

Entrée

$P_{A0} = t(x)$

consigne A0/A3

$var A1 \text{ (stack)} = u_1 * \dots * u_k$

$[A3] = q$

$var A4 = v_1 * \dots * v_k$

Pre en libe  $var A2$  (facteur non legal) =  $w_1 * \dots * w_k$

$w_i = [mdmod(t(x) * v_i(x), u_i(x), q)] * q$

LIFTA : MOVEM.L / A0/A3/A6, -(SP)

MOVE.L (A1)+, (A6)+

\* 4oct

MOVE (A4)+, D6

nb de fact + 1

ADDQ #2, A4

t(x)
q
libe

MJ80 : SUBQ #1, D6

D1/A1/A4

BEQ MJ82

→ fin

MOVE.L (A4)+, D0

MOVE.L A4, A0  $v_i(x)$

ADD.L D0, A4  $t, q$

~~MOVEM.L (SP), A1/A3~~ ← ADDQ #4, A6

MOVEM.L D6/A1/A4/A6, -(SP) ← MOVEM.L 16(SP), A1/A3

BSR XMPMUL  $t(x) v_i(x)$  consigne A3

MOVE.L 4(SP), A1

MOVE.L (A1)+, D0

ADD.L D0, 4(SP) ←  $addq \#4, D0$   $w_i(x) = P_{A1}$

MOVE.L A2, A0

BSR XMPMOD  $mdmod$

MOVE.L A2, A0

MOVE.L A3, A1  $q$

BSR XMCTE  $P_{A2} = q * mdmod = w_i$

MOVEM.L (SP)+, D6/A1/A4

MOVE.L (SP), A0

BSR XLB76

MOVE #1, (A6)+

MOVE.L (SP)+, A0

MOVE.L A6, D0

SUB.L A0, D0

MOVE.L D0, -(A0)

BRA MJ80

MJ82 : MOVEM.L (SP)+, A0/A3

MJ83 : MOVE.L (SP)+, A2

RTS