(10) entrée : $P_{A0}$ = g polynome produit de facteurs irréductibles, de degré d = D5 (dans corps)

d = D5
p = [A3]

conserve { A0/A3 / D5

sort : pose en libre $var_{A2}$ = forme factorisée (mais pas nécessairement de façon complète)

```
MJ12 :MOVEM.L (SP)+,D5/A0/A3/A6
XMFMD1:MOVE.L (A0),D0          D0.W = (x) litteral.
       MOVEM.L D5/A0/A3/A6,-(SP)
       MOVE  D5,D1
       SUBQ  #1,D1
       MOVE  D1,(SP)           k = 2d-1
       ADD   D5,D1
       BSR   XMPRND            met le polynome aléatoire
                               t(x) = Σ_{i=0}^{k} rnd(p) x^i
       TST.L (A2)
       BEQ   MJ12        →     t(x) = cte : recommencer
MJ14 : SUBQ  #1,(SP)           Calcul de T(t) ≡ t + t^p + .. + t^{p^{d-1}}  mod p
X      BMI   MJ18              mod g
       MOVE.L A2,A0      t     cas p=2 ↗
       MOVE.L 4(SP),A4   g     calcule t^p
       MOVE.L 8(SP),A3   p
       MOVE.L A3,A1
       BSR   XMPEXP
       MOVE.L A2,A0      t^p
       MOVE.L 12(SP),A1  t
       MOVE.L 8(SP),A3   p
       BSR   XMPADD            t^p + t
       MOVE.L 12(SP),A0
       BSR   XLB76
       BRA   MJ14
```

{ MOVE.L 8(SP),A0 p ; CMP #$4002,(A0) ; BNE MJ16 → p ≠ 2

{ MOVEM.L (SP),D5/A0/A3/A4 (g, p, t) ; EXG A0,A4 (t, g)

| k | d |
|---|---|
| g | |
| p | |
| t | |

MJ16 : ici en libre a a $T_{A2} = t + \dots + t^{p^{d-1}}$ où t est aléatoire

```
MJ16 :MOVE.L (SP),D1        d = D1.W          Calcule
      BSR  XEXPD2           pose [A2] = p^d   t^((p^d-1)/2)
      MOVE.L A2,A0
      MOVEQ #-1,D2
      BSR  XROT             (p^d-1)/2
      MOVEM.L (SP),D0/D1/A0/A3
                              g   p   t
      EXG  A0,A3
           t   p
      MOVE.L A2,A1          (p^d-1)/2
      MOVE.L D1,A4          g
      BSR  XMPEXP           t^((p^d-1)/2)
      MOVE.L A2,A0
      MOVE.L 8(SP),A3       p
      LEA  TCONSTU,A1       (1)
      BSR  XMPSUB           t^((p^d-1)/2) - 1
      MOVE.L 12(SP),A0
      BSR  XLB76
```

MJ18

```
MJ18: MOVEM.L (SP), ~~D0~~/A0/A3/A4
      MOVE.L  A4, A1
      BSR     XMFPAR          Q = mod pgcd(g, T, p)
      BEQ     MJ12            → Q=1 changer t
      CMP     #1,(A3)
      BEQ     MJ12            → A/Q = 1 : changer t
      MOVE.L  A3, A0
      MOVE.L  A5, A1
      BSR     XCONCP          g/Q * Q
      MOVE.L  12(SP), A0
      BSR     XLB76
      MOVEM.L (SP)+, D5/A0/A3/A4
      MOVE.L  A4, A2
      RTS
```