⑤ mdff (A, p) A polynome à un littéral
|p| ≠ 0, 1 nb premier

factorise A (mod p)

YMDFF : BSR WCALMD2 décode A, p [A3] = p
P_{A_0} = A

MOVE.L A5, -(SP)
ADDQ #6, A6
BSR XMFPLU pose en tête A^F mod p
MOVE.L (SP)+, A5
BRA POPNEW { ote P_0 et P_{-1} A2 A6) mis sur pile

MOVEM.L A0/A3/A6, -(SP)
MOVE.L A3, A0 p premier ?
BSR XMPT
MOVEM.L (SP)+, A0/A3/A6
CMP # $4000, -(A6)
BEQ ERRINPR → non premier
BSR XMPPM pose A' ≡ A mod p
MOVE.L A2, A0
BSR XMFPLU pose A^F mod p
MOVE.L (SP), A0
BSR XLB76
MOVEM.L (SP)+, A2/A5
BRA POPNEW { ote P_0 et P_{-1} A2 A6 mis sur pile

ERRINPT :