Finite Field

1). A finite field is a field with a finite number of elements.

2). The number of elements in the set is called the order of the field.

3). A field with order m exists if m is a prime power, i.e. $[m = p^n$ for some integer n and with p a prime integer.

4) $GF(P)$ = The elements of the finite fields can be represented by $0, 1, \ldots, p-1$. $GF(2) = \{0, 1\}$.

5). Elements are represented as polynomials over $GF(P)$.

Polynomials over a field :-

A polynomial over a field F is an expression of the form:

$$b(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_0.$$

Operations on Polynomials

i) Addition.

$$c(x) = a(x) + b(x) \Leftrightarrow c_i = a_i + b_i \; ; 0 \leq i \leq n.$$

[0 is the identity element. the inverse of an element can be found by replacing each coefficient of the polynomial by its inverse in F]

Example : We have $a(x) \rightarrow$ and we have to find the identity inverse $[b(x)]$ $\rightarrow [a(x)]^{-1}$ over addition operation

For $GF(2^8)$

$$a(x) = a_7 x^7 + a_6 x^6 + \cdots + a_0$$

So for addition. $\boxed{a(x) + b(x) = 0.}$

$$b(x) = b_7 x^7 + b_6 x^6 + \cdots + b_0.$$

so $\Rightarrow$ $a_7 \oplus b_7 = 0 \Rightarrow a_7 = b_7$

In $GF(2) \Rightarrow$ we have 2 elements $\{0, 1\}$

$$\begin{Bmatrix} 0 \oplus 0 = 0 \\ 1 \oplus 1 = 0 \end{Bmatrix}$$

0 is the identity inverse of 0.
1 is " " " , 1.

Example :-

ii) Multiplication :-

In order to make the multiplication, we select a polynomial $m(x)$ of degree l, called the reduction polynomial.

The multiplication is then defined as follows:

$$\left[c(x) = a(x) \cdot b(x) \Leftrightarrow c(x) \equiv a(x) \times b(x) \pmod{m(x)} \right]$$

Example :-

if $\{1,2,3,4,5\}$ doing mod 6 operations

$2^{-1} \bmod 6 \Rightarrow$ not defined

i.e. $\gcd(2,6) \neq 1$. i.e. 2 and 6 are not co-prime to each other.

If $\{1,2,3,4,5,6\}$ doing mod 7 operation. $\boxed{\text{all no. are co-prime to number 7}}$

multiplicative inverse $\longleftrightarrow$ prime modulo.

To define a multiplicative inverse, we require that our modulo to be prime number.

Irreducible Polynomial :-

A polynomial $d(x)$ is irreducible over the field $GF(P)$ if there exists no two polynomials $a(x)$ and $b(x)$ with coefficients in $GF(P)$ such that $\left[d(x) = a(x)\, b(x) \right]$; where $a(x)$ and $b(x)$ are of degree >0.

Example :- (1) conside $GF(2^4)$ and polynomial (x^4+x+1) is irreducible polynomial. so

x^4+x+1 can't be written as $a(x) \times b(x)$

$$x^4+x+1 \neq a(x) \times b(x)$$

(2). $x^4+1 \Rightarrow$ is irreducible ?

$x^4+1 = (x+1)^4 =$ (Expand it) take modulo 2 operation.

x^4+1, has got factor $x+1$ $\boxed{x+1 \in GF(2^4)}$

so (x^4+1) is not irreducible polynomial.

Example (1) $x^4+x^3+1 \rightarrow$ Irreducible polynomial

(2) $x^4+x^3+x^2+x+1 \rightarrow$ " "

Example:-

1) Polynomial Addition.

$f(x) = x^5 + 3x^3 + 4$

$g(x) = 6x^6 + 4x^3$.

$f(x)+g(x)$

$$\begin{array}{r} x^5 + 3x^3 + 4 \\ +6x^6 + \quad + 4x^3 \\ \hline 6x^6 + x^5 + 7x^3 + 4 \end{array}$$

2). Polynomial Subtraction.

$f(x) = x^5 + 3x^3 + 4$.

$g(x) = 6x^6 + 4x^3$

$f(x) - g(x)$

$$\begin{array}{r} x^5 + 3x^3 + 4 \\ -\ 6x^6 + \quad + 4x^3 \\ \hline -6x^6 + x^5 - 1x^3 + 4. \end{array}$$

3). Polynomial Multiplication

$f(x) = x^5 + 3x^3 + 4$.

$g(x) = 6x^6 + 4x^3$.

