⑤ prinv(a, p)

a } entiers exacts $\neq 0$
p } $|p| \neq 1$

met b : $ab \equiv \text{pgcd}(|a|, |p|)$
$b \in [1, |p|[$

(si p est premier $b \equiv a^{-1} \bmod p$)

```
YPRINV: BSR   WENTIER        a = {A0}
        CMP   #$4000,(A0)    ⊗
        BEQ   ERRNIN         erreur inverse
        BSR   DECCRVE        > on err
        BNE   ERRIS
        BSR   MB230          a = {A0}
        CMP   #$4000,(A1)    p = {A1}
        BEQ   ERRNIN         ⊗ ⊗ BSR WENTIERP  décode |p| ≠ 0,1
        BCLR  #7,(A1)        ⊗ ⊗ BSR MB231
        CMP   #$4001,(A1)    ⊗ ⊗ LEA XMINVS,A2
        BEQ   ERRNIN         ⊗ ⊗ BRA MI34
                             ⊗ ⊗ MI34
        MOVE.L A5,-(SP)      (copie YPRCDR)
        ADDQ  #6,A6          mov.l a6,-(sp)
        MOVE  PRIOR,(A6)+
        BNE   MI18
        CLR.L (A6)+
MI18:   BSR   XMINVS
        MOVEM.L (SP)+,A2/A5
        BRA   POPNEW         b remplace P-1 (a), P0 (p)
```

(5) ~~ex~~ exécute le prg (A2) qui met un nombre P/q
et remplace p_0 et p_{-1} par ce nombre
caserne A5

```
MI34: MOVE.L   A5,-(SP)
      ADDQ #6, A6
      MOVE.L   A6,-(SP)
      MOVE     PRIOR,(A6)+
      BNE      MI35
      CLR.L    (A6)+
MI35: JSR      (A2)          met {p/q} ~~ext~~ libre
      MOVEM.L  (SP)+, A2/A5
      BRA      POPNEW        remplace p-1, p0 } par nouveau p/q
```