Finite Fields

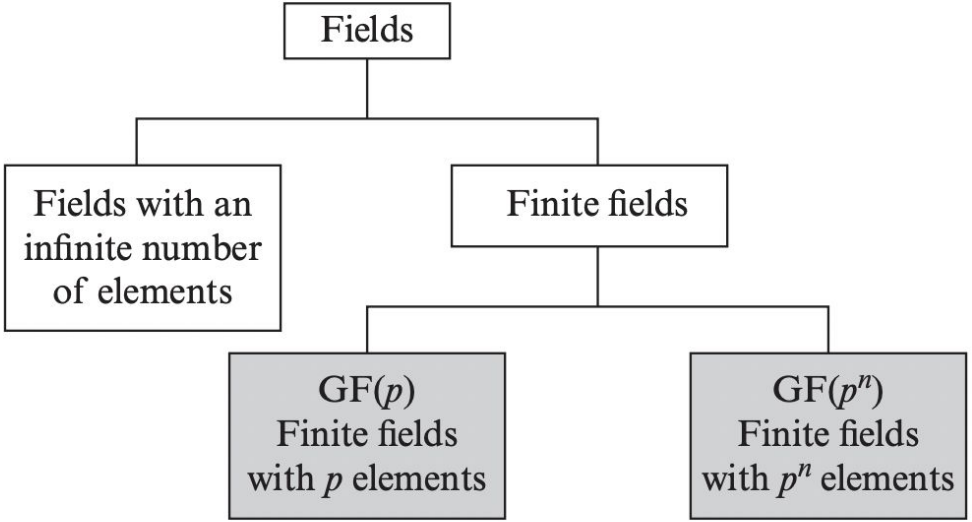

Figure 5.3 Types of Fields

Multiplicative inverse (w^{-1})	For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod p$

Finite Fields of Order p - GF(2) $\{0, 1\}$

1. $a+b \bmod p$
2. $a^*b \bmod p$
3. $a+a^{-1} \bmod p = 0$
4. $a^*a^{-1} \bmod p = 1$

$(a+a^{-1}) \bmod 2 = 0$

$(a * a^{-1}) \bmod 2 = 1$

a	b	+
0	0	0
0	1	1
1	0	1
1	1	0

a	b	+
0	0	0
0	1	0
1	0	0
1	1	1

a	Add inv	Mul inv
0	0	—
1	1	1


THANK YOU!


LIKE
COMMENT
SHARE
SUBSCRIBE

Addition Modulo 7

$GF(7) = \{0,1,2,3,4,5,6\}$

$(a+b) \bmod 7$

$0 \to 0$
$1 \to 6$

$(a + a^{-1}) \bmod 7$
$= 0$

$a \downarrow$ / $b \to$	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

Multiplication Modulo 7

$(a \times b) \bmod 7$

$0 \to$ undefined
$1 \to 1$
$2 \to 4$

	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	$\boxed{1}$	3	5
3							
4							
5							
6							

+	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
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

additive →

mul →

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

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	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	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

1. GF(p) consists of p elements.
2. The binary operations $+$ and $\times$ are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse, and division is performed by multiplication by the multiplicative inverse.

Finding Multiplicative Inverse for large values

a =1759 b= 550 Find b^{-1}

a, b $\Rightarrow$ co-prime

$\Rightarrow$ $bb^{-1} \bmod a = 1$

Extended-euclid

$b^{-1} = 355$

$(550 \times 355) \bmod 1759 = 1$


LIKE
COMMENT
SHARE
SUBSCRIBE


THANK YOU!

Polynomial Arithmetic

1. Addition
2. Subtraction
3. Multiplication
4. Division
5. GCD

Addition

$$f(x) = x^3 + x^2 + 2 \text{ and } g(x) = x^2 - x + 1$$

$$\Rightarrow x^3 + x^2 + 2 + x^2 - x + 1$$

$$\Rightarrow x^3 + 2x^2 - x + 3 \,//$$

Subtraction

$$f(x) = x^3 + x^2 + 2 \text{ and } g(x) = x^2 - x + 1$$

$$f(x) - g(x) = \begin{array}{r} x^3 + x^2 \quad\quad + 2 \\ -\quad x^2 - x + 1 \\ \hline \end{array}$$

$$\Rightarrow x^3 + x + 1$$

Multiplication

$$f(x) = x^3 + x^2 + 2 \text{ and } g(x) = x^2 - x + 1$$

x^4 $\quad -x^3$ $\quad x^2$

x^5 $\quad -x^4$ $\quad x^3$

$2(x^2 - x + 1)$

$= \underbrace{2x^2 - 2x + 2}$

$$x^5 - \cancel{x^4} + \cancel{x^3} + \cancel{x^4} - \cancel{x^3} + x^2 + 2x^2 - 2x + 2$$

$$x^5 + 3x^2 - 2x + 2 \;//$$

Division

$f(x)/g(x)$

$f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

$x+2 \longrightarrow$ quotient

$\underbrace{x^2 - x + 1}_{\text{divisor}}$

$x^3 + x^2 + 2$

$(-)\ x^3 - x^2 + x$

$0 + 2x^2 - x + 2$

$(-)\ 2x^2 - 2x + 2$

$0 + x$

$\hookrightarrow$ remainder

GCD - Step 1

low power → divisor

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 $b(x)$:

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

new term inside

Rem ⇒

remainder

divisor new

Step 2

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

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

$$
\begin{array}{rl}
 & x + 1 \\ \cline{2-2}
\text{divisor} \Rightarrow \; x^3 + x^2 + 1 \big) & x^4 + x^2 + x + 1 \\
 & x^4 + x^3 + x \\ \cline{2-2}
 & x^3 + x^2 + 1 \\
 & x^3 + x^2 + 1 \\ \cline{2-2}
 & 0 \rightarrow \underline{\text{stop}}
\end{array}
$$

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

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

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

LIKE

COMMENT

SHARE

SUBSCRIBE