(b) entrée $[A0] = a \in [0, p-1[$ ($a \geq 0$)
$[A1] = b \in [0, p-1[$ ($a \geq 0$)
$[A3] = p$
pour en lieu $ab \bmod p \in [0, p-1[$ conserve A3

```
XMMUL:MOVE.L  A3,-(SP)
      BSR     XMUL1          pour [A0]*[A1]
      MOVE.L  (SP),A3
      MOVE.L  A2,A0
      MOVE.L  A0,-(SP)
      BSR     XMPOSE         pour ab mod p
      BRA     MI19
```