

$d = DS$
 $P = [A3] \neq 0, 1$

Remplace $\Phi = \text{var } A0$ par forme produit de facteurs irréductibles de degré d
 produit de poly de degré d

Méthode: Knuth 4.6.2 ex 30 si $p=2$ ou p430 si $p \neq 2$

Identité: $t^{p^d} - t \equiv \prod_{\lambda=0}^{p-1} (T(t) - \lambda) \pmod{p}$

où $T(t) = t + t^p + t^{p^2} + \dots + t^{p^{d-1}} = t + (t + (t + \dots + (t^{p^{p^{d-1}}})^p \dots)^p)^p$

[preuve: $\prod_{d=0}^{p-1} (x - \lambda) \equiv x^p - x$ (Knuth p423) et faire $x = T(t) = t + t^p + \dots + t^{p^{d-1}}$
 $A1^S = A0^e$ ($A0$ déduit)

répète XREDDA

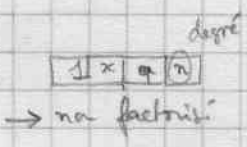
```

XMFMD: MOVE.L A0, A1
        MOVE (A0)+, D1
        SUBQ #2, D1
        BMI MI97
        BSR SLNG0
        ADD D0, A0
  
```

examine si Φ contient des facteurs de degré $> DS$

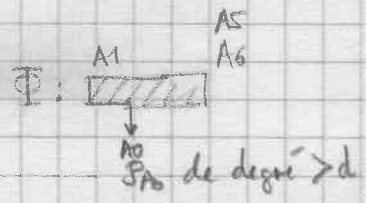
```

MI96: MOVE.L (A0)+, D0
        CMP 6(A0), D5
        BCS MI98
        ADD.L D0, A0
        DBRA D1, MI96
  
```



```
MI97: RTS
```

```
MI98: MOVE.L A6, AS
```



```
MOVEM.L DS/A1/A3, -(SP)
        d Phi P
```

```
LEA XMFMD1, A2 ) passe forme factorisée de P_A0 plus
```

```

BSR XREP
MOVE.L (SP)+, DS d
MOVE.L (SP), A0
BSR XLB76
MOVEM.L (SP)+, A0/A3
        Phi P
BRA XMFMD
  
```