$f(x) * g(x)$.

$$\begin{array}{r} x^5 + 3x^3 + 4 \\ \times \qquad 6x^6 + 4x^3 \\ \hline 4x^8 + 12x^6 + 16x^3 \\ 6x^{11} + 18x^9 \quad + 24x^6 \\ \hline 6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3. \end{array}$$

4) Polynomial Division

$f(x) = 6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3$

$g(x) = x^5 + 3x^3 + 4$.

$$\begin{array}{r} 6x^6 + 4x^3 \\ x^5+3x^3+4 \enclose{longdiv}{6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3} \\ -\ 6x^{11} + 18x^9 \quad + 24x^6 \\ \hline 4x^8 + 12x^6 + 16x^3 \\ -\ 4x^8 + 12x^6 + 16x^3 \\ \hline 0 \end{array}$$

But in many cases, the divisors cannot divide the dividents, which means we will have remainders. For example:-

$f(x) = 3x^6 + 7x^4 + 4x^3 + 5$

$g(x) = x^4 + 3x^3 + 4$

$$\begin{array}{r} 3x^2 - 9x + 34 \\ x^4+3x^3+4 \enclose{longdiv}{3x^6 + 7x^4 + 4x^3 + 5} \\ -\ 3x^6 + 9x^5 + 12x^2 \\ \hline -9x^5 + 7x^4 + 4x^3 - 12x^2 + 5 \\ -\ 9x^5 - 27x^4 - 36x \\ \hline 34x^4 + 4x^3 - 12x^2 + 36x + 5 \\ 34x^4 \pm 102x^3 + \qquad \pm 136 \\ \hline -98x^3 - 12x^2 + 36x - 131 \end{array}$$

$\boxed{\text{Remainder:-}\ -98x^3 - 12x^2 + 36x - 131}$

→ If a polynomial is divisible only by itself and constants, then we call this polynomial an <u>irreducible polynomial</u>.

→ If the coefficients are taken from the field F, then we say it is a polynomial over F.

→ With polynomials over field GF(P), you can add, multiply polynomials just like you have always done but the coefficients need to be reduced modulo P.

For example: Results with polynomials over GF(11). for last example

$f(x) = x^5 + 3x^3 + 4$

$g(x) = 6x^6 + 4x^3$

$f(x) + g(x) = \boxed{6x^6 + x^5 + 7x^3 + 4.}$

$f(x) - g(x) = -6x^6 + x^5 - 1.x^3 + 4 = \boxed{5x^6 + x^5 + 10x^3 + 4}$

$f(x) * g(x) = 6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3$

$= \boxed{6x^{11} + 7x^9 + 4x^8 + 3x^6 + 5x^3}$

$f(x) \div g(x) = 3x^2 - 9x + 34$ with remainder $-98x^3 - 12x^2 + 36x - 131$

$= \boxed{3x^2 + 2x + 3}$ with remainder $\boxed{x^3 + 10x^2 + 3x + 1}$

<u>Residue classes modulo 11 are:-</u>

[0] = {..., -22, -11, 0, 11, 22, ...}
[1] → {..., -21, -10, 1, 12, 23, ...}
[2] = {..., -20, -9, 2, 13, 24, ...}
[3] → {..., -19, -8, 3, 14, 25, ...}
[4] = {..., -18, -7, 4, 15, 26, ...}
[5] = {..., -17 -6, 5, 16, 27, ...}
[6] → {..., -16, -5, 6, 17, 28, ...}
[7] = {..., -15, -4, 7, 18, 29, ...}
[8] = {..., -14, -3, 8, 19, 30 ...}
[9] → {..., -13, -2, 9, 20, 31, ...}
[10] = {..., -12, -1, 10, 21, 32, ...}

Example :- $f(x) = x^6 + x^4 + x^2 + x + 1.$ (01010111)
$g(x) = x^7 + x + 1$ (10000011)

Irreducible polynomial for $m(x) = x^8 + x^4 + x^3 + x + 1. = GF(2^8) = GF(p^n).$

Addition :-

$f(x) + g(x) = x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1.$

$= x^7 + x^6 + x^4 + x^2 + 2x + 2.$

Arithmetic on the coefficient is performed modulo p.

Applied

Here $p = 2.$

$= x^7 + x^6 + x^4 + x^2 + 0.x + 0.1$

$\boxed{f(x) + g(x) = x^7 + x^6 + x^4 + x^2}$

Multiplication :-

$f(x) \times g(x) = (x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$

$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1.$

Applied with $p = 2$.

If multiplication results in a polynomial of degree greater than $n-1$, then the polynomial is reduced modulo some irreducible polynomial $m(x)$ of degree n.

We devide by $m(x)$ and ~~kep~~ keep the remainder.

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

So. $\boxed{F(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1}$

Note :- The residue class $[x+1]$ consists of all polynomials $a(x)$ that Statisfy the equality $\boxed{a(x) \bmod m(x) = x + 1}$