(10) pgcd mod p — entrée $\mathcal{P}_{A_0}$, $\mathcal{P}_{A_1}$, $[A3]=p$ } à 1 ~~littéral~~ x

Pose en libre $\mathcal{P}_{A_2} = \text{pgcd}(\mathcal{P}_{A_0}, \mathcal{P}_{A_1})$ (normalisé)

```
XMPGCD1 :MOVE.L  A4, A1
XMPGCD :MOVEM.L  A1/A6,-(SP)
        BSR   XMPNOR          a = λ P_A0  mod p, a normé
        MOVE.L  (SP)+, A0
        BSR   XMPNOR          b = λ P_A1  mod p, b normé

MI78 :MOVE.L  A2,A0           } ici  [A3] = p
        BSR   XMPDEG
        TST.L  D5
        BPL   MI81
        cas b=0 : renvoie a
        MOVE.L  A2, A6
        MOVE.L  (SP)+, A2
        RTS

MI81 : BNE   MI82
        cas b = cte : renvoie 1
        MOVE.L (SP)+, A6
        BRA   XPSP1

MI82 :MOVE.L  (SP), A0
        MOVE.L  A2, A1
        MOVE.L  A2, -(SP)
        BSR   XMPMOD          pose a' ≡ a mod b   deg(a) < deg(b)
        MOVE.L  A2, A0
        MOVE.L  A2, -(SP)
        BSR   XMP NOR         normalise a' : a'' ≡ λ a'
        MOVE.L  A6, A5        ] a''
        MOVE.L  A2, A4
        MOVE.L  (SP)+, A6     fin b
        MOVE.L  (SP)+, A2     debut de b
        MOVE.L  (SP), A0      a
        BSR   XLB76           b remplace a
        EXG   A5, A6
        MOVE.L  A4, A2
        BSR   XLB76
        MOVE.L  A5, A2
        BRA   MI78
```