

5

mdpgcd(A(x), B(x), p)

A(x) } poly à 1 lit
B(x) }

|p| ≠ 0, 1

met $W \equiv \text{pgcd}(A(x), B(x)) \pmod p$

norm(W) = 1 (si W ≠ 0)

nota : $\text{pgcd}(A, 0) = A'$ où $A' \equiv \lambda A$

YMDPGCD: BSR WCALMD1
LEA XMPGCD1, A2
BRA MI84

décade A, v, p

p = [A3]
A = PA0
v = PA4