(10) exp mod p mod v(x) entrée $P_{A0}=x$ poly à 1 ll/ord

$n=[A1]$ ~~de~~ de signe 99

$[A3]=p$

$P_{A4}=v$

repete XMEXP Pose $P_{A2}=(P_{A0})^{n}$ mod p mod v(x) en libre

XMPEXP:

```
        BSR   XPSP1          pose 1 = y
        CMP   #$4000,(A1)    n=0 ?
x       BEQ   MI74           oui → rts

        MOVEM.L A2/A3/A4,-(SP)
        MOVE.L  A6,-(SP)
        EXG     A0,A1
        BSR     XPOSE
        MOVE.L  A1,A0
        MOVEM.L 8(SP),A3/A4
MI700:  BSR     XMPMOD1      pose ~~z~~ ≡ x mod p mod v
MI701:  MOVE.L  A2,-(SP)
MI70:   MOVEM.L (SP),A0/A1/A2/A3/A4
        BTST    #0,-1(A0)
        BNE     MI71         → N impair
                             ↓ N pair recopie y
        MOVE.L  A2,A0
        BSR     XPSAP        conserve A0/A1/A3/A4
        BRA     MI72
MI71:   MOVE.L  A2,A1        N impair pose y*z mod p mod v(x)
        BSR     XMMMUL       conserve A3/A4
MI72:   MOVE.L  A2,-(SP)     y'
        MOVE.L  8(SP),A0     N
        MOVEQ   #-1,D2
        BSR     XROT         pose N'=N/2  conserve A3/A4
```

z
N
y
p
v(x)

```
        BCLR  #7,(A2)
        BEQ   MI700          cas n<0 pose x^-1
        BSR   XMPINV
        BRA   MI701
```

N=n

```
        CMP  #$4000,(A2)
        BNE  MI75
        Cas N'=0   la réponse est y'
        MOVE.L  A2,A6
        MOVE.L  (SP)+,A2
        ADDQ  #8,SP
        MOVE.L  (SP),A0
        BSR  XLB76
        MOVEM.L  (SP)+,A2/A3/A4
MI74:   RTS
MI75:   MOVE.L  A2,-(SP)
        MOVE.L  8(SP),A0        Z
        MOVE.L  A0,A1
        BSR  XMMMUL             pose Z²  mod p=[A3]
                                         mod v=ℬA4
        MOVE.L  A2,A1           Z'
        MOVE.L  A6,A4           Z'fin
        MOVE.L  (SP)+,A6        fin y'
        MOVE.L  (SP)+,A2        y'
        ADDQ  #8,SP
        MOVE.L  (SP),A0
        BSR  XLB76              copie y'
        MOVE.L  A6,-(SP)
        MOVE.L  A1,A6           fin de N'
        BSR  XLB76              copie N'
        MOVE.L  A6,-(SP)
        MOVE.L  A4,A6
        BSR  XLB76              copie Z'
        BRA  MI70
```