(5) rdpwre ~~rfpwr~~ (a, b, p) met $a^b \bmod |p|$

(a, b entiers qq ; si $b<0$ il faut que pgcd(a,p)=1)
$p \neq 0, \pm 1$

```
MP  E
YEERPWR: BSR    WENTIER          a
         BSR    DECCRVE          (9) ou erreur

         BSR    WENTIER          b
         BSR    DECCRVE          (9) ou erreur

         BSR    WENTIER.P        |p| ≠ 0,1
         MOVE.L A0,-(SP)
         MOVE   TVARN,D0
         SUBQ   #2,D0
         BSR    XHREEL           [A0] = a

         BSR    MB231            P-2        P-1
         EXG    A0,A1            [A0] = a   [A1] = b
         MOVE.L (SP)+,A3         [A3] = P/P0
         LEA    XMEXP,A2         } a^b mod p remplace P0
         BSR    MI34             }                    P-1
         BRA    POPPR            ôte P-1
```