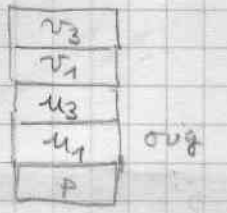
(10) inverse de $a = P_{A0}$ mod $p = [A3]$
mod $v(x) = [A4]$

pose $b = P_{A2}$ et libre tel que $ab \equiv 1$ mod p
mod $v(x)$
$\deg(b) < \deg(v)$

[Algorithme d'Euclide étendu Knuth p325]

repete XMINV

```
XMPINV: MOVE.L  A3,-(SP)
        MOVE.L  A6,-(SP)        u1 = 1
        BSR     XPSP1
        MOVE.L  A4/A6,-(SP)     } u3 ≡ a mod p
        BSR     XMPPM
        MOVE.L  (SP)+,A0
        MOVE.L  A6,-(SP)        } v1 = 0
        BSR     XPSP0
        MOVE.L  A6,-(SP)        } v3 ≡ v(x) mod p
        BSR     XMPPM
MI90:   MOVE.L  (SP),A1         v3
        TST.L   (A1)            v3 = 0 ?
        BNE     MI92
        CMP     #$4000,4(A1)
        BNE     MI92            → non
fin     ADDQ    #8,SP
        MOVE.L  (SP)+,A6
        MOVEM.L (SP)+,A2/A3
```



u1 p

vérif que le pgcd $(a, v(x)) =$ cte $\neq 0$

```
        TST.L   (A6)
        BNE     ERRDV           → pgcd non
        CMP     #$4000,4(A6)
        BEQ     ERRDV           → pgcd = 0
        RTS
```

fin

```
ADDQ  #4,SP
MOVE.L (SP)+,A6
MOVE.L (SP)+,A0          u3
TST.L  (A0)+
BNE    ERRDV             u3 ≠ cte
MOVE.L 4(SP),A1          P
BSR    XMINVS            u3^-1
MOVEM.L (SP),A0/A3       u1  P
MOVE.L A2,A1             u3^-1
BRA    MI690             met  u1 u3^-1
```

```
MI92: MOVEM.L  8(SP), A0/A2/A3      u3  x  p
      BSR      XMPDIV
      MOVE.L   A3,-(SP)    r = t3
      MOVE.L   A2,A0       q
      MOVE.L   8(SP),A1    v1
      MOVE.L   20(SP),A3   p
      BSR      XMPMUL      qv1   conserve A3
      MOVE.L   A2,A1
      MOVE.L   16(SP),A0   u1
      BSR      XMPSUB      t1 = u1 - qv1   conserve A3
      MOVE.L   (SP),A0     t3
      MOVE.L   A2,-(SP)
      BSR      XPSAP       recopie t3 = r
      MOVEM.L  A2/A6,-(SP)
      MOVEM.L  16(SP), A0/A2/A3/A6
                           v3 v1 u3 u1

      EXG      A0,A6
      BSR      XLB76       copie nouveau u1 (ou v1)
      MOVE.L   A6,24(SP)
      MOVE.L   12(SP),A6   fin de v3
      BSR      XLB76       copie nouveau u3
      MOVE.L   A6,20(SP)   nouveau v1
      MOVE.L   (SP)+,A6    t3 = fin t1
      MOVE.L   (SP)+,A1    fin t3
      MOVE.L   (SP)+,A2    t1
      BSR      XLB76       copie nouveau v1 = t1
      ADDQ     #8,SP
      MOVE.L   A6,-(SP)    nouveau v3
      MOVE.L   A1,A6       fin t3
      BSR      XLB76       copie nouveau v3
      BRA      MI90
```