TOPIC : 1 – Polynomials

FINITE FIELDS AND POLYNOMIALS

Def: polynomial Ring:

R is a ring under the operation of Addition & Multiplication.

Assume that $n \geq m$,

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x$$

where $b_i = z$ for $i > m$

$$f(x) \cdot g(x) = (a_n b_m) x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \dots + (a_1 b_0 + a_0 b_1) x^1 + (a_0 b_0) x^0$$

is called the polynomial ring (or) ring of polynomials over R.

Example 1:

Let $f(x), g(x) \in Z_7(x)$, where

$f(x) = 2x^4 + 2x^3 + 3x^2 + x + 4$ and

$g(x) = 3x^3 + 5x^2 + 6x + 1$, determine the

values of $f(x) + g(x)$, $f(x) - g(x)$

$f(x) * g(x)$

Solution:

$$f(x) + g(x) = (2x^4 + 2x^3 + 3x^2 + x + 4) + (3x^2 + 5x^2 + 6x + 1)$$

$$= 2x^4 + 5x^3 + 8x^2 + 7x + 5$$

$(8 \equiv 1 \pmod 7)$, $(7 \equiv 0 \bmod 7)$

$$= 2x^4 + 5x^3 + 1x^2 + 5$$

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

$$= 2x^4 + 5x^3 + 1x^2 + 0x + 5$$

$$= 2x^4 - x^3 - 2x^2 - 5x + 3.$$

$(-1 \equiv 6 \pmod 7)$, $(-2 \equiv 5 \pmod 7)$,

$(-5 \equiv 2 \pmod 7)$

$$= 2x^4 + 6x^2 + 5x^2 + 2x + 3$$

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

$$= (6x^7 + 10x^6 + 12x^5 + 2x^4) + (6x^6 + 10x^5 + 12x^4 + 2x^3)$$

$$+ (9x^5 + 15x^4 + 18x^3 + 3x^2) + (3x^4 + 5x^3 + 6x^2)$$

$$= 6x^7 + 16x^6 + 31x^5 + 32x^4 + 37x^3 + 29x^2 + 25x + 4$$

$$= 6x^7 + 2x^6 + 3x^5 + 4x^4 + 2x^3 + x^2 + 4x + 4$$

Since $16 \equiv 2 \pmod 7$, $31 \equiv 3 \pmod 7$,

$32 \equiv 4 \pmod 7$, $37 \equiv 2 \pmod 7$

$29 \equiv 1 \pmod 7$