ECT-434
SECURE COMMUNICATION

Module 2: Finite Fields

1. Groups,Rings and Fields
2. Modular arithmetic
3. Euclidean algorithm
4. Finite Fields of the form GF(p)
5. Polynomial arithmetic

Bushara A R
AP, ECE
KMEA ENGG.COLLEGE

1. Groups,Rings and Fields

- Groups, rings, and fields are the fundamental elements of a branch of mathematics known as **abstract algebra, or modern algebra.**

<u>Groups</u>

A group G, sometimes denoted by {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 • b) in G, such that the following axioms are obeyed:

(A1) Closure: If a and b belong to G, then **a · b** is also 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 = e.

A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: a · b = b · a for all a, b in G.

Rings

A ring R, sometimes denoted by **{R, +, x}**, 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.

(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.

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.

A ring is said to be **integral domain**, which 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.

Fields

A field F, sometimes denoted by {F, +, x}, 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:

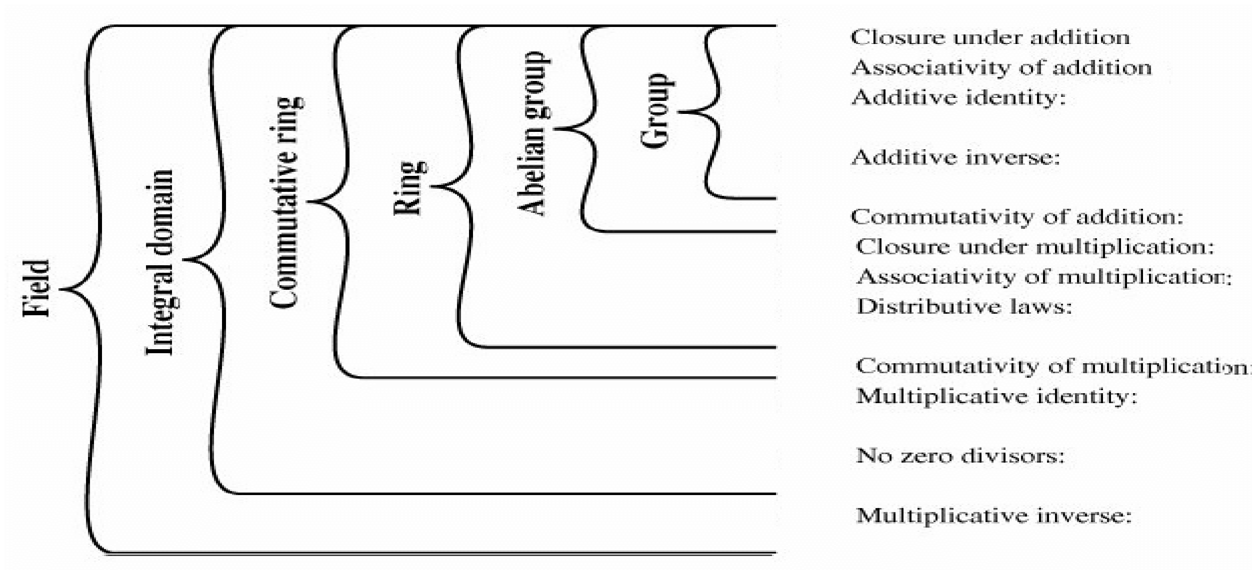
(A1-M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

Examples of Field:

- Rational Numbers
- Real Numbers
- Complex Numbers

Set of Integers not a field…



2. Modular arithmetic

–Given any positive integer *n* and any integer *m*, if we divide *m* by *n*, we get an integer quotient, *q*, and integer remainder, *r*, that obey the following relationship: m=5,n=3 r=2 q=1 5mod3=2

$$m = qn + r \qquad (0 \le r < n;\ q = \lfloor m / n \rfloor)$$

–The remainder, *r*, is often referred to as a ***residue*** of modulo *n*, and is the smallest non-negative integer that differs from *m* by a multiple of *n*.

