(10) Entrée $[A_0] = a \in [0, p[$

$[A_1] = b \in [0, p[$

$|[A_3]| = p$

sort en libre $[A_2] = a - b \bmod p \in [0, p[$ congrue A_3

```
XMSUB:MOVE.L  A3,-(SP)
      BSR     XSUBS1        a-b
      TST     (A2)
      BPL     MI21          a-b ≥ 0
      MOVE.L  (SP),A0       p
      MOVE.L  A2,A1         a-b
      MOVE.L  A2,-(SP)
      BRA     MI24
```

```
XMSUB:MOVEM.L  A0/A3,-(SP)
      BSR      XCMP1
      MOVEM.L  (SP)+,A0/A1
      BCC      MI25          → a ≥ b
      MOVE.L   A1,-(SP)
      MOVE.L   A1,-(SP)
      MOVE.L   4(SP),A1
      BSR      XADDM         p+a
      MOVE.L   A2,A0
      MOVE.L   (SP)+,A1
      MOVE.L   A2,-(SP)
      BRA      MI24
MI25: BSR      XSUB1
      BRA      MI21
```