Lattices

Problem Session 2

Task: Implement NTT and NTT^{-1} over $Z_{257}[X]/(X^{32} + 1)$

$$\begin{aligned} X^{32} + 1 = {} & (X-46)(X+46)(X-35)(X+35)(X-117)(X+117)(X-73)(X+73) \\ & (X-70)(X+70)(X-92)(X+92)(X-23)(X+23)(X-111)(X+111) \\ & (X-67)(X+67)(X-44)(X+44)(X-11)(X+11)(X-81)(X+81) \\ & (X-88)(X+88)(X-123)(X+123)(X-95)(X+95)(X-22)(X+22) \end{aligned}$$

$$mod\ 257$$

Coefficient representation

CRT representation

$$f = a_0 + a_1 x + \cdots + a_{31} x^{n-1} \longrightarrow \hat{f} = (f(46), f(-46), \ldots, f(22), f(-22))$$

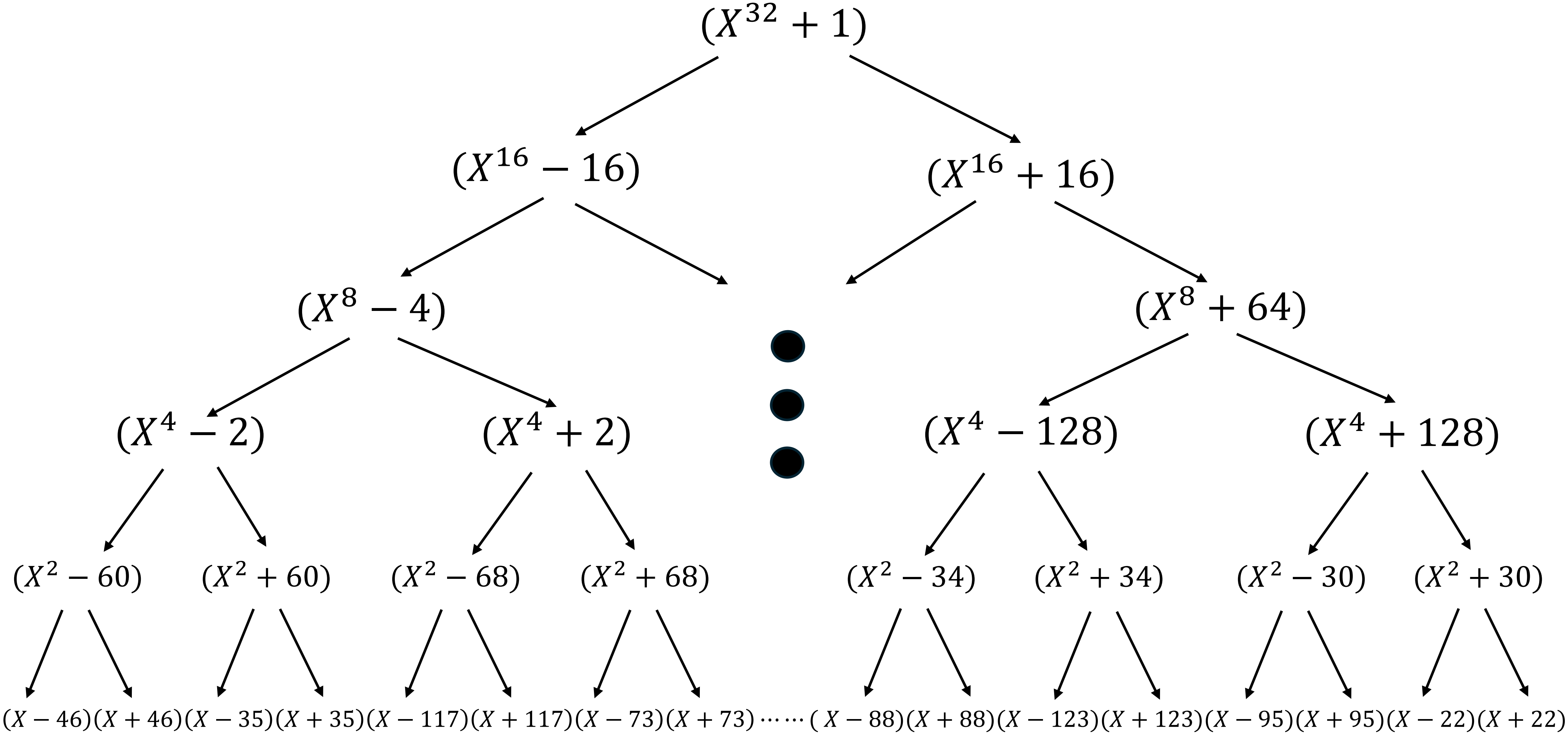
Naive solution

$$\begin{aligned} X^{32} + 1 = \; & (X-46)(X+46)(X-35)(X+35)(X-117)(X+117)(X-73)(X+73) \\ & (X-70)(X+70)(X-92)(X+92)(X-23)(X+23)(X-111)(X+111) \\ & (X-67)(X+67)(X-44)(X+44)(X-11)(X+11)(X-81)(X+81) \\ & (X-88)(X+88)(X-123)(X+123)(X-95)(X+95)(X-22)(X+22) \quad mod\ 257 \end{aligned}$$

$$f = a_0 + a_1 x + \cdots + a_{31} x^{n-1} \longrightarrow \hat{f} = (f(46), f(-46), \dots, f(22), f(-22))$$

$$\begin{pmatrix} 1 & 46 & 46^2 & \cdots & 46^{30} & 46^{31} \\ 1 & -46 & (-46)^2 & \cdots & (-46)^{30} & (-46)^{31} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 22 & 22^2 & \cdots & 22^{30} & 22^{31} \\ 1 & -22 & (-22)^2 & \cdots & (-22)^{30} & (-22)^{31} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{30} \\ a_{31} \end{pmatrix} = \begin{pmatrix} \\ \\ \hat{f} \\ \\ \\ \end{pmatrix}$$

