Polynomial Arithmetic

- Ordinary Polynomial Arithmetic
- With Coefficients in Z_p
- Defined by mod m(x) with coefficients in Z_p

ORDINARY 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.

Ordinary Polynomial Arithmetic

- Zero Degree Polynomial (when $n = 0$)
- Monic Polynomial (when $a_n = 1$)
- In Abstract Algebra, x is also called as indeterminate.

Ordinary Polynomial Arithmetic

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

(a) Addition

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

(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

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

(d) Division

Modular Polynomial Arithmetic

- $r(x) = f(x) \bmod g(x)$
- When $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 – x + 1$, $r(x) = x$
- When $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ and $g(x) = x^3 + x + 1$, $r(x) = 0$

Polynomials in GF(p)

GF(2)

- Polynomial Addition and Subtraction are the same.
- Polynomial Addition is equivalent to XOR operation.
- Polynomial Multiplication is equivalent to Logical AND operation.

GF(2) (Example 1)

- $f(x) = x^6 + x^5 + x^2 + 1$
- $g(x) = x^3 + x^2 + 1$
- In GF(2), $f(x) + g(x) = ?$

Solution:-

- $f(x) + g(x) = x^6 + x^5 + x^3$

GF(2) (Example 2)

- $f(x) = x^6 + x^3 + x^2 + 1$
- $g(x) = x^6 + x^5 + x^3 + x + 1$
- In GF(2), $f(x) + g(x) = ?$

<u>Solution:-</u>

- $f(x) + g(x) = x^5 + x^2 + x$

GF(2) (Example 3)

- $f(x) = x^6 + x^3 + x^2 + 1$
- $g(x) = x^6 + x^5 + x^3 + x + 1$
- In GF(2), $f(x) * g(x) = ?$

Solution:-

- $f(x) * g(x) = x^6 * (x^6 + x^5 + x^3 + x + 1) + x^3 * (x^6 + x^5 + x^3 + x + 1) + x^2 * (x^6 + x^5 + x^3 + x + 1) + (x^6 + x^5 + x^3 + x + 1)$
- $f(x) * g(x) = x^{12} + x^{11} + x^6 + x^4 + x^3 + x^2 + x + 1$

GF(2) (Example 4)

- $f(x) = x^3 + x^2 + x + 1$
- In GF(2), $[f(x)]^2 = ?$

Solution:-

- $[f(x)]^2 = x^6 + x^4 + x^2 + 1$

GF(2) (Example 5)

- $f(x) = x^6 + x^5 + x^2 + x + 1$
- $g(x) = x^3 + x^2 + 1$
- In GF(2), $f(x)/g(x) = ?$, $f(x) \bmod g(x) = ?$

Solution:-

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

GF(2) (Example 6)

- $f(x) = x^7 + x^6 + x^5 + x^2 + 1$
- $g(x) = x^3 + x^2 + x + 1$
- In GF(2), $f(x)/g(x) = ?$, $f(x) \bmod g(x) = ?$

Solution:-

- $f(x)/g(x) = x^4 + x + 1$
- $f(x) \bmod g(x) = x^2$

GF(2) (Example 7)

- $f(x) = x^4 + x^3 + x^2 + x$
- $g(x) = x^2 + 1$
- In GF(2), $f(x)/g(x) = ?$, $f(x) \bmod g(x) = ?$

Solution:-

- $f(x)/g(x) = x^2 + x$
- $f(x) \bmod g(x) = 0$

Irreducible Polynomials in GF(2)

- $f(x)$ is irreducible if it can't be expressed as a product of any 2 non-constant polynomials of lower degrees.
- Also called as Prime polynomials.

