



FINITE FIELDS AND POLYNOMIALS

Def: polynomial Ring:

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

Assume that $n \geq m$,

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

where $b_i = 0$ 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 .

Ex: 1
Ex: 2
Ex: 3
Ex: 4
Ex: 5
Ex: 6
Ex: 7
Ex: 8
Ex: 9
Ex: 10
Ex: 11
Ex: 12
Ex: 13
Ex: 14
Ex: 15
Ex: 16
Ex: 17
Ex: 18
Ex: 19
Ex: 20
Ex: 21
Ex: 22
Ex: 23
Ex: 24
Ex: 25
Ex: 26
Ex: 27
Ex: 28
Ex: 29
Ex: 30
Ex: 31
Ex: 32
Ex: 33
Ex: 34
Ex: 35
Ex: 36
Ex: 37
Ex: 38
Ex: 39
Ex: 40
Ex: 41
Ex: 42
Ex: 43
Ex: 44
Ex: 45
Ex: 46
Ex: 47
Ex: 48
Ex: 49
Ex: 50
Ex: 51
Ex: 52
Ex: 53
Ex: 54
Ex: 55
Ex: 56
Ex: 57
Ex: 58
Ex: 59
Ex: 60
Ex: 61
Ex: 62
Ex: 63
Ex: 64
Ex: 65
Ex: 66
Ex: 67
Ex: 68
Ex: 69
Ex: 70
Ex: 71
Ex: 72
Ex: 73
Ex: 74
Ex: 75
Ex: 76
Ex: 77
Ex: 78
Ex: 79
Ex: 80
Ex: 81
Ex: 82
Ex: 83
Ex: 84
Ex: 85
Ex: 86
Ex: 87
Ex: 88
Ex: 89
Ex: 90
Ex: 91
Ex: 92
Ex: 93
Ex: 94
Ex: 95
Ex: 96
Ex: 97
Ex: 98
Ex: 99
Ex: 100



Example 1:

Let $f(x), g(x) \in \mathbb{Z}_7[x]$, where

$$f(x) = 2x^4 + 2x^3 + 3x^2 + x + 4 \text{ and}$$

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

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

$$f(x) + g(x)$$

Solution:

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

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

$$(8 \equiv 1 \pmod{7}), (7 \equiv 0 \pmod{7})$$

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

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

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

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

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

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

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



$$\begin{aligned}f(x) * g(x) &= (2x^4 + 8x^3 + 22x^2 + x + 4) * (32x^3 + 15x^2 + 11x + 1) \\&= (6x^7 + 10x^6 + 12x^5 + 2x^4) + (6x^6 + 10x^5 + 12x^4 + 2x^3) \\&\quad + (9x^5 + 15x^4 + 18x^3 + 32x^2) + (32x^4 + 15x^3 + 6x^2) \\&= 6x^7 + 16x^6 + 13x^5 + 32x^4 + 27x^3 + 27x^2 + 25x + 4 \\&= 6x^7 + 2x^6 + 3x^5 + 4x^4 + 2x^3 + x^2 + x + 4\end{aligned}$$

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

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

$29 \equiv 1 \pmod{7}$