

(10) exp mod p mod v(x)

entree $P_{A_0} = x$ poly à 1 littéral

$n = [A1]$ de signe ?

$[A3] = p$

$P_{A_4} = v$

en libe

répète XMEXP

pose $P_{A_0} = (P_{A_0})^n \pmod{p}$
 $\pmod{v(x)}$

XMPEXP:

BSR XPSPI

CMP # \$4000, (A1)

BEQ MI74

MOVEM.L A2/A3/A4, -(SP)

MOVE.L A6, -(SP)

EXG A0, A1

BSR XPOSE

MOVE.L A1, A0

MOVEM.L 8(SP), A3/A4

MI700: BSR XMPMOD1

MI701: MOVE.L A2, -(SP)

MI70: MOVEM.L (SP), A0/A1/A2/A3/A4

BTST #0, -1(A0)

BNE MI71

MOVE.L A2, A0

BSR XPSAP

BRA MI72

MI71: MOVE.L A2, A1

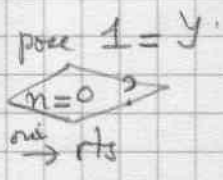
BSR XMMUL

MI72: MOVE.L A2, -(SP)

MOVE.L 8(SP), A0

MOVEQ #-1, D2

BSR XROT



Z
N
Y
P
v(x)

$N = n$

BCLR #7, (A2)
 BEQ MI700
 cas $n < 0$ pose x^{-1}
 BSR XMPINV
 BRA MI701

pose $Z \equiv x \pmod{p}$
 \pmod{v}

→ N impair
 ↓ N pair recopie Y

conserv A0/A1/A3/A4

N impair pose $Y * Z \pmod{p}$
 $\pmod{v(x)}$

conserv A3/A4

Y'

N

pose $N' = N/2$ conserv A3/A4

```

CMP #\$4000, (A2)
BNE MI75
    cas N'=0 la réponse est y'
MOVE.L A2, A6
MOVE.L (SP)+, A2
ADDQ #8, SP
MOVE.L (SP), A0
BSR XLB76
MOVEM.L (SP)+, A2/A3/A4

```

MI74:RTS

```

MI75:MOVE.L A2, -(SP)
MOVE.L 8(SP), A0 Z
MOVE.L A0, A1

```

```

BSR XMMMUL
    pose Z^2 mod p = [A3]
    mod v = 3A4

```

```

MOVE.L A2, A1 Z'
MOVE.L A6, A4 Z'fin
MOVE.L (SP)+, A6 fin y'
MOVE.L (SP)+, A2 y'

```

```

ADDQ #8, SP
MOVE.L (SP), A0
BSR XLB76 copie y'

```

```

MOVE.L A6, -(SP)
MOVE.L A1, A6 fin de N'
BSR XLB76 copie N'

```

```

MOVE.L A6, -(SP)
MOVE.L A4, A6
BSR XLB76 copie Z'
BRA MI70

```