pgcd [XGCD]
(suite res)

u et v = cte $\longrightarrow$ pgcdr(u, v)

$\deg(u) \geq \deg(v)$

x = 1er var de u

$u = a_m x^m + \dots a_0$

$v = b_n x^n + \dots a_0$

$\alpha = \text{cont}(u) = \text{pgcd}(a_m, \text{pgcd}(a_{m-1} \dots a_0))$

$\beta = \text{cont}(v) = \text{pgcd}(b_n, \dots b_0)$

$d = \text{pgcd}(\alpha, \beta)$

si $\deg(v) = 0 \longrightarrow d$

$u = u/\alpha$

$v = v/\beta$

$g = 1$

$h = 1$

$\delta = m - n$

$B^{\delta+1} u = qv + r \longmapsto \delta, B, q, r$

$r = 0$? oui

$\deg(r) = 0$? oui $\longrightarrow 1 \longrightarrow d$

$\alpha = \text{cont}(v)$

$\text{pgcd} = \frac{v}{\alpha} \cdot d$

$u = v$

$v = r / g\, h^{\delta}$

$g = B$

$\delta = 0$? oui

$\delta = 1$? oui $\longrightarrow h = g$

non

$a = g^{\delta}$

$b = h^{\delta - 1}$

$h = a/b$