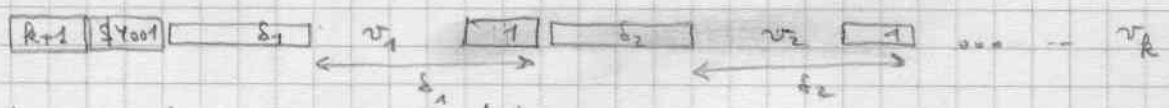
(10) Entrée "var_{A_0}" = $\lambda u_1 \dots u_k$ u_i : poly à 1 seul littéral x

P = [A3] $pgcd(u_i, u_j) = 1$

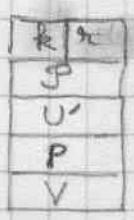
conserve A3

Sortie crée une pseudo variable var_{A_2} en tête



où v_i est un polynome en x (entier)
mais en général v_i $pgcd(v_i, v_j) \neq 1$ et var_{A_2} n'a pas l'ordre canonique.

Les v_i sont tels que $\sum_{i=1}^{k} \frac{v_i}{u_i} = \frac{1}{u_1 u_2 \dots u_k}$ et $deg(v_i) < deg(u_i)$




```
XMFBEZ:MOVEM.L   A3/A6,-(SP)
       MOVE.L  #$24001,(A6)+   } crée V = 1 * 1
       MOVE.L  #8,(A6)+
       BSR XPSP1 ← MOVE #1,(A6)+   → crée P = 1
       BSR XPSP1
       MOVEQ #1,D0                 n = 1
       MOVEM.L  D0/A2,-(SP)
```


```
MJ32 : MOVE.L   (SP),D5/A0/A1/A3
                 k  P  U  P
       CMP   (SP),D5
       BCS   MJ36
fin MOVE.L  A0,A6
       LEA   -2(A0),A6
       ADD   #16,SP
       MOVE.L  (SP)+,A2
       RTS
```

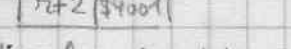
```
MOVE (A0)+,D1    k+1
BSR  SLNGO
ADD  D0,A0
SUBQ #1,D1
MOVE.L  A0,-(SP)
MOVE.L  A2,-(SP)
MOVE  #1,-(SP)   n
MOVE  D1,-(SP)   k
```

(10)

Calcule $\mathcal{P}' = \mathcal{P}_{\mathcal{P}_{A_1}} \cdot u_r$

```
MJ34:ADD.L  (A1)+,A2
MJ36:SUBQ   #1,D5
     BNE    MJ34
```

```
     MOVE.L  (A1)+,D0        P_A0 = u_r
     PEA     4(A0,D0.L)      P_A2 = u_{r+1}
                             [A3] = p
     BSR     XMPMUL          nouveau P' = u_1 ... u_r
     MOVE.L  (SP)+,A0        u_{r+1}
     MOVEM.L A2/A6,-(SP)
     MOVE.L  A2,A4           P'
     BSR     XMPINV          pose a : a u_{r+1} ≡ 1 (mod P')
     MOVE.L  A6,-(SP)        Construction de V'
     MOVEM.L -8(SP),D4/D5/D6/A2/A3/A5
                             a r x U P V
     MOVE.L  D4,A0           a
     ADDQ    #1,(A5)
     MOVE.L  (A5)+,(A6)+     place pour δ
MJ38 :ADDQ   #4,A6           Ser-i
     SUBQ    #1,D5           Boucle i = 1 à r
     BMI     MJ40            fin
     MOVE.L  (A5)+,D0
     MOVE.L  A5,A1           v_i
     ADD.L   D0,A5           [δv_{i+1}]
     MOVE.L  (A2)+,D0
     MOVE.L  A2,D4           u_i
     ADD.L   D0,A2           [δu_{i+1}]
     SUBQ    #1,D5
     BMI     MJ40
```




```
     MOVEM.L D4/D5/A0/A2/A3/A5/A6,-(SP)
             u_i r-i a  U_S P  V_S
     BSR     XMPMUL          } av_i mod p
     MOVE.L  A2,A0           }
     MOVE.L  (SP)+,A1        u_i
     BSR     XMPMOD          av_i mod u_i, mod p
     MOVE.L  20(SP),A0
     BSR     XLB76
     MOVEM.L (SP)+,D5/A0/A2/A3/A5
             r-1 a  U_S P  V_S
```

(10)

```
        MOVE.L  (SP)+,A1
        MOVE#1,(A6)+        (exposant fidèle)
        MOVE.L  A6,D0
        SUB.L   A1,D0
        MOVE.L  D0,-(A1)    δ
        BRA     MJ38

MJ40:   MOVE.L  D4,A1       u_{r+1}
                            P_{A0}=a

        MOVE.L  A6,-(SP)
        BSR     XMPMUL      au_{r+1} mod p
        MOVE.L  A2,A1
        LEA     TCONSTU,A0  1
        BSR     XMPSUB      1-au_{r+1} mod p
        MOVE.L  A2,A0
        MOVE.L  8(SP),A1    P
        BSR     XMPDIV      a3 a2 a6 | 0 | 9 |
repète  MOVE.L  (SP),A0     <- TST.L (A3)+   ⊗
début   BSR     XLB76          BNE   ERRDIV
pour    MOVE.L  (SP)+,A1       CMP #$4000,(A3)
        MOVE    #1,(A6)+       BNE   ERRDIV
        MOVE.L  A6,D0          exposant
        SUB.L   A1,D0
        MOVE.L  D0,-(A1)    δ
        MOVE.L  (SP)+,A2    V'
        MOVE.L  24(SP),A0   axis
        BSR     XLB76
        MOVEM.L (SP)+,A2/A6
                            P'
        MOVEM.L (SP)+,D5/D6
        ADDQ    #1,D5       r+1
        MOVEM.L D5/A0,-(SP) nouveau P'
        BSR     XLB76       copie P'
        BRA     MJ32
```

```
                    V' P' X
MOVEM.L (SP)+, D6/A0/A1
BSR     XPSAP           recopie P'
MOVE.L  A6,A5
MOVE.L  A2,A6           ]V'
MOVE.L  D6,A2
MOVE.L  16(SP),A0       orig
BSR     XLB76           copie V'
MOVEM.L (SP)+, D5/D6
                        R  X
ADDQ    #1,D5
MOVEM.L D5/A0,-(SP)
MOVE.L  A5,A6
BSR     XLB76           copie P'
BRA     MJ32
```