Degree	**Irreducible Polynomials**
1	x, $(x+1)$
2	$x^2 + x + 1$
3	$(x^3 + x + 1)$, $(x^3 + x^2 + 1)$
4	$(x^4 + x + 1)$, $(x^4 + x^3 + 1)$, $(x^4 + x^3 + x^2 + x + 1)$
5	$(x^5 + x^2 + 1)$, $(x^5 + x^3 + 1)$, $(x^5 + x^3 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x + 1)$, $(x^5 + x^4 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x^2 + 1)$

Pseudocode for GCD(f(x),g(x))

```
GCD{f(x),g(x)}
{
if(g(x)==0)
    return f(x);
else
    return GCD{g(x), f(x) mod g(x)}
}
```

GCD (Example 1)

- $f(x) = x^6 + x^5 + x^4 + x^2 + x + 1$
- $g(x) = x^4 + x + 1$
- GCD{f(x), g(x)} = ?

<u>Solution:-</u>

GCD{f(x), g(x)} = GCD{g(x), f(x) mod g(x)} =

GCD{$(x^4 + x + 1)$, $(x^6 + x^5 + x^4 + x^2 + x + 1)$ mod $(x^4 + x + 1)$} =

GCD{$(x^4 + x + 1)$, (x^3+x^2+x)} =

GCD{(x^3+x^2+x), $(x^4 + x + 1)$ mod (x^3+x^2+x)} =

GCD {(x^3+x^2+x), 1} =

GCD{1, (x^3+x^2+x) mod 1} =

GCD(1, 0) = 1

Polynomials in GF(p^m)

- $f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots\ldots\ldots\ldots + a_1 x + a_0$, where all the coefficients belong to GF(p).
- All the operations are performed modulo any irreducible polynomial (m(x)) with degree m.
- For example, for Polynomial arithmetic over GF(2^8), the coefficients are binary values, and a potential irreducible polynomial would be $(x^8 + x^4 + x^3 + x + 1)$.

Polynomial Arithmetic (Example 1)

- $f(x) = x^4 + x^3 + x^2 + x + 1$
- $g(x) = x^2 + 1$
- $m(x) = x^4 + x + 1$
- $f(x) + g(x) = ?$

Solution:-

- $[f(x) + g(x)] \bmod m(x) = [(x^4 + x^3 + x^2 + x + 1) + (x^2 + 1)] \bmod (x^4 + x + 1)$
- $[f(x) + g(x)] \bmod m(x) = (x^4 + x^3 + x) \bmod (x^4 + x + 1)$
- $[f(x) + g(x)] \bmod m(x) = x^3 + 1$

Polynomial Arithmetic (Example 2)

- $f(x) = x^5 + x^4 + x^2 + x + 1$
- $g(x) = x^5 + x^4 + x^3 + x^2 + x + 1$
- $m(x) = x^8 + x^4 + x^3 + x + 1$
- $f(x) * g(x) = ?$

<u>Solution:-</u>

- $[f(x) * g(x)] \bmod m(x) = [(x^5 + x^4 + x^2 + x + 1) * (x^5 + x^4 + x^3 + x^2 + x + 1)] \bmod (x^8 + x^4 + x^3 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = (x^{10} + x^7 + x^5 + x^3 + x^2 + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = x^7 + x^6 + 1$

Polynomial Arithmetic (Example 3)

- $f(x) = x^4 + x + 1$
- $g(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
- $m(x) = x^6 + x^5 + x^4 + x + 1$
- $f(x) * g(x) = ?$

Solution:-

- $[f(x) * g(x)] \bmod m(x) = [(x^4 + x + 1) * (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1)] \bmod (x^6 + x^5 + x^4 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = (x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x + 1) \bmod (x^6 + x^5 + x^4 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = x^5 + x$

Extended Euclidean Algorithm (EEA) on Polynomials in GF(p) and GF(p^m)

Pseudocode for EEA

```
EEA{a(x), b(x)}
{
u1(x)=1, u2(x)=0, v1(x)=0, v2(x)=1;
while(b(x)≠0)
{
    q(x)=a(x)/b(x); r(x)=a(x) mod b(x); u(x)=u1(x)-q(x)*u2(x); v=v1(x)-q(x)*v2(x);
a(x)=b(x); b(x)=r(x); u1(x)=u2(x); u2(x)=u(x); v1(x)=v2(x); v2(x)=v(x);
}
return(a(x), u1(x), v1(x))
}
```

