

⑤ mdmod(A(x), v(x), p)

$\left. \begin{matrix} A(x) \\ v(x) \end{matrix} \right\} \text{poly à 1 littéral}$
 $|p| \neq 0, 1$

ret $A'(x) \equiv A(x) \begin{pmatrix} \text{mod } p \\ \text{mod } v(x) \end{pmatrix}$
 $\text{deg } A'(x) < \text{deg } v(x)$

YMDMOD: BSR

WCALMD1

décode A, v, p

$p = [A3]$
 $A = \mathcal{P}_{A0}$
 $v = \mathcal{P}_{A4}$

LEA

XMPMOD1, A2

BRA

MIS~~4~~