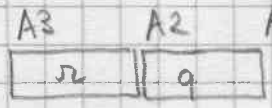
division mod p

entrée $P_{A_0} = a$ } à 1 littéral
$P_{A_1} = b$
$[A3] = p$

$b = \lambda b'$ normé
$a = q\lambda^{-1} b$
b'
$a \equiv qb + r \pmod p$

ret a libre




```
XMPDIV:MOVEM.L  A1/A3,-(SP)
       BSR      XMPDIV1

       MOVE.L   (SP)+,A0      b
       MOVEM.L  A1/A2/A3/A6,-(SP)
       MOVE     (A0)+,D0
       ADD      D0,D0         } 4 ou 0
       ADD      D0,D0         }
       ADDQ     #2,D0           6 ou 2
       ADD      D0,A0         pointe le 1er coef de b = [λ]
       MOVE.L   16(SP),A1     p
       BSR      XMINVS        λ^-1
       MOVE.L   8(SP),A0/A1/A3
                r    p
       BSR      XMPPM         r' ≡ r (mod p)
       MOVEM.L  (SP)+,D0/A0
                b'  q
       ADDQ     #4,SP
       MOVE.L   (SP)+,A1/A3
                (λ^-1)  p
       MOVEM.L  D0/A2',-(SP)
       BSR      XMPCMULS      q' ≡ λ^-1 q (mod p)
       MOVE.L   (SP)+,A0      b'
       MOVE.L   A6,A5         fin q'
       MOVE.L   A2,A6         fin r'
       MOVE.L   (SP)+,A2      r'
       MOVE.L   A0,A3         r'
       BSR      XLB76
       EXG      A5,A6         fin q'
       BSR      XLB76
       MOVE.L   A5,A2
       RTS
```