Introduction to Number Theory

Contd..

Finite Field

- A finite field is a fieldA finite field is a field with a finite order (i.e., number of elements), also called a Galois field.
- The order of a finite field is always a primeThe order of a finite field is always a prime or a powerThe order of a finite field is always a prime or a power of a prime.
- Finite fields of order p can be defined using arithmetic (mod p) and denoted as Z_p or GF(p).
- (Note : Z_n is a field iff n is prime)

GF(p) Fields

- Finite fields of order $p^{n,}$, for n>1, can be defined using arithmetic over Polynomials.

- When $n = 1$, we have GF(p) field. This field can be the set $Z_{p=}$ {0, 1, ..., p − 1}, with two arithmetic operations:
  1.) (mod p) addition
- 2.) (mod p) multiplication.

Contd.

- A very common field in this category is GF(2) with the set {0, 1} and two operations, addition and multiplication mod 2, as shown

GF(2)

$\{0, 1\}$ $+$ $\times$

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

a	0	1
−a	1	0

a	0	1
a^{-1}	—	1

Inverses

Contd.

- We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
$-a$	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	–	1	3	2	4

Multiplicative inverse

GF(2^n) FIELDS

- There exist a unique finite field of order 2^n for each positive integer n which is denoted by GF(2^n).
- We can work in GF(2^n). The elements in this set are n-bit words. Order of GF(2^n) is 2^n
- The elements of GF(2^n) can also be represented by polynomials of degree at most n-1, with coefficients in GF(2) .

Polynomials

- A polynomial of degree $n - 1$ is an expression of the form

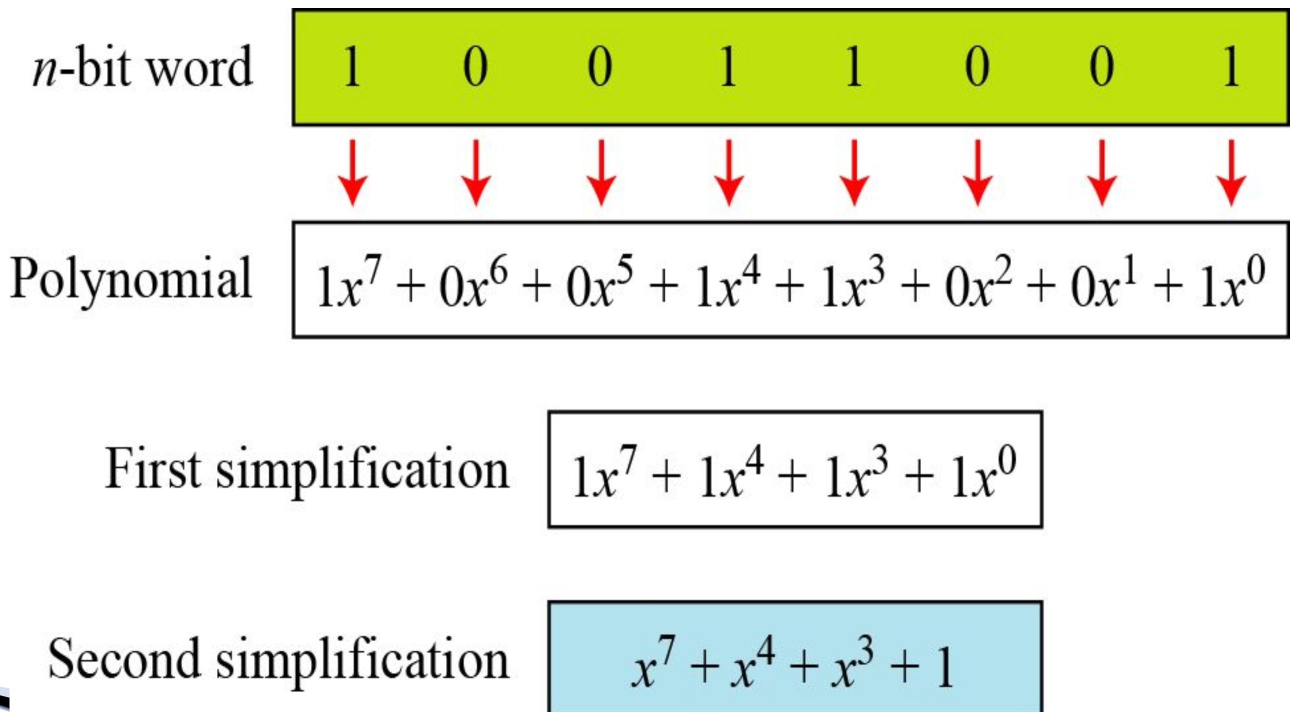
$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x^1 + a_0 x^0$$

where x^i is called the i^{th} term and a_i is called coefficient of the i^{th} term.

- The **degree** of a **polynomial** is the highest **degree** of its terms. The degree is the value of the greatest exponent of its terms. The degree is the value of the greatest exponent of any expression (except the constant) in the polynomial.

Contd.

- Below figure show how we can represent the 8-bit word (10011001) using a polynomials.



Contd.

