(10) entrée 10(SP) R.N
12(SP) q
16(SP) n
20(SP) n-1
[A0] = x >1 $x \in]1, n[$

$n = 1 + 2^k q$

Retour normal si n premier
en MI41 si n non premier

```
XMPT3: MOVEM.L 12(SP),A1/A3        (q, n)
       BSR   XMEXP                 y = x^q mod n
       MOVE.L A2,-(SP)
       CLR.L -(SP)
       MOVEQ #0,D0
       MOVEM.L D0/A2,-(SP)
       CMP   #$4001,(A2)           si x^q = 1  n premier
       BNE   MI50
MI49:  MOVEM.L (SP)+,D0/A6
       RTS
MI50:  MOVE.L 4(SP),A0             y
       MOVE.L A0,-(SP)             y
       MOVE.L 28(SP),A1            n-1
       BSR   XCMP1
       BEQ   MI49                  -> y = n-1  n premier sans doute
       MOVE.L (SP)+,D0
       MOVE.L (SP),A0
       CMP   #$4001,(A0)
       BEQ   MI52                  -> non premier
       ADDQ  #1,D0
       CMP   16(SP),D0             (*)
       BCC   MI52
       MOVE.L D0,-(SP)
       MOVE.L A0,A1
       BSR   XMMUL                 y^2
       MOVE.L 4(SP),A0
       BSR   XLB76                 remplace y
       BRA   MI50
MI52:  ADD   #24,SP
       MOVE.L (SP)+,A6
       BRA   MI41
```