(10) Entrée $A = \mathcal{P}_{A_0} = u(x)$ unitaire

$p = [A_3]$

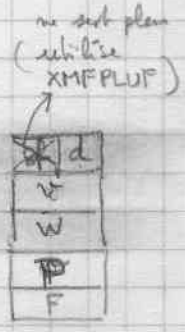
Pose en libre la forme factorisée de A mod p

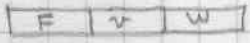
(Knuth p429)

⊗ { XMFPLU : ST XMFPLUF { -1 facteur multiple ; 0 pas de facteur multiple
{ XMFPLUF : MOVE (A0), D0 nb de bit

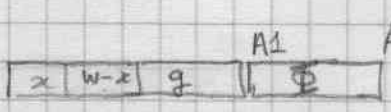
```
        BEQ   XPSAF          → met aussi A2 = P_A0
        MOVEM.L A0/A3/A6,-(SP)
        ADDQ  #8,A0
        MOVE  #1,(A6)+
        BSR   XMPOSE         F = norm(A)^F mod p
        MOVE.L (SP)+,A0
        BSR   XMPNOR         pose v(x) = A normalisé (poly)
        MOVEM.L A2/A6,-(SP)
        MOVE.L (A2),D2       x
        BSR   LB17           w(x) = x (poly)
⊗ { CLR.L -(SP)              d = 0
  { ~~ST -(SP)~~             sf ≠ 0 (ne sert plus)
MJ24 : MOVEM.L (SP),D5/A0    d  v
        TST.L (A0)+
        BEQ   MJ26           → deg(v) < 2(d+1)
        MOVE.L (A0),D0       D0.W = deg(v)
        ADDQ  #1,D5
        MOVE.L D5,(SP)       d+1
        ADD   D5,D5
        CMP   D5,D0
        BCC   MJ28           → deg(v) ≥ 2(d+1)
MJ26 : MOVEM.L (SP)+,D0/A0   v
        BSR   XPSAF          factorise v
        MOVE.L A2,A1
        ADDQ  #8,SP
        MOVE.L (SP),A0
        BSR   XCONCP         F = F * v^F
        BRA   KL860
```

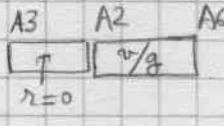
× fin

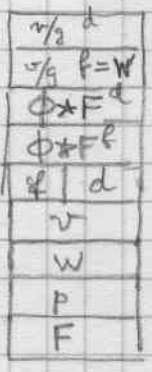




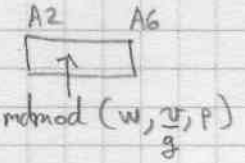
```
                                        v  W  P
MJ28: MOVEM.L (SP), D0/D1/A0/A1          remplace W par W mod v
                                                       P  P
      MOVE.L  D1, A4   v
      MOVE.L  A1, A3   P
      BSR     XMPEXP
      MOVE.L  8(SP), A0
      BSR     XLB76
                                        x  v  W  P
MJ30: MOVEM.L (SP), D0/A0/A1/A3          calcule g = mdpgcd(v, W-x, P)
      MOVE.L  (A0), D2     x
      MOVE.L  A1, A0       W
      MOVE.L  A6, A1       x
      BSR     LB17         red x
      BSR     XMPSUB                    W-x
      MOVEM.L (SP), D0/A0/A1/A3
                            v  x  P
      MOVE.L  A2, A1                    W-x
      BSR     XMPGCD                    pose g
      TST.L   (A2)
      BEQ     MJ24                      → g = Cte (=1)
      MOVE.L  A2, A0   ← MOVE.L A2, -(SP)
      BSR     XPSAF                     Φ = g^F   produit sans carrés de
      MOVE.L  A2, A0                            facteurs irred de degré d
      MOVEM.L (SP), D0/D5/A1/A2/A3
                      d  x  x  P
      BSR     XMFMD                     factorise les facteurs de
                                        degré > d
      MOVE.L  20(SP), A0   (F)
      BSR     XCONCP       F*Φ
      MOVE.L  (SP)+, A1    g
      MOVEM.L A2/A6, -(SP)
      MOVEM.L 12(SP), A0/A2/A3
                      v  x  P
      BSR     XMPDIV
      MOVEM.L A2/A6, -(SP)
```







```
                                  w  ~~w~~  p
MOVEM.L  2~~4~~(SP), A0~~/A5~~/A3
~~EXG  A0,A1~~ MOVE.L A2,A1
BSR   XMPMOD
```




```
MOVE.L  A6,A5        fin w'
MOVEM.L  8(SP),A2/A6        ΦxF
MOVE.L  32(SP),A0
BSR   XLB76          copie ΦxF
MOVEM.L  (SP)+,A2/A6        } v/g
ADDQ  #8,SP
MOVE.L  A0,4(SP)
BSR   XLB76          copie v/g
MOVE.L  A0,8(SP)
MOVE.L  A5,A6        } w
BSR   XLB76          copie w
```

⊗ ~~TST (SP)~~ TST.B XMFPLUF } → cas facteurs multiples possibles
BNE MJ30
BRA MJ24 → cas u(x) entrée sans facteurs répétés