(10) entrée [A0] = u, |[A1]| = p $u \neq 0$ $p \neq 0$

met en libre [A2] = v tel que $uv \equiv 1 \pmod{p}$

il faut pgcd(u,p) = 1 sinon : a) XMINVS → erreur

→ $v \in [1, |p|[$ b) XMINVS1 → met 0

XMINVS : BSR XMINVSA pour divers prgr

BNE ERRDV

(SP) XMINVSB : TST (A2) met |p|−|v| si v<0

BPL MI17 → rts

MOVE.L A2,A1

MOVE.L A2,-(SP)

BSR XSUB1

BRA KL860

(SP) XMINVSA : MOVE.L A1,-(SP)

TST (A0)

BPL MI14 → u>0

BSR XMINV ↓ <0

BCHG #7,(A2)

BRA MI16

MI14 : BSR XMINV

MI16 : MOVE.L (SP)+,A0

CMP #$4001, (A6) pgcd = 1 ?

MI17 : RTS

XMINVS1 : BSR XMINVSA pour prinv

BNE XMINVSB → pgcd = 1

↓ non

MOVE.L A2,A6

BRA MIS20 → met $[a^2]_5 = 0$