EEA (Example 1)

- $a(x) = x^3 + x + 1$
- $b(x) = x^2 + 1$
- Calculate GCD{a(x), b(x)}= a(x)*u1(x)+b(x)*v1(x), and calculate u1(x) and v1(x), in GF(2)

Solution:-

Iteration 1:-

$a(x) = x^3 + x + 1$; $b(x) = x^2 + 1$; $q(x) = x$; $r(x) = 1$; $u1(x) = 1$; $u2(x) = 0$; $u(x) = 1$; $v1(x) = 0$; $v2(x) = 1$, $v(x) = x$

EEA (Example 1) (Contd..)

Iteration 2:-

$a(x) = x^2 + 1$, $b(x) = 1$; $q(x) = x^2 + 1$; $r(x) = 0$; $u1(x) = 0$; $u2(x) = 1$; $u(x) = x^2 + 1$; $v1(x) = 1$; $v2(x) = x$, $v(x) = x^3 + x + 1$

Iteration 3:-

$a(x) = 1$; $b(x) = 0$; $u1(x) = 1$, $u2(x) = x^2 + 1$, $v1(x) = x$, $v2(x) = x^3 + x + 1$

- Therefore GCD{(a(x), b(x)} = 1; $u1(x) = 1$; $v1(x) = x$;
- Also, we can say that $MI(x^3 + x + 1) \bmod (x^2 + 1) = 1$

EEA (Example 2)

- Calculate $MI(x^2+1) \bmod (x^4 + x + 1)$ in $GF(2^4)$

Solution:-

Iteration 1:-

$a(x) = x^4 + x + 1$; $b(x) = x^2 + 1$; $q(x) = x^2 + 1$; $r(x) = x$;

$v1(x) = 0$; $v2(x) = 1$; $v(x) = x^2 + 1$

Iteration 2:-

$a(x) = x^2 + 1$; $b(x) = x$; $q(x) = x$; $r(x) = 1$;

$v1(x) = 1$; $v2(x) = x^2 + 1$; $v(x) = x^3 + x + 1$

EEA (Example 2) (Contd..)

Iteration 3:-

$a(x) = x;\ b(x) = 1;\ q(x) = x;\ r(x) = 0;$

$v1(x) = x^2 + 1;\ v2(x) = x^3 + x + 1;\ v(x) = (x^4 + x + 1) \bmod (x^4 + x + 1) = 0$

Iteration 4:-

$a(x) = 1;\ b(x) = 0;$

$v1(x) = x^3 + x + 1;\ v2(x) = 0$

- Therefore, $MI(x^2+1) \bmod (x^4 + x + 1) = (x^3 + x + 1)$

EEA (Example 3)

- Calculate MI($x^4 + x^3 + x^2 + 1$) mod ($x^8 + x^4 + x^3 + x + 1$)

Solution:-

Iteration 1:-

$a(x) = x^8 + x^4 + x^3 + x + 1$; $b(x) = x^4 + x^3 + x^2 + 1$;

$q(x) = x^4 + x^3 + x + 1$; $r(x) = x^2$;

$v1(x) = 0$; $v2(x) = 1$; $v(x) = x^4 + x^3 + x + 1$

Iteration 2:-

$a(x) = x^4 + x^3 + x^2 + 1$; $b(x) = x^2$; $q(x) = x^2 + x + 1$; $r(x) = 1$;

$v1(x) = 1$; $v2(x) = x^4 + x^3 + x + 1$; $v(x) = x^6$

EEA (Example 3) (Contd..)

Iteration 3:-

$a(x) = x^2$; $b(x) = 1$; $q(x) = x^2$; $r(x) = 0$;

$v1(x) = x^4 + x^3 + x + 1$; $v2(x) = x^6$; $v(x) = 0$;

Iteration 4:-

$a(x) = 1$; $b(x) = 0$; $v1(x) = x^6$; $v2(x) = 0$;

- Therefore, $MI(x^4 + x^3 + x^2 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = x^6$