B_3 = 1 \rightarrow bB_2 = 1 - mB_1 \rightarrow bB_2 \equiv 1 \bmod m$.

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

(a) Addition modulo 7

Source: Table 4.3, Stallings 2006

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

(b) Multiplication modulo 7

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

(c) Additive and multiplicative inverses modulo 7

Source: Table 4.3, Stallings 2006

Polynomial Arithmetic

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Source: Figure 4.3, Stallings 2006

Polynomial Arithmetic over $GF(2)$

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\cline{2-2}
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\
\cline{2-2}
\end{array}
$$

(d) Division

Source: Figure 4.4, Stallings 2006

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

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

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; it 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.

For the AES algorithm, the irreducible polynomial modulus is

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

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

(a) Addition

Source: Table 4.5, Stallings 2006

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

(b) Multiplication

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

Source: Table 4.5, Stallings 2006

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

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

1. $[A_1(x), A_2(x), A_3(x)] \leftarrow [1, 0, m(x)]; [B_1(x), B_2(x), B_3(x)] \leftarrow [0, 1, b(x)]$
2. if $B_3(x) = 0$ then return $A_3(x) = \gcd(m(x), b(x))$; no inverse
3. if $B_3(x) = 1$ then return $A_3(x) = \gcd(m(x), b(x)); B_2(x) = b^{-1}(x) \pmod{m(x)}$
4. $Q(x) =$ the quotient of $A_3(x)/B_3(x)$
5. $[T_1(x), T_2(x), T_3(x)]$
   $\leftarrow [A_1(x) - Q(x)B_1(x), A_2(x) - Q(x)B_2(x), A_3(x) - Q(x)B_3(x)]$
6. $[A_1(x), A_2(x), A_3(x)] \leftarrow [B_1(x), B_2(x), B_3(x)]$
7. $[B_1(x), B_2(x), B_3(x)] \leftarrow [T_1(x), T_2(x), T_3(x)]$
8. goto 2

Invariants: $m(x)A_1(x) + b(x)A_2(x) = A_3(x)$ and $m(x)B_1(x) + b(x)B_2(x) = B_3(x)$.

If $\gcd(m(x), b(x)) = 1$, then $B_2(x)$ equals the multiplicative inverse of $b(x)$ modulo $m(x)$ when the algorithm terminates.

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

	+	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
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 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 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

Source: Table 4.6, Stallings 2006

A Run of Extended Euclid

Initialization	$A1(x) = 1; A2(x) = 0; A3(x) = x^8 + x^4 + x^3 + x + 1$ $B1(x) = 0; B2(x) = 1; B3(x) = x^7 + x + 1$
Iteration 1	$Q(x) = x$ $A1(x) = 0; A2(x) = 1; A3(x) = x^7 + x + 1$ $B1(x) = 1; B2(x) = x; B3(x) = x^4 + x^3 + x^2 + 1$
Iteration 2	$Q(x) = x^3 + x^2 + 1$ $A1(x) = 1; A2(x) = x; A3(x) = x^4 + x^3 + x^2 + 1$ $B1(x) = x^3 + x^2 + 1; B2(x) = x^4 + x^3 + x + 1; B3(x) = x$
Iteration 3	$Q(x) = x^3 + x^2 + x$ $A1(x) = x^3 + x^2 + 1; A2(x) = x^4 + x^3 + x + 1; A3(x) = x$ $B1(x) = x^6 + x^2 + x + 1; B2(x) = x^7; B3(x) = 1$
Iteration 4	$B3(x) = \gcd[(x^7 + x + 1), (x^8 + x^4 + x^3 + x + 1)] = 1$ $B2(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

Source: Table 4.7, Stallings 2006

Bytes and Polynomials in GF(2^8)

In the AES algorithm, the basic unit for processing is a byte.

A byte $b_7b_6b_5b_4b_3b_2b_1b_0$ 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)

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 GF(2^8)

For the AES algorithm, the irreducible polynomial modulus is

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

Multiplication by x, assuming $b_7 = 1$:

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

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

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 4.8, Stallings 2006

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 0	001 1	010 g	100 g^2	011 g^3	110 g^4	111 g^5	101 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 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

(b) Multiplication

Source: Table 4.9, Stallings 2006