

10

entrée $[A0]$ = entier > 1

pose en $A2$ _{libre} un nombre aléatoire $\in [0, [A0]^e[$

XRND: BSR XBNS $D1.L = nb$ de bits de $[A0]$

ASR.L #4, D1 nb de mots

ADDQ #1, D1 ← MOVE D1, D3

ADD D1, D1 ← ADDQ #1, D1

MOVE.L A0/A6, -(SP)

MOVE D1, (A6)+ ← { ADD D1, A6
BSR VERAG
SUB D1, A6

MI36: MOVE #17, -(SP)

TRAP #14

ADDQ #2, SP

MOVE D0, (A6)+

DECR D3, MI36

MOVE.L (SP)+, A3

MOVE.L (SP), A0

BSR XMPOSE

BRA KL860

BSR MOORE ⊗

4811
4830
13800

(MI36) al.c.s