- To find the 8-bit word related to the polynomial $x^5 + x^2 + x$, we first supply the omitted terms. Since $n = 8$, it means the polynomial is of degree 7. The expanded polynomial is

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

- This is related to the 8-bit word 00100110

Arithmetic in GF(2^n)

- We may add, subtract polynomials in as we do for ordinary arithmetic . Even though the coefficients are elements of GF(2) instead of actual integers, it is easy to do the calculations so long as we remember to always reduce coefficients mod 2.

Contd.

- Note: Addition and subtraction operations on polynomials are the same operation in (mod 2) arithmetic.
- Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$. We use the symbol $\oplus$ to show that we mean polynomial addition. The following shows the procedure:

$$
\begin{array}{lll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus & \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & & \\
\text{--} & & \\
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow & x^5 + x^3 + x + 1
\end{array}
$$

Multliplication in GF(2^n)

- The coefficient multiplication is done in GF(2).
- The multiplying x^i by x^j results in x^{i+j}.
- The multiplication may create terms with degree more than $n - 1$, which means the result needs to be reduced using a modulus polynomial (the final answer is obtained by reducing the result of multiplication by an irreducible polynomial of degree n).

Irreducible polynomials (modulus polynomials).

- A polynomialA polynomial is said to be irreducible if it cannot be factored into polynomials of lower positive degrees over the same field

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

Contd.

- Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$. Note that we use the symbol $\otimes$ to show the multiplication of two polynomials.

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$

$$P_1 \otimes P_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$

$$P_1 \otimes P_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

- To find the final result, divide the polynomial of degree 12 by an irreducible polynomial of degree 8 (the modulus) and keep only the remainder. Next shows the process of division.

Contd.

- *Polynomial division with coefficients in GF(2)*

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\cline{2-2}
\text{Remainder} & \boxed{x^5 + x^3 + x^2 + x + 1}
\end{array}
$$

Contd

- When , GF(2^n) can be represented as) can be represented as the field) can be represented as the field of equivalence classes) can be represented as the field of equivalence classes of polynomials) can be represented as the field of equivalence classes of polynomials whose coefficients) can be represented as the field of equivalence classes of polynomials whose coefficients belong to GF(2). Any irreducible polynomial) can be represented as the field of equivalence classes of polynomials whose coefficients belong to GF(2). Any irreducible polynomial of degree n yields the same

Addition table for GF(2^3)

$\oplus$	000 (0)	001 (1)	010 (x)	011 ($x + 1$)	100 (x^2)	101 $x^2 + 1$	110 ($x^2 + x$)	111 ($x^2 + x + 1$)
000 (0)	000 (0)	001 (1)	010 (x)	011 ($x + 1$)	100 (x^2)	101 ($x^2 + 1$)	110 ($x^2 + x$)	111 ($x^2 + x + 1$)
001 (1)	001 (1)	000 (0)	011 ($x + 1$)	010 (x^2)	101 ($x^2 + 1$)	100 ($x^2 + x$)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)
010 (x)	010 (x)	011 ($x + 1$)	000 (0)	001 (1)	110 ($x^2 + x$)	111 ($x^2 + x + 1$)	100 ($x^2 + x$)	101 ($x^2 + 1$)
011 ($x + 1$)	011 ($x + 1$)	010 (x)	001 (1)	000 (0)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)	101 ($x^2 + 1$)	100 (x^2)
100 (x^2)	100 (x^2)	101 ($x^2 + 1$)	110 ($x^2 + x$)	111 ($x^2 + x + 1$)	000 (0)	001 (1)	010 (x)	011 ($x + 1$)
101 ($x^2 + 1$)	101 ($x^2 + 1$)	100 (x^2)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)	001 (1)	000 (0)	011 ($x + 1$)	010 (x)
110 ($x^2 + x$)	110 ($x^2 + x$)	111 ($x^2 + x + 1$)	100 (x^2)	101 ($x^2 + 1$)	010 (x)	011 ($x + 1$)	000 (0)	001 (1)
111 ($x^2 + x + 1$)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)	101 ($x^2 + 1$)	100 (x^2)	011 ($x + 1$)	010 (x)	001 (1)	000 (0)

Multiplication table for GF(2^3)

$\otimes$	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
010 (x)	000 (0)	010 (x)	100 (x)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	001 (1)	011 ($x+1$)
011 ($x+1$)	000 (0)	011 ($x+1$)	110 (x^2+x)	101 (x^2+1)	001 (1)	010 (x)	111 (x^2+x+1)	100 (x)
100 (x^2)	000 (0)	100 (x^2)	101 (x^2+1)	001 (1)	111 (x^2+x+1)	011 ($x+1$)	010 (x)	110 (x^2+x)
101 (x^2+1)	000 (0)	101 (x^2+1)	111 (x^2+x+1)	010 (x)	011 ($x+1$)	110 (x^2+x)	100 (x^2)	001 (1)
110 (x^2+x)	000 (0)	110 (x^2+x)	001 (1)	111 (x^2+x+1)	010 (x)	100 (x^2)	011 ($x+1$)	101 (x^2+1)
111 (x^2+x+1)	000 (0)	111 (x^2+x+1)	011 ($x+1$)	100 (x^2)	110 (x^2+x)	001 (1)	101 (x^2+1)	010 (x)