For example,

$$m = 11; \quad n = 7; \quad 11 = 1 \times 7 + 4 \quad r = 4$$

$$m = -11; \quad n = 7; \quad -11 = (-2) \times 7 + 3 \quad r = 3$$

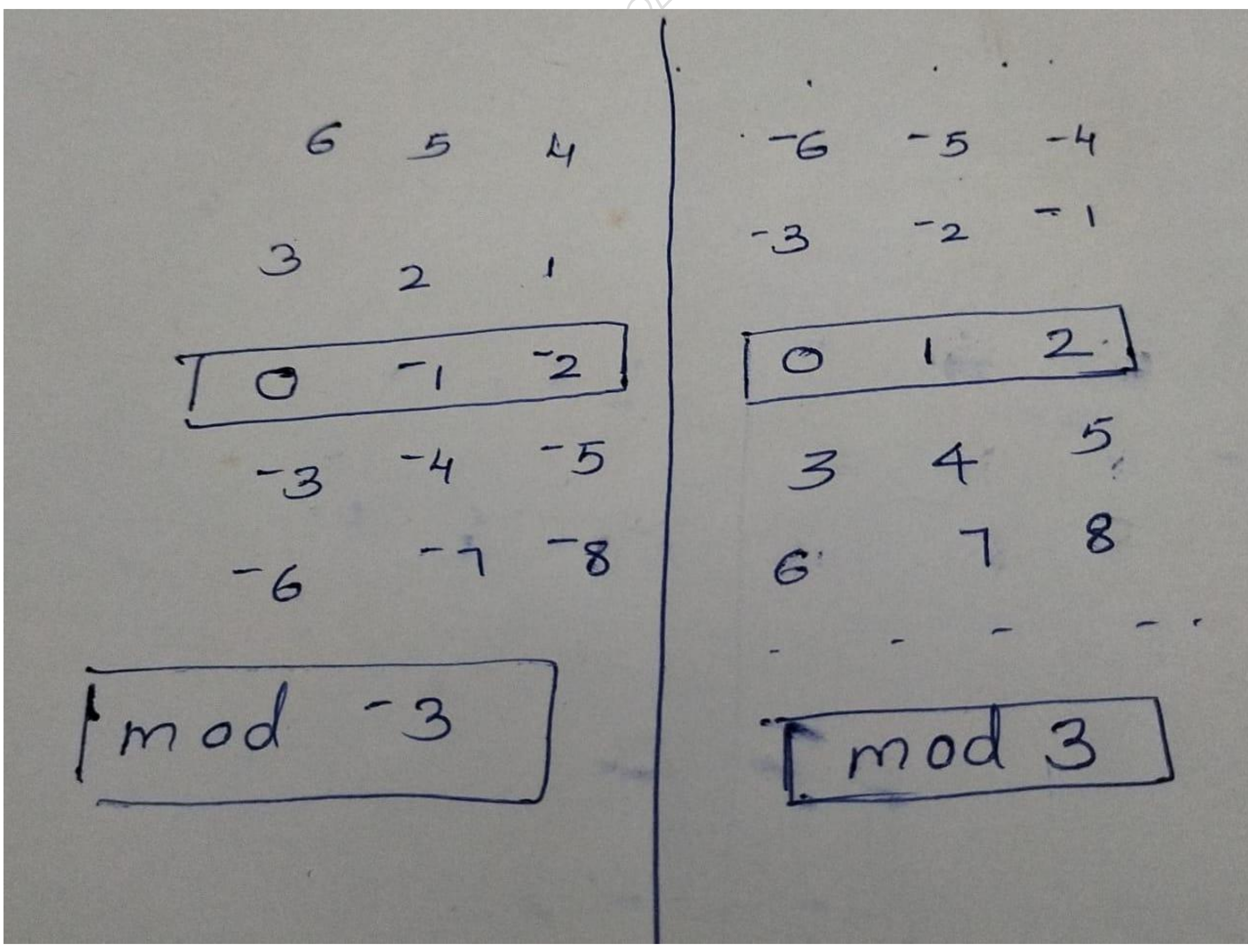
0,1.....6

5 mod 3

-5 mod 3

5 mod -3

-5 mod -3



•Two integers, *a* and *b* are said to be ***congruent*** (denoted by) if:

amod m=b

that is, "***a* is congruent to *b* modulo *m***"

