(10) entrée $a = [A0]$ sortie pour a libre $[A2] = a^n \bmod p \in [0, p-1]$

$n = [A1]$

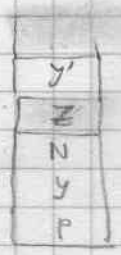
$p = |[A3]|$ $p > 1$

```
XMEXP:MOVE.L   A3,-(SP)
      MOVE.L   A6,-(SP)
      MOVE     #$4001,(A6)+        Y=1
      MOVEM.L  A0/A6,-(SP)
      MOVE.L   A1,A0
      BSR      XPOSE               N = |n|
      BCLR     #7,(A2)             MOVE.L (SP)+,A0   a
      BEQ      MI26                MOVE.L 8(SP),A3   ⊗
      cas      n<0      : pose Z = a^-1
      MOVE.L   8(SP),A1            p
      BSR      XMINVS
      BRA      MI27
MI26: BSR      XMPOSE              cas n>0 pose a mod p
MI27: MOVE.L   A2,-(SP)
MI28: MOVE.L   4(SP),A0            N = 0 ?
      CMP      #$4000,(A0)
      BNE      MI29                → non
      ADDQ     #8,SP               ↓ oui réponse = Y
      MOVE.L   A0,A6
      BRA      MI20
MI29: MOVE.L   (SP),A0             Z
```

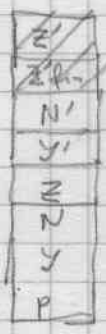
CMP #$4000,(A1) si n=0 met 1
BEQ MI20

Z
N
Y
P

```
                                    Z N Y P
MI28: MOVEM.L (SP), A0/A1/A2/A3
      CMP  #$4000,(A1)
      BNE  MI29          → N≠0
      ADD  #16,SP          ↓ où réponse = Y
      MOVE.L A1,A6         N=0
      TS
      BTST #0,-1(A0)                    N pair ?
      BNE  MI30          → N impair
                         ↓ N pair : recopie Y en libre
      MOVE.L A2,A0
      BSR  XPOSE  ← MOVE.L 12(SP),A3
      BRA  MI31
MI30: MOVE.L A2,A1          N impair pose Y*Z mod p
      BSR  XMMUL
MI31: MOVE.L A2,-(SP)       y'
      MOVE.L 8(SP),A0       N
      MOVEQ #-1,D2
      BSR  XROT             pose N/2 = N'   conserve A3
      CMP  #$4000,(A2)
      BNE  MI32
cas N'=0   la réponse est y'
MI315: MOVE.L A2,A6
      MOVE.L (SP)+,A2       y'
      ADDQ #8,SP
      BRA  MI19
MI32: MOVE.L A2,-(SP)
      MOVE.L 8(SP),A0       Z = [A0] = [A1]
      MOVE.L A0,A1          (A3 = p)
      BSR  XMMUL            pose Z² mod p = Z'
      MOVEM.L A2/A6,-(SP)
      MOVE.L A2,A1          Z'
      MOVE.L A6,A4          Z'fin
```




```
      MOVE #$4000,D0
      CMP  (A2),D0
      BEQ  MI315    → N'=0 réponse y'
      MOVE.L 4(SP),A0   (Z)
      CMP  #$4000,(A0),D0
      BNE  MI32     → continue
      MOVE.L (SP)+,A2   ↓ Z=0 réponse
      MOVE D0,(A2)+     (0)
```



```
                  N'  y'                        fin y'
MOVEM.L   8(SP),A2/A6          MOVE.L  (SP)+,A6
      y'  fin y'               MOVE.L  (SP)+,A2   y'
EXG       A2,A6                ADDQ    #8,SP
MOVE.L    8(SP),A0             MOVE.L  (SP),A0
BSR       XLB76                copie y'
MOVE.L    A6,-(SP)             nouveau N
MOVE.L    A1,A6                fin de N'
BSR       XLB76                copie N'
MOVE.L    A6,-(SP)
MOVE.L    A4,A6
ADDQ      #8,SP
BSR       XLB76                copie Z'
BRA       MI28
```