Galois Field

Finite (Galois) Fields: GF(p)

Order of Finite Field must be a power of prime number $GF(p^n)$

When $n = 1$ we get $GF(p)$ The structure is different then that of $GF(p^n)$

Else $n > 1$ $GF(p^n)$

- $GF(p) :=$ set of Z_p integers $\{0,1,2 \ \dots \ p-1\}$
- Eg: $GF(2) :=$ $\boxed{F = < Z_p, +, * >}$ $:= GF(2^1)$

+	0	1
0	0	1
1	1	0

XOR

*	0	1
0	0	0
1	0	1

AND

a	$-a$	a^{-1}
0	0	-
1	1	1

Inverse

The identity of additive inverse does not have multiplicative inverse

- Galois Field $GF(p)$
- Modular Polynomial Arithmetic
- Galois Field $GF(2^n)$

Finite (Galois) Fields: GF(p)

- Eg: $GF(7) \coloneqq Z_7$

+	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

*	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

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

Modulo 8 domain Z_8

Integer	1	2	3	4	5	6	7
Frequency	4	8	4	12	4	8	4

Frequency of elements is evenly distributed in Addition

+	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

Frequency of elements is not evenly distributed in Multiplication

*	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

Multiplicative Inverse of elements does not exi

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

Justification for Galois Field

Better Solution
$GF(2^n)$

- We need to perform +,-,* and ÷. So we need something that qualifies for a field.
- Z_p qualifies to be a field.
- Problems:
  - But if we have 3 bits representation then the we are dealing with Z_8 domain.
  - For 8 bits representation we have Z_{256}
  - All of theses are even integer domains and none of them, except Z_2, are in Z_p
  - Z_{256}, Z_8 etc are Commutative Rings
- Solution: Not Good
  - We can opt for largest prime number in the given $Z_n$domain.
  - 3 bits can have Z_7 and 8 bits can have Z_{251}. But this leads to inefficiency.

GF(2^3) $GF(2^n) \equiv GF(p^n)$

Integer	1	2	3	4	5	6	7
Frequency	7	7	7	7	7	7	7

Frequency of elements is evenly distributed in Addition

	+	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6 (110)	7 (111)
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

Frequency of elements is not evenly distributed in Multiplication

	*	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6 (110)	7 (111)
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

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

Modular Polynomial Arithmetic

1	0	0	1	0	1	0	1
x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0

$$x^7 + x^4 + x^2 + x^0$$

$$\boxed{x^7 + x^4 + x^2 + 1}$$

0	1	1	0	1	0	1	0
x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0

$$x^6 + x^5 + x^3 + x^1$$

$$\boxed{x^6 + x^5 + x^3 + x}$$

000	$\mathbf{0}$
001	$\mathbf{1}$
010	$\boldsymbol{x}$
011	$\boldsymbol{x+1}$
100	$\boldsymbol{x^2}$
101	$\boldsymbol{x^2+1}$
110	$\boldsymbol{x^2+x}$
111	$\boldsymbol{x^2+x+1}$

Example of $\boldsymbol{GF(2^3)}$

For $\boldsymbol{GF(2^n)}$ order of polynomial will never exceed $\boldsymbol{n-1}$

If, after some operation, the order exceeds $\boldsymbol{n-1}$ then perform $\boldsymbol{mod}$ order $\boldsymbol{n}$ **Irreducible Polynomial**

Irreducible Polynomial of order $\mathbf{3}$ is $\boldsymbol{x^3 + x + 1}$

Operation on Mod Poly. Arth.

Example in $GF(2^3)$

$f(x) = x^2 + x + 1 \qquad g(x) = x^2 + 1 \qquad m(x) = x^3 + x + 1$

Operation on Mod Poly. Arth.

Example in $GF(2^3)$

$f(x) = x^2 + x + 1 \qquad g(x) = x^2 + 1 \qquad m(x) = x^3 + x + 1$

Addition:
$$
\begin{aligned}
&= f(x) + g(x) \\
&= (x^2 + x + 1) + (x^2 + 1) \\
&= (\color{red}{x^2} + x + \color{red}{1}) + (\color{red}{x^2} + \color{red}{1}) \\
&= x
\end{aligned}
$$

Multiplication:
$$
\begin{aligned}
&= f(x) * g(x) \\
&= (x^2 + x + 1) * (x^2 + 1) \\
&= (x^4 + x^3 + x^2) + (x^2 + x + 1) \\
&= (x^4 + x^3 + \color{red}{x^2}) + (\color{red}{x^2} + x + 1) \\
&= x^4 + x^3 + x + 1
\end{aligned}
$$

$$
\begin{aligned}
&= f(x) * g(x) \bmod m(x) \\
&= (x^4 + x^3 + x + 1) \bmod (x^3 + x + 1) \\
&= x^2 + x
\end{aligned}
$$

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

Relevant Information

Example in $GF(2^8)$

$f(x) = x^6 + x^4 + x^2 + x + 1 \qquad g(x) = x^7 + x + 1 \qquad m(x) = x^8 + x^4 + x^3 + x + 1$

Addition:

$f(x) + g(x)$

$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) \quad = (x^7 + x^6 + x^4 + x^2)$ **Polynomial Notation**

$(01010111) \oplus (10000011) \quad = (11010100)$ **Binary Notation**

$\{57\} \oplus \{83\} \quad = \{D4\}$ **HexaDecimal Notation**

Inverse of $\{95\}$ in $GF(2^8)$ $\quad \{95\} = (10010101) = x^7 + x^4 + x^2 + 1$

q	r1	r2	r	t1	t2	t
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	0	1	x
$x^2 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	x	1	x	$x^3 + x^2 + x + 1$
$x^4 + x^3$	$x^5 + x^4 + 1$	x	1	x	$x^3 + x^2 + x + 1$	$x^7 + x^3 + x$
x	x	1	0	$x^3 + x^2 + x + 1$	$x^7 + x^3 + x$	
	1	0		$x^7 + x^3 + x$		