

2) $P_{A_0} = \{A_1\}$ pose $P_{A_2} = \text{polynome } P_{A_0} \text{ mod } p$ [pour les coef] conserve A1

```

XMODPR : BSR XPSPO
          MOVEM.L M(A2, -(SP))
          MOVE (A0)+, D2
          MOVE.L A0, A1
          ADD D2, D2
          ADD D2, A0
          MOVE (A0)+, D1

```

A2=0
S=0
A1 pointe 1er var
D2 = 2 x nb de var
D1 = nb de mon - 1

```

KG80 : BSR XMONO
       MOVEM.L D1/D2/A0/A1/A4, -(SP)
       MOVE.L 20(SP), A1
       BSR XDIVMS
       CMP #4000, (A3)
       BNE KG84

```

$P = \{A1\}$
A3 n A2 x
boule sur les valeurs

```

Cas r=0
MOVEM.L (SP)+, D1/D2/A0/A1/A6

```

```

KG82 : BSR SLNGO
       ADD D0, A0
       DBRA D1, KG80
       MOVEM.L (SP)+, A1/A2
       RTS

```

```

KG84 : MOVE.L A2, A6
       MOVE.L 24(SP), A0
       MOVE.L 16(SP), A1
       BSR XADDP
       BSR XLB76
       MOVEM.L (SP)+, D1/D2/A0/A1/A4
       BRA KG82

```

S
m
S+m
remplace S