Computational Algebra: List 3

Manuel Aceda Sánchez

$\boxed{2}$ Let R be a UFD, $f \in R[x]$. Show that $f = pp(f)$ if and only if f is primitive.

Recall that given $p \in R[x]$ with R a UFD we say that it is primitive if for $p = \sum_{i=0}^{m} a_i x^i$, the unique elements of R dividing all $a_0 \dots a_m$ is the multiplicative identity of R. Regarding to the notion of content, we say that for some $p \in R[x]$ is primitive if $cont(p) = 1 \in R$.

Therefore,

$\underline{\leftarrow}|$ f is primitive $\overset{\text{by def}}{\Rightarrow}$ $cont(f) = 1$. Recall that we define $pp(f)$ of f by $f = cont(f)pp(f)$, so $f = 1 \cdot pp(f) \Rightarrow f = pp(f)$

$\rightarrow|$ R is a UFD $\rightarrow$ $R[x]$ is a UFD so f uniquely factorizes as follows:

$f = u \cdot f_1 \cdots f_m$ where u is a unit an $f_1 \dots f_m$ are irreducibles of $R[x]$.

For a given $f \in R[x]$ $pp(f) \in R[x]$ and $pp(f)$ uniquely decomposes into a product of irreducibles $pp(f) = u \cdot f_1 \cdots f_m$ with $u = 1$.

Therefore $f = cont(f) \cdot pp(f) = pp(f) \Rightarrow cont(f) = 1$.

$\boxed{18}$ Why do the Mathematica commands PolynomialGCD[x^2+1, $x+1$, Modulus $\rightarrow$ 2] and PolynomialMod[PolynomialGCD[x^2+1, $x+1$], 2] compute different things

Preguntar en clase.

In this case $h = gcd(x^2+1, x+1) = 1$

$$res(f/h, g/h) = res(f,g) = \det\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = 2 \equiv 0 \bmod (2)$$

Therefore $\overset{2}{\overset{\shortparallel}{p}} \mid res(f/h, g/h)$ and so $deg(gcd(x^2+1, x+1)) \neq deg(gcd((x^2+1) \bmod 2, (x+1) \bmod 2))$

In this case the gcd of the reductions does not coincide in degree with the reductions of the gcd.

In fact, we could note that $x+1 \equiv x-1 \bmod 2$ and $(x+1)(x-1) = (x^2+1)$ and so PolynomialGCD[x^2+1, $x+1$, Modulus $\rightarrow$ 2] $= x+1$.

$\boxed{6}$ Let $f, g \in \mathbb{Z}[x]$, $r = res(f,g) \in \mathbb{Z}$ and $u \in \mathbb{Z}$. Prove that $gcd(f(u), g(u))$ divides r.

Let $f, g \in \mathbb{Z}[x]$ and let S be its Sylvester matrix, let $u \in \mathbb{Z}$ and $\bar{u} = (u^{n+m-1}, \dots, u, 1)$ where $n = deg(f)$ and $m = deg(g)$. Therefore, $\bar{u}S = (u^{m-1}f(u), \dots, f(u), u^{n-1}g(u), \dots, g(u))$ and $gcd(f,g)$ divides componentwise $\bar{u}S$. Note that $\bar{u}S = u^{n+m-1}S^1 + \dots + S^{n+m}$ where S^i is the ith row of S. Therefore, $S^{n+m} \equiv \overset{0}{\bar{u}S} - u^{n+m-1}S^1 + \dots + S^{n+m-1} \bmod (gcd(f,g))$ componentwise and so $\det S \equiv 0 \bmod (gcd(f,g)) \Rightarrow resultant(f,g) \equiv 0 \bmod (gcd(f,g))$ ∎