Finite fields for the Advanced Encryption Standard (AES)

Killian O’Brien

6G6Z0024 Applied Cryptography 2025/26

Lecture Week 05 – Mon 27 October 2025

Introduction

- Cryptography relies heavily on mathematics
- The notion of **finite fields** and **modular polynomial arithmetic** are important in ciphers like AES and Eliptic Curves.
- These mathematical systems provide the security and operational requirements needed by the ciphers.

The familiar system $(\mathbb{R}, +, \cdot)$

- Consider the set of real numbers $\mathbb{R}$
- $\mathbb{R}$ can be thought of as consisting of every number on the *real number line*, a line extending from $-\infty$ to $+\infty$.
- Real numbers x can be written down as numbers with a (potentially infinite) decimal expansion.
- The real numbers, together with the usual operations of addition, $+$, and multiplication, $\cdot$, have the structure of what mathematicians call a **field**.
- That is, the system $(\mathbb{R}, +, \cdot)$ satisfies the following properties.
  - **(A1)** *Closure for addition:* If $a, b \in \mathbb{R}$ then $a + b \in \mathbb{R}$.
  - **(A2)** *Associativity for addition:* For all $a, b, c \in \mathbb{R}$ we have $(a + b) + c = a + (b + c)$.
  - **(A3)** *Additive identity element:* There is an element $0 \in \mathbb{R}$ such that for all $a \in \mathbb{R}$ we have $a + 0 = 0 + a = a$.
  - **(A4)** *Additive inverses:* For each $a \in \mathbb{R}$ there exists an element $b \in \mathbb{R}$ such that $a + b = b + a = 0$. This element b is of course the *negative of* a and usually written as $b = -a$.
  - **(A5)** *Commutativity of addition:* For all $a, b \in \mathbb{R}$ we have $a + b = b + a$.

- A system $(S, +)$ satisfying (A1) - (A4) is called a **group**, and if it also satisfies (A5) it is called an **abelian group**.

The familiar system $(\mathbb{R}, +, \cdot)$

- The system also satisfies
  - **(M1)** *Closure for multiplication:* If $a, b \in \mathbb{R}$ then $a \cdot b \in \mathbb{R}$.
  - **(M2)** *Associativity for multiplication:* For all $a, b, c \in \mathbb{R}$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
  - **(M3)** *Distributive laws:*
    - for all $a, b, c \in \mathbb{R}$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$.
    - for all $a, b, c \in \mathbb{R}$ we have $(b + c) \cdot a = b \cdot a + c \cdot a$.
  - **(M4)** *Commutativity of multiplication:* For all $a, b \in \mathbb{R}$ we have $a \cdot b = b \cdot a$.
  - **(M5)** *Multiplicative identity:* There is an element $1 \in \mathbb{R}$ such that for all $a \in \mathbb{R}$ we have $a \cdot 1 = 1 \cdot a = a$.
  - **(M6)** *No zero-divisors:* If $a, b \in \mathbb{R}$ and $a \cdot b = 0$ then $a = 0$ or $b = 0$.
- A system $(S, +, \cdot)$ satisfying (A1) - (A4) and (M1)-(M3) is called a **ring**, and if it also satisfies (M4) it is called an **abelian ring**.
- A system $(S, +, \cdot)$ satisfying (A1) - (A4) and (M1)-(M6) is called an **integral domain**.
- Finally,
  - **(M7)** *Multiplicative inverses:* If $a \in \mathbb{R}$ and $a \neq 0$ then there exists an element $b \in \mathbb{R}$ such that $a \cdot b = b \cdot a = 1$. This element b is of course the *reciprocal of* a and usually written as $b = a^{-1}$.
- A system $(F, +, \cdot)$ satisfying (A1) - (A4) and (M1)-(M7) is called a **field**.

Fields

- Essentially, a field $(F, +, \cdot)$ is a system within which we can perform addition, subtraction, multiplication and division, without leaving the set F, and the usual proeprties we are familiar with, from $\mathbb{R}$ say, hold true.
- Subtraction and division are defined in terms of addition and multiplication as
    - $a - b = a + (-b)$
    - $a/b = a \cdot b^{-1}$
- Fields provide a mathematical system in which we have a rich calculation environment following well understood rules.
- They, and other related agebraic structures, are of intense interest for their purely mathematical properties ….
- … and also find applications in other mathematical areas such as geometry, and more practical application areas such as cryptography and computer science.

Finite fields of the form $\mathrm{GF}(p)$

- $\mathrm{GF}(m)$ notation named for *Galois Field* after French mathematician Évariste Galois. It stands for a finite field containing m elements.
- In cryptography, two of the important finite fields are $\mathrm{GF}(2)$ and, more generally, $\mathrm{GF}(p)$, for a prime p.
- $\mathrm{GF}(2)$: This just consits of the binary elements 0 and 1, under the following rules.

