

10

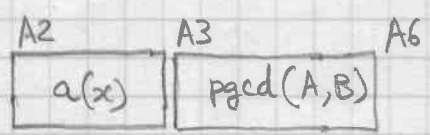
Entrée

$$P_{A_0} = A(x)$$

$$P_{A_1} = B(x)$$

} unilittéraux $\in \mathbb{Z}[x]$

Sortie



$$\text{pgcd}(A,B) = x^m + \dots$$

(normalisé à 1)
coef rationnels

[Algorithme d'Euclide étendu Knuth p325]

repite XMPINV

XJPINV: MOVE.L A6, -(SP)

BSR XPSP1 $u_1 = 1$

MOVE.L A6, -(SP)

BSR XPSAP $u_3 = A$

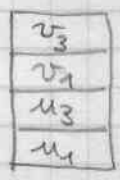
MOVE.L A1, A0

MOVE.L A6, -(SP)

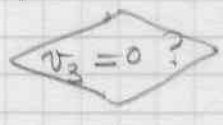
BSR XPSPO $v_1 = 0$

MOVE.L A6, -(SP)

BSR XPSAP $v_3 = B$



MK11: MOVE.L (SP), A1

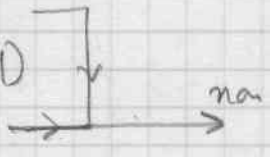


TST.L (A1)

BNE MK12

CMP #4000, 4(A1)

BNE MK12



ADDQ #4, SP

MOVE.L (SP)+, A6

MOVE.L (SP), A1

MOVE (A1)+, D0

ADD D0, D0 ← ADD D0, D0

ADD D0, A1

ADDQ #2, A1

u_3



$A1 = \{2\}$ coef de u_3

(10)

normalize u_1

~~MOVE.L (A0), A1~~

BSR XDCTE

u_1

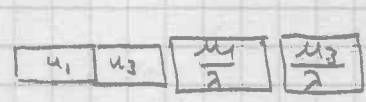
$\frac{u_1}{2}$

(conserve A1)

MOVE.L (SP)+, A0

u_3

MOVEM.L ~~(A0)~~



BSR XDCTE

$\frac{u_3}{2}$

MOVE.L A6, A3

MOVEM.L (SP)+, A2/A6 ⊗

MOVE.L (SP), A0

BSR XLB76

copy $u_1/2$

~~EXG~~ A3, A6

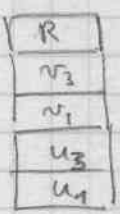
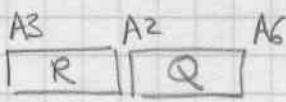
BSR XLB76

copy $u_3/2$

MOVE.L (SP)+, A2

RTS

MK12: MOVE.L 8(SP), A0^{u3}



BSR XJPDIV

MOVE.L A3, -(SP) R=t3

MOVE.L A2, A0

MOVE.L 8(SP), A1 v1

BSR XMULP Q*v1

MOVE.L A2, A1

MOVE.L 16(SP), A0 u1

BSR XSUBP t1 = u1 - Q*v1

MOVE.L (SP), A0 t3

MOVE.L A2, -(SP)

BSR XPSAP recopic t3 = R

MOVEM.L A2/A6, -(SP)

MOVEM.L 16(SP), A0/A2/A3/A6
v3 v1 u3 u1

EXG A0, A6

BSR XLB76 copie u1 ↔ v1

MOVE.L A6, 24(SP)

MOVE.L 12(SP), A6 find v3

BSR XLB76 u3 ← v3

MOVE.L A6, 20(SP)

MOVE.L (SP)+, A6 t3

MOVE.L (SP)+, A1 fin t3

MOVE.L (SP)+, A2 t1

BSR XLB76

ADDQ #8, SP

MOVE.L A6, -(SP)

MOVE.L A1, A6

BSR XLB76

BRA MK11