•Alternatively, **in arithmetic modulo *m***, *a* and *b* are ***equivalent*** if their difference, (*a* - *b*), is a multiple of *m*; that is, *m* | (*a* - *b*)

$$a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$$

•The set of integers $\boldsymbol{Z_m}$ = {0,1, … *m* - 1} form **the complete set of residues modulo *m*** -- there are only *m* different integers, mod *m*

•The operation *a* mod *m* denotes the residue of *a*, such that the residue is some integer from 0 to *m* - 1. This operation is known as a ***modular reduction***.

Example: $10 \equiv 2 \pmod{4}$ because $4 \mid (10 - 2)$

10 mod 4 = 2

•**Properties of modular arithmetic is:**

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$(a-b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$$

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

$$(a \cdot (b+c)) \bmod m = (((a \cdot b) \bmod m) + ((a \cdot c) \bmod m)) \bmod m$$

11 mod 8 = 3; 15 mod 8 = 7
[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2 (11 + 15) mod 8 = 26 mod 8 = 2
[(11 ***mod*** 8) (15 ***mod*** 8)] ***mod*** 8 = 4 ***mod*** 8 = 4 (11 15) ***mod*** 8 = 4 ***mod*** 8 = 4
[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8 = 165 mod 8 = 5

5 mod 6 = 5

+	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

×	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

- Recall that ***exponentiation*** is defined:

$$a^0 = e, \quad \text{the identity element}$$

$$a^n = a \bullet a \bullet \cdots \bullet a \quad (\text{i.e.} \bullet \text{ applied } n\text{-1 times})$$

$$a^{-n} = (a')^n, \ \text{where } a' \text{ is the inverse of } a$$

Exponentiation is performed by repeated multiplication, as in ordinary arithmetic.

11 mod 13 =11

To find 11^7 mod 13, we can proceed as follows:
$11^2 = 121 \equiv 4 \pmod{13}$
$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$
$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

3.Euclidean algorithm

❖ One of the basic techniques of number theory is the **Euclidean algorithm**, which is a simple procedure for determining the **greatest common divisor** of two positive integers.

Greatest Common Divisor

gcd(a, b) - greatest common divisor of a and b.

The positive integer c is said to be the **greatest common divisor** of a and b if

1. c is a divisor of a and of b;
2. any divisor of a and b is a divisor of c.

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b).$$

In general, $\mathbf{\gcd(a, b) = \gcd(|a|, |b|)}$.

gcd(60, 24) = gcd(-60, 24) = 12

Finding the Greatest Common Divisor

- The Euclidean algorithm is based on the following theorem:
- For any nonnegative integer a and any positive integer b,

gcd(a,b) = gcd(b, a mod b)

gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11

gcd(18, 12) = gcd(12, 6) = gcd(6, 0) = 6

gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1

EUCLID(a, b)

1. A ← a; B ← b
2. if B = 0 return A = gcd(a, b)
3. R = A mod B
4. A ← B
5. B ← R
6. goto 2

To find gcd(1970, 1066)

A	B	R
1970	1066	904
1066	904	162
904	162	94
162	94	68
94	68	26
68	26	16
26	16	10
16	10	6
10	6	4
6	4	2
4	2	0

HOME WORK

a. Determine gcd(24140, 16762).

b. Determine gcd(4655, 12075).