The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

$+$	0	1
0	0	1
1	1	0

Addition

$\times$	0	1
0	0	0
1	0	1

Multiplication

w	$-w$	w^{-1}
0	0	–
1	1	1

Inverses

In this case, addition is equivalent to the exclusive-OR (XOR) operation, and multiplication is equivalent to the logical AND operation.

Finite fields of the form $\mathrm{GF}(p)$

- A finite field $\mathrm{GF}(p)$ can be formed by our familiar modular arithmetic modulo p, i.e. $\mathrm{GF}(p) = \mathbb{Z}_p$.
- Table to the right show the operation and inverse tables for $\mathbb{Z}_7$.
- Note that $\mathbb{Z}_m$, where m is not a prime, will not be a field due to the lack of multiplicative inverses for all elements.
- For example, consider the operation and inverse tables of $\mathbb{Z}_8$ shown on the right.
- Finding mutliplicative inverses in $\mathrm{GF}(p) = \mathbb{Z}_p$:
    - If p is a prime and $1 \leq a < p$ then necessarily $\gcd(a, p) = 1$.
    - Run the extended Euclidean algorithm to find integers x, y such that

$$ax + py = \gcd(a, p) = 1.$$

    - Then reducing this equation modulo p gives

$$ax \equiv 1 \pmod{p},$$

so $a^{-1} = (x \bmod p)$.

Table 5.1 Arithmetic Modulo 8 and Modulo 7

+	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

+	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

(d) Addition modulo 7

×	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

×	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

(e) Multiplication modulo 7

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

(c) Additive and multiplicative inverses modulo 8

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

(f) Additive and multiplicative inverses modulo 7

Polynomial arithmetic

- So for $\mathrm{GF}(p)$ we have a model $\mathbb{Z}_p$. But what about $\mathrm{GF}(m)$ for other useful values of m such as $m = 2^n$?
- For this we will need **polynomial arithmetic**.
- A **polynomial of degree** n is a function $f(x)$ of the form

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

- The coefficients a_i will be coming from some specified set such as the integers $\mathbb{Z}$, modular integers $\mathbb{Z}_m$ or some finite field.
- We will be interested in the polynomial object f itself, not so much in its particular values. So the x will remain mostly unspecified, or *indetermined*.
- **Polynomial arithmetic** includes the operations of addition and multiplication of polynomials. For example, with coefficients from the set S of integers

As an example, let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$, where S is the set of integers. Then

$$f(x) + g(x) = x^3 + 2x^2 - x + 3$$
$$f(x) - g(x) = x^3 + x + 1$$
$$f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$$

Figures 5.5a through 5.5c show the manual calculations. We comment on division subsequently.

- Can be shown that the system of polynomials $\sum_{i=0}^{n} a_i x^i$, with coefficients a_i coming from the field $\mathbb{Z}_p$, will form a commutative ring.
- The division process among such polynomials can still be carried out, but it will be a process of *division with remainder* like we have seen previously in the system $\mathbb{Z}$.

Polynomial division

- For a first example consider the system of polynomials with integer coefficients.
- Let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$, then we can say that

$$f(x) = (x + 2)g(x) + x,$$

  i.e. that dividing $f(x)$ by $g(x)$ gives a *quotient* of $(x + 2)$ and a *remainder* of x.
- We can write $(f(x) \mod g(x)) = x$.
- We require that the remainder polynomial has degree strictly less than the degree of the divisor polynomial, i.e. $g(x)$ in the equation above.
- Can carry out the calculation using some form of *long division*, see boards.
- Can multiply out the above equation to verify the result.

Polynomial arithmetic with coefficients in $\mathrm{GF}(2) = \mathbb{Z}_2$

- For cryptography purposes, polynomials with coefficients in $\mathrm{GF}(2) = \mathbb{Z}_2$ are of most interest.
- That is, these are polynomials with binary coefficients, i.e. 0 or 1, and these coefficients follow the rules of arithmetic in $\mathbb{Z}_2$,

$$0+0=0, 1+1=0, 1+0=1, 1-1=0, 0-1=1, \ldots$$

- This setup can make the resulting polynomial arithmetic tricky to follow.
- See the examples on the right for polyomial arithmetic operations two such polys $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ and $g(x) = x^3 + x + 1$.
- A polynomial $f(x)$ with coefficients from a field F is called **irreducible** if and only if $f(x)$ cannot be expressed as a product of two other such polynomials, both of degree greater than 0 and less than the degree of f.
- For example,
  - for polynomials over $\mathbb{Z}_2$, the poly $f(x) = x^4 + 1$ is reducible as

$$x^4 + 1 = (x+1)(x^3 + x^2 + x + 1).$$

  - but $g(x) = x^3 + x + 1$ is irreducible since neither x nor $x+1$, the only such polys of degree 2, is a factor of it.