Fast solution: Number Theoretic Transform



$(X^{32} + 1)$

$(X^{16} - 16)$ $(X^{16} + 16)$

$(X^{8} - 4)$ $(X^{8} + 64)$

$(X^{4} - 2)$ $(X^{4} + 2)$ $(X^{4} - 128)$ $(X^{4} + 128)$

$(X^{2} - 60)$ $(X^{2} + 60)$ $(X^{2} - 68)$ $(X^{2} + 68)$ $(X^{2} - 34)$ $(X^{2} + 34)$ $(X^{2} - 30)$ $(X^{2} + 30)$

$(X - 46)(X + 46)(X - 35)(X + 35)(X - 117)(X + 117)(X - 73)(X + 73) \cdots\cdots (X - 88)(X + 88)(X - 123)(X + 123)(X - 95)(X + 95)(X - 22)(X + 22)$

In the code…

$$\begin{aligned} X^{32} + 1 = \; & (X-46)(X+46)(X-35)(X+35)(X-117)(X+117)(X-73)(X+73) \\ & (X-70)(X+70)(X-92)(X+92)(X-23)(X+23)(X-111)(X+111) \\ & (X-67)(X+67)(X-44)(X+44)(X-11)(X+11)(X-81)(X+81) \\ & (X-88)(X+88)(X-123)(X+123)(X-95)(X+95)(X-22)(X+22) \end{aligned}$$

- RLIST: [46, 211, 35, 222, 117, 140, 73, 184, 70, 187, 92, 165, 23, 234, 111, 146, 67, 190, 44, 213, 11, 246, 81, 176, 88, 169, 123, 134, 95, 162, 22, 235]

- RTREE: [[16], [4, 64], [2, 32, 8, 128], [60, 68, 17, 15, 120, 121, 34, 30], [46, 35, 117, 73, 70, 92, 23, 111, 67, 44, 11, 81, 88, 123, 95, 22]]