4. Finite Fields of the form GF(p)

Finite Fields of Order p

For a given **prime, p,** the finite field of order p, GF(p) is defined as the set Zp of integers {0, 1,..., p 1}, together with the arithmetic operations **modulo p.**

Finding the Multiplicative Inverse in GF(p)

Table 4.5 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

×	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

- For large values of p, this approach is not practical.

22

Finding the Multiplicative Inverse in GF(p)

EXTENDED EUCLID(m, b)

1. (A1, A2, A3) ← (1, 0, m);
   (B1, B2, B3) ← (0, 1, b)
2. if B3 = 0 return A3 = gcd(m, b); **no inverse**
3. if B3 = 1 return B3 = gcd(m, b);
   B2 ← M.I of b mod m
4. Q = A3 / B3
5. (T1, T2, T3) = (A1 - QB1, A2 - QB2, A3 - QB3)
6. (A1, A2, A3) ← (B1, B2, B3)
7. (B1, B2, B3) ← (T1, T2, T3)
8. goto 2

1. Find the Multiplicative Inverse of 550 mod 1759

Calculating Multiplicative Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	$\boxed{355}$	$\boxed{1}$

The multiplicative inverse of 550 is 355, because 550 x 355 ≡ 1 mod 1795

Step 1:

T1 = 1-3*0 = 1

T2 = 0-3*1 = -3

T3 = 1759 - 3*550 = 109

Step 2:

T1 = 0-5*1 = -5

T2 = 1-5*-3 = 16

T3 = 550 - 5*109 = 5

Step 3:

T1 = 1-21*-5 = 106

T2 = -3-21*16 = -339

Calculating Multiplicative Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	$\boxed{355}$	$\boxed{1}$

T3 = 109 - 21*5 = 4

Step 4:

T1 = -5-1*106 = -111

T2 = 16-1*-339 = 355

T3 = 5- 1*4 = 1

The Multiplicative Inverse of 550 mod 1759 is 355

HomeWork

Using the extended Euclidean algorithm, find the multiplicative inverse of

a. 1234 mod 4321
b. 24140 mod 40902
c. 550 mod 1769

6. Polynomial arithmetic

Ordinary Polynomial Arithmetic

A **polynomial** of degree ***n*** (integer $n \geq 0$) is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

where the a_i are elements of some designated set of numbers ***S***, called the **coefficient set**, and $a_n \neq 0$. We say that such polynomials are defined over the coefficient set ***S***.

Addition and subtraction are performed by adding or subtracting corresponding coefficients.

$$f(x) = \sum_{i=0}^{n} a_i x^i; \quad g(x) = \sum_{i=0}^{m} b_i x^i; \quad n \geq m$$

then addition is defined as

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$$

and multiplication is defined as

$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i$$

where

$\boldsymbol{c_k = a_0 b_{k1} + a_1 b_{k1} + \ldots + a_{k1} b_1 + a_k b_0}$

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg
  - let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

    $f(x) + g(x) = x^3 + 2x^2 - x + 3$

    $f(x) - g(x) = x^3 + x + 1$

    $f(x) \text{ x } g(x) = x^5 + 3x^2 - 2x + 2$

$$\begin{array}{rrrrr}
x^3 & +\,x^2 & & & +\,2 \\
+ & (x^2 & -\,x & & +\,1) \\
\hline
x^3 & +\,2x^2 & -\,x & & +\,3
\end{array}$$

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Polynomial Arithmetic with Modulo Coefficients

- when computing value of each coefficient do calculation modulo some value
- could be modulo any prime
- but we are most interested in mod 2
  - ie all coefficients are 0 or 1

- mod 2:
- 1 + 1 = 1-1 = 0;
- 1 + 0 = 1 - 0 = 1;
- 0 + 1 = 0 - 1 = 1.