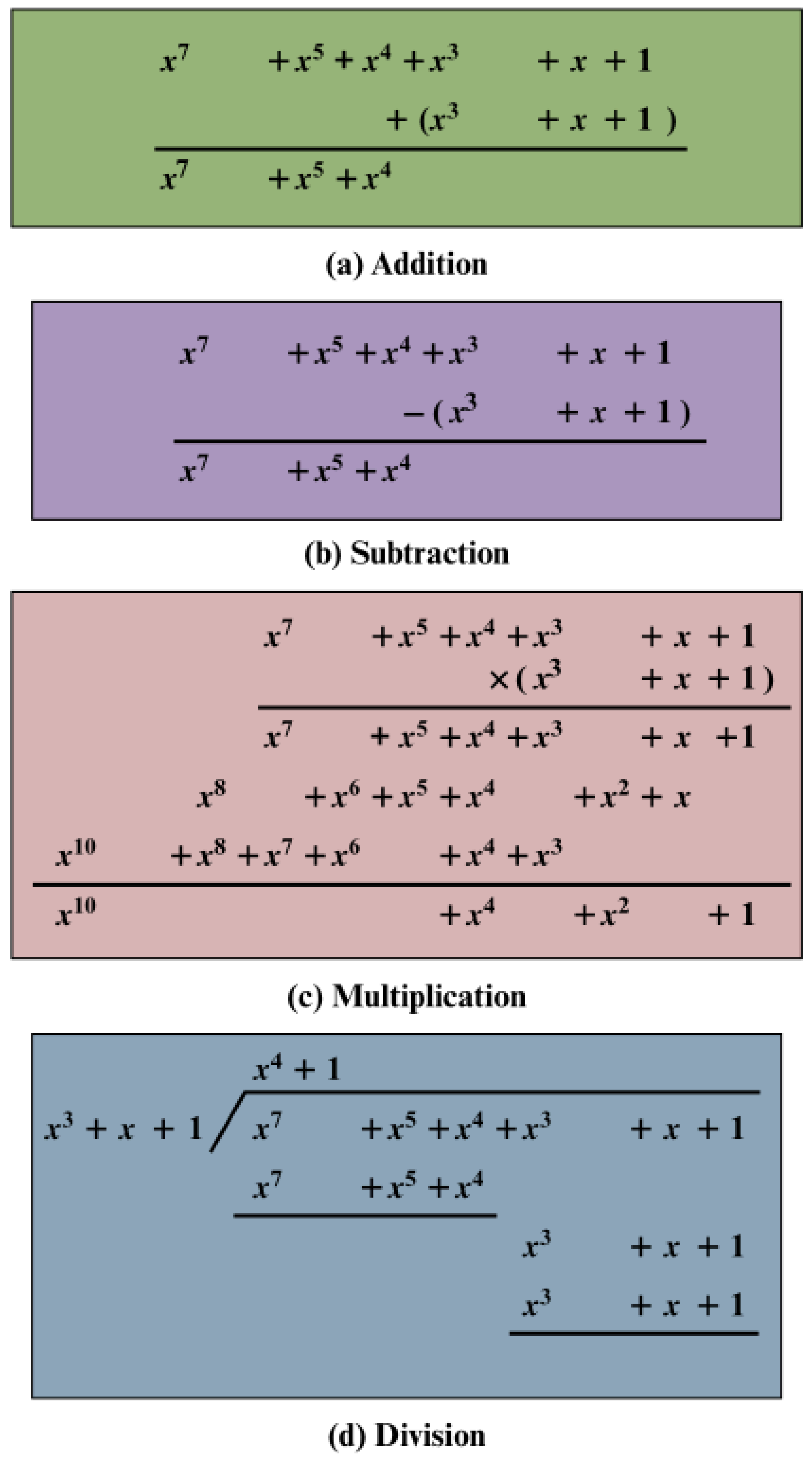

Figure 5.6 Examples of Polynomial Arithmetic over GF(2)

GCD and Euclidean algorithm for polynomials

- For polynomials with coefficients from some particular field F we can define $\gcd$ and the Euclidean algorithm, just like we did within the system $\mathbb{Z}$.
- For polynomials $a(x)$ and $b(x)$, their $\gcd$ is the polynomial $c(x)$ such that
    - $a(x)$ and $b(x)$ are both divisible by $c(x)$.
    - Any other common divisor of $a(x)$ and $b(x)$, also divides $c(x)$.
- Or equivalently, the $\gcd$ of $a(x)$ and $b(x)$ is the polynomial of maximum degree, that divides both $a(x)$ and $b(x)$.
- See specification on the right (from Stallings), which is essentially the previous specification for the Euclidean algorithm, but now taking place for polynomials.

