

⑤ mdinv (A(x), v(x), p)

poly A } à 1 littéral
v irred }
|P| ≠ 0, 1

ret B(x) ~~est~~ l'inverse de A(x) :
B(x) A(x) ≡ 1 mod $\begin{matrix} p \\ v(x) \end{matrix}$
deg(B) < deg(v)

YMDINV:BSR WCALMD1

décodes
A, v, p

p = [A3]
A = $\int A_0$
v = $\int A_4$

LEA XMPINV, A2
BRA MI84