

(10)

6a

(après XMMUL)

entrée $[A0] = a$
 $[A1] = b$
 $[A3] = p$ } signes qq

pose en libra $ab \text{ mod } p \in [0, p-1[$ conserve A3

```

XMMULS: MOVE (A0), D0  MOVE (A1), D1
        EOR D1 D0, D0
        MOVE D0, -(SP)
        BSR  XMMUL
        MOVE (SP)+, D0
        BMI  XMCHG
        RTS

```