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

GCD and Euclidean algorithm for polynomials

- On the right, from Stallings, is an example showing the EA run to find the $\gcd(a(x), b(x))$, where

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

and

$$b(x) = x^4 + x^2 + x + 1,$$

are polynomials with coefficients in $\mathbb{Z}_2$.

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 $b(x)$:

$$\begin{array}{r@{\,}l}
 & x^2 + x \\
x^4 + x^2 + x + 1 \,\big) & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & x^6 \qquad\;\; + x^4 + x^3 + x^2 \\ \hline
 & \quad x^5 \qquad\qquad\qquad\quad + x + 1 \\
 & \quad x^5 \qquad\; + x^3 + x^2 + x \\ \hline
 & \qquad\qquad x^3 + x^2 \qquad + 1
\end{array}$$

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

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

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

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

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

Finite fields of the form $\mathrm{GF}(2^n)$

- In computer science we commonly work with capacities (of memory size, size of comms channel, message block size, etc) of size 2^n, for some integer n. As these are all based on a certain number of binary bits.
- With n bits we can represent 2^n numbers: the integer 0, and the $2^n - 1$ integers $1, 2, 3, \ldots, 2^n - 1$.
- So we wish to have a finite field $\mathrm{GF}(2^n)$. Where does such a field come from?
- It can't be the integers under the usual arithmetic modulo 2^n, as this will lack multiplicative inverses for half the elements.
- See table on the right for an example showing $\mathrm{GF}(2^3)$ exists and then we'll describe the general construction.

Table 5.2 Arithmetic in $\mathrm{GF}(2^3)$

		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

		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

Modular polynomial arithmetic and $\mathrm{GF}(p^n)$

- The finite fields $\mathrm{GF}(p^n)$ for primes p and any positive integer exponent n do indeed exist, and can be constructed from **modular polynomial arithmetic** as follows.
- Define S to be the set of all polynomials of degree $n-1$, or less, and with coefficients coming from the field $\mathbb{Z}_p$, i.e. the coefficients follow the rules of integer arithmetic modulo p.
- So S consists of all polynomials $f(x)$ of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n-1} a_i x^i, \quad a_i \in \mathbb{Z}_p.$$

- In total, there are p^n such polynomials, since there is a choice of p elements for each of the n coefficients $a_0, \ldots, a_{n-1}$.
- The behaviour of $+$ and $\cdot$ on S will follow the usual rules of polynomial arithmetic and
  - arithmetic with the coefficients a_i is done under the rules of $\mathbb{Z}_p$, i.e. integer arithmetic modulo p,
  - if multiplication of polynomials results in a polynomial of degree n or greater then the result is reduced modulo some specified irreducible polynomial $m(x)$, of degree n. That is, we divide the result by $m(x)$ and keep the remainder polynomial $r(x)$, which must have degree less than n.
- The resulting system $(S, +, \cdot)$ will be a field of p^n elements. This shows that finite fields $\mathrm{GF}(p^n)$ do exist.

AES and $\mathrm{GF}(2^8)$.

- The Advanceed Encryption Standard (AES) uses such a field $\mathrm{GF}(2^8)$, consisting of polynomials of degree less than or equal to 7, with binary coefficients and polynomial operations carried out modulo the irreducible polynomial

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

- The figure on the right shows the calculation of an example product in $\mathrm{GF}(2^8)$.
- The properties of $\mathrm{GF}(2^8)$, specifically the taking of multiplicative inverses, is a crucial step in a **S-box** substitution operation carried out on the bytes of a block in the AES cipher.

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

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

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

$$\begin{array}{r|l} & x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \cline{2-2} & x^{11} + x^4 + x^3 \\ & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \cline{2-2} & x^7 + x^6 + 1 \end{array}$$

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

$\mathrm{GF}(2^3)$ again.

- The tables below show addition and multiplication in $\mathrm{GF}(8)$
- The Extended Euclidean algorithm can be used to obtain multiplicative inverses just as before. See Stallings for examples.
- The polynomial operations do have efficient implementations in terms of bit sequence operations which means that computations in $\mathrm{GF}(8)$ (and by generalization other $\mathrm{GF}(2^n)$) can be carried out very fast. See Stallings for details.

Table 5.3 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

(a) Addition

		000	001	010	011	100	101	110	111
	$\times$	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+1	x^2	$x+1$

(b) Multiplication