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Polynomial GCD

- gcd[a(x), b(x)] is the polynomial of maximum degree that divides both a(x) and b(x).
- gcd[a(x), b(x)] = gcd[b(x), a(x)mod(b(x))]
- Euclid[$a(x)$, $b(x)$]

1. $A(x) \leftarrow a(x)$; $B(x) \leftarrow b(x)$
2. **if** $B(x) = 0$ **return** $A(x) = \gcd[a(x), b(x)]$
3. $R(x) = A(x) \bmod B(x)$
4. $A(x) \leftarrow B(x)$
5. $B(x) \leftarrow R(x)$
6. **goto** 2

Find gcd[$\boldsymbol{a}(\boldsymbol{x})$, $\boldsymbol{b}(\boldsymbol{x})$] for $\boldsymbol{a}(\boldsymbol{x}) = \boldsymbol{x}^6 + \boldsymbol{x}^5 + \boldsymbol{x}^4 + \boldsymbol{x}^3 + \boldsymbol{x}^2 + \boldsymbol{x} + 1$ and $\boldsymbol{b}(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{x}^2 + \boldsymbol{x} + 1$.

A($\boldsymbol{x}$) = $\boldsymbol{a}(\boldsymbol{x})$; B($\boldsymbol{x}$) = $\boldsymbol{b}(\boldsymbol{x})$

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

R($\boldsymbol{x}$) = A($\boldsymbol{x}$) mod B($\boldsymbol{x}$) = $\boldsymbol{x}^3 + \boldsymbol{x}^2 + 1$

A($\boldsymbol{x}$) = $\boldsymbol{x}^4 + \boldsymbol{x}^2 + \boldsymbol{x} + 1$; B($\boldsymbol{x}$) = $\boldsymbol{x}^3 + \boldsymbol{x}^2 + 1$

$$
\begin{array}{r|ccccc}
 & x & + 1 & & & \\
\hline
x^3 + x^2 + 1 & x^4 & & + x^2 & + x & + 1 \\
 & \underline{x^4} & \underline{+ x^3} & & \underline{+ x} & \\
 & & x^3 & + x^2 & & + 1 \\
 & & \underline{x^3} & \underline{+ x^2} & & \underline{+ 1}
\end{array}
$$

R($\boldsymbol{x}$) = A($\boldsymbol{x}$) mod B($\boldsymbol{x}$) = 0

gcd[$\boldsymbol{a}(\boldsymbol{x})$, $\boldsymbol{b}(\boldsymbol{x})$] = A($\boldsymbol{x}$) = $\boldsymbol{x}^3 + \boldsymbol{x}^2 + 1$

Multiplicative Inverse of a Polynomial Arithmetic

```
EXTENDED EUCLID[m(x), b(x)]
1. [A1(x), A2(x), A3(x)] ⟵ [1, 0, m(x)]; [B1(x), B2(x),
   B3(x)] ⟵ [0, 1, b(x)]
2. if B3(x) = 0   return  A3(x) = gcd[m(x), b(x)]; no
   inverse
3. if B3(x) = 1   return  B3(x) = gcd[m(x), b(x)];
   B2(x) = b(x)1 mod m(x)
```

```
4. Q(x) = quotient of A3(x)/B3(x)
5. [T1(x), T2(x), T3(x)] ⟵ [A1(x) - Q(x)B1(x), A2(x) -
   Q(x)B2(x), A3(x) - QB3(x)]
6. [A1(x), A2(x), A3(x)] ⟵ [B1(x), B2(x), B3(x)]
7. [B1(x), B2(x), B3(x)] ⟵ [T1(x), T2(x), T3(x)]
8. goto 2
```

Table 4.7 shows the calculation of the multiplicative inverse of ($x^7 + x + 1$) mod ($x^8 + x^4 + x^3 + x + 1$). The result is that ($x^7 + x + 1)^1$ = (x^7). That is, ($x^7 + x + 1$)(x^7) $\equiv$ 1 (mod ($x^8 + x^4 + x^3 + x + 1$)).

Table 4.7. Extended Euclid [($x^8 + x^4 + x^3 + x + 1$), ($x^7 + x + 1$)]

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