

10

Entrée: $P_{A_0} = A$

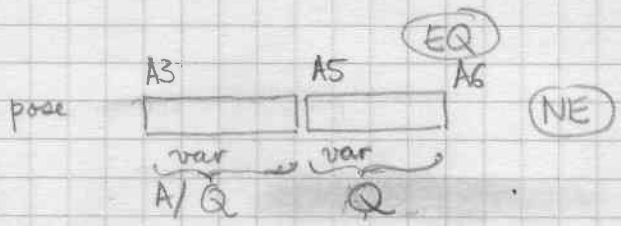
$P_{A_1} = B$

$[A_3] = P$

Calculer $Q = \text{pgcd}(A, B) \text{ mod } P$

EQ $Q = 1$

NE $Q \neq 1$



XMF PAR: MOVE.L A0/A3/A6 - (SP)

BSR XMPGCD $\text{pose } Q = \text{pgcd}(A, B, P)$

MOVE.L (SP)+, A0/A3
A P

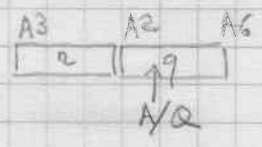
TST.L (A2)

BNE MJ20

MOVE.L (SP)+, A6 $\downarrow Q = 1 (=1)$

RTS

MJ20: MOVE.L A2, A1 Q



BSR XMPDIV

MOVE.L A2, A0

BSR XPSAF $3 \text{ A/Q forme factoris\u00e9e}$

MOVE.L (SP)+, A0 Q

MOVEM.L A0/A2/A6, -(SP)



BSR XPSAF $Q \text{ factoris\u00e9}$

MOVE.L A6, A5 $\text{fu } Q^F$

MOVEM.L (SP)+, A0/A2/A6

MOVE.L A0, A3

BSR XLB76

EXG A5, A6

BSR XLB76

MOVEQ #1, D0 $) \text{NE}$

RTS