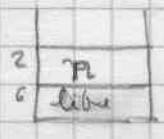
(10) Teste si $n = 1 + 2^k q$ est premier [A0] $n > 1$

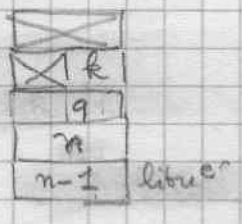
EQ n probablement premier
NE n non premier

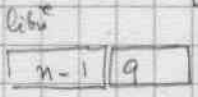
```
XMPT1: BSR   SLNH0
       BTST  #0,-1(A0,D0.W)
       BNE   XMPT2
MI41:  MOVEQ #1,D0
MI42:  RTS

XMPT2: MOVEM.L A0/A6,-(SP)
       LEA   TCONST1,A1
       BSR   XSUB1          A2 = 2^k q
       MOVE.L A2,A0         détermine k = D2
       BSR   SLNH0          MOVE.L A6,A2 ⊗
       ADD   D0,A2
       MOVEQ #0,D2
MI43:  MOVE.B -(A2),D0
       BNE   MI45
       ADDQ  #8,D2
       BRA   MI43
MI44:  ADDQ  #1,D2
MI45:  ROR.B #1,D0
       BCC   MI44
       [illegible]
       NEG   D2
       BSR   XROT           calcule q
       LEA   TCONST2,A0
       BSR   XMPT3
```

← MOVEM.L D0/D2/A6,-(SP) (9) (k)







(10)

```
LEA   TCONST3,A0
BSR   XMPT3
LEA   TCONST8,A0
BSR   XMPT3
ADDQ  #4,SP
MOVE.L 8(SP),A0        n
LEA   TCONSE8,A1
BSR   XCMP1
BCC   MI46             n>10^8
LEA   TCONST0,A3       cas recherche complète
ADDQ  #8,SP
MOVE.L (SP)+,A0/A6
BSR   XPF3
MOVE.L A2,A6
TST   4(A6)
BRA   MI42             ⊗
MI46:MOVE  #24,(SP)    recherche probabiliste 25 fois
     MOVE.L A6,-(SP)
MI48:MOVE.L (SP),A6
MI4:MOVE.L 12(SP),A0
     BSR   XRND
     MOVE  (A2),D0
     SUB   #$4000,D0
     CMP   #7,D0
     BCS   MI48
     MOVE.L A2,A0
     BSR   XMPT3
     SUBQ  #1,4(SP)
     BNE   MI48
     ADD   #16,SP
     MOVE.L (SP)+,A6
     MOVEQ #0,D0
     RTS
```