FLAG - TD 03.06.23

$$A = a_0 + a_1 x + \text{—} a_m x^m$$

$$A(1/x) = a_0 + \frac{a_1}{x} + \text{—} + \frac{a_m}{x^m} \to \tilde{A} = a_m + a_{m-1} + \text{—} + a_0 x^m$$

multiplication of power series is same as polynomial multiplication

~~Example~~

Problem

$A = x^9 + x^3 + 2$ in $\mathbb{F}_3[x]$

$B = x^3 + 2x + 2$, A/B.

$\tilde{A} = 1 + x^6 + 2x^9$, $\tilde{B} = 1 + 2x^2 + 2x^3$

$m = 9$, $n = 3$; precision $m - n + 1 = 7$, $O(x^7)$

$\tilde{Q} = \tilde{A}\tilde{B}^{-1}$

Compute a inverse of $\tilde{B}$.

$S = 1 + 2x^2 + 2x^3 + O(x^7)$ $O(x^{\lceil n/2 \rceil})$

$n = 7$

$S = 1 + 2x^2 + 2x^3 + O(x^4)$

$n = 4$

$S = 1 + O(x^2)$

$n = 2$ $S = 1 + O(x)$

$n = 1$

$S = 1^{-1} + O(x) = 1 + O(x)$

$$U = T + (1 - ST)T + O(x^2)$$

$$= 1 + (1 - 1\cdot 1)1 + O(x^2)$$

$$= 1 + O(x^2)$$

$$V = U + (1 - US)U + O(x^4)$$

$$= 1 + (1 - 1\cdot(1 + 2x + 2x^3)\cdot 1 + O(x^4)$$

$$= 1 + (1 - 1 - 2x^2 - 2x^3)\cdot 1 + O(x^4)$$

$$= 1 + (\cancel{1} + 2 + x^2 + x^3) + O(x^4)$$

$$= 1 + x^2 + x^3 + O(x^4)$$

$$T = V + (1 - VS)V + O(x^7)$$

$$= (1 + x^2 + x^3) + (1 - (1 + x^2 + x^3)(1 + 2x^2 + 2x^3))(1 + x^2 + x^3) + O(x^7)$$

$$= (1 + x^2 + x^3) + (1 - (1 + 2x^2 + \cancel{2x^3} + x^2 + 2x^4 + 2x^5 \cancel{+ x^3} + 2x^5 + 2x^6)$$

$$(1 + 2x^2 + 2x^3)$$

$$= (1 + x^2 + x^3) + (\cancel{1} - 1 - \cancel{3x^2} - \cancel{3x^3} - 2x^4 - 4x^5 - 2x^6)(1 + x^2 + x^3) + O(x^7)$$

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

$$= (1 + x^2 + x^3) + (x^4 + x^6 + 2x^5 + x^6) + O(x^7)$$

$$= 1 + x^2 + x^3 + x^4 + 2x^5 + 2x^6 + O(x^7)$$

FLAG-TD 06.03.23

$$\tilde{B}^{-1} = 1+x^2+x^3+x^4+2x^5+2x^6$$

$$\hat{A}\hat{B}^{-1} = (1+x^6+2x^9)(1+x^2+x^3+x^4+2x^5+2x^6)$$
$$= 1+x^2+x^3+x^4+3x^6$$
$$= 1+x^2+x^3+x^4+2x^5$$

[1, 0, 1 1, 1, 2]

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

$$R = A - BQ$$

$$BQ = (x^3+2x+2)(2x+x^2+x^3+x^4+x^6)$$
$$= \cancel{2x^4}+\cancel{x^5}+x^6+\cancel{x^2}+2x^3+2x^4+\cancel{2x^5}$$
$$+x+\cancel{2x^2}+2x^3+\cancel{2x^4}+\cancel{2x^6}+\cancel{2x^7}+\cancel{x^7}+x^9$$
$$= x+x^3+x^9$$

$$R = (x^9+x^3+2)-(x^9+x^3+x)$$

$$= 2-x = 2x+2$$

$$(Q,R) = (2x+x^2+x^3+x^4+x^6,\ 2x+2)$$