(5)

mdpwr (A(x), n, v(x), p)

A(x), v(x) } poly à 1 Id

$n \geq 0$

$|p| \neq 0, 1$

met $W \equiv A(x)^n \mod p \mod v(x)$

$\deg(W) < \deg v(x)$

```
YMDPWR: BSR   WPOLYU      décode A(x)
        BSR   DECCRVE     (5)
        BSR   WENTIER     (n)
        MOVE  TVARN,D0    } échange p0 et p-1
        MOVE  D0,D2       }
        SUBQ  #1,D2       }
        BSR   MG79        }
        BSR   WCALMD      décode v, p      [A3] = p
                                           PA4 = v(x)
                                           PA0 = A(x)
        MOVE.L A0,A1
        MOVE  D4,D0
        SUBQ  #1,D0
        BSR   XHREEL      met [A0] = n     Conserve A1/A3/A4
        EXG   A0,A1
        LEA   XMPEXP,A2
        BSR   MI84
        BRA   POPPR
```