

10) pgcd mod p

entrée P_{A0}
 P_{A1} } à 1 littéral x
 $[A3]_{\text{FP}}$

Pose en libre $P_{A2} = \text{pgcd}(P_{A0}, P_{A1})$ (normalisé)

```
XMPGCD1: MOVE.L A4, A1
XMPGCD: MOVEM.L A1/A6, -(SP)
```

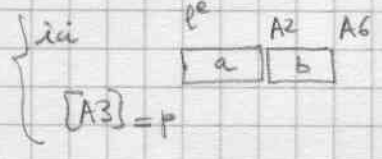
```
BSR XMPNOR
MOVE.L (SP)+, A0
BSR XMPNOR
```

$a \equiv \lambda P_{A0} \pmod p$
 a non nul



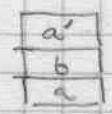
$b = \lambda' P_{A1} \pmod p$
 b normalisé

```
MI78: MOVE.L A2, A0
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=0 : renvoie 1
MOVE.L (SP)+, A6
BRA XPSP1
```

```
MI82: MOVE.L (SP), A0
MOVE.L A2, A1
MOVE.L A2, -(SP)
```



```
BSR XMPMOD
MOVE.L A2, A0
MOVE.L A2, -(SP)
BSR XMPNOR
```

par $a' \equiv a \pmod b$
 $\text{deg}(a) < \text{deg}(b)$

```
MOVE.L A6, A5
MOVE.L A2, A4
```

normalise a' : $a'' = \lambda a'$

```
MOVE.L (SP)+, A6
MOVE.L (SP)+, A2
MOVE.L (SP), A0
```

fin b
 debut de b
 a
 b remplace a

```
BSR XLB76
EXG A5, A6
MOVE.L A4, A2
BSR XLB76
MOVE.L A5, A2
BRA MI78
```