

Corrigé du TD 3 : Arithmétique et polynômes

Jean Sébastien ROY

Polynômes

Préliminaire utile dans la suite :

```
> with(numtheory):  
Warning, new definition for order
```

Une factorisation difficile

```
> factor(x^2458+x^1229+1);  
Warning, computation interrupted  
Manifestement Maple n'y arrive pas. Que dire de 1229 ?  
> isprime(1229);  
true  
C'est probablement un nombre premier (pas sûr, car isprime est un test probabiliste). De plus :  
> 2*1229;  
2458  
Factorisons donc quelques polynômes de la forme  $x^{2p}+x^p+1$  avec  $p$  premier.  
> seq(factor(x^(2*p)+x^p+1), p=seq(ithprime(i), i=3..5));  
( $x^2+x+1$ ) ( $x^8-x^7+x^5-x^4+x^3-x+1$ ), ( $x^2+x+1$ ) ( $x^{12}-x^{11}+x^9-x^8+x^6-x^4+x^3-x+1$ ),  
( $x^2+x+1$ ) ( $x^{20}-x^{19}+x^{17}-x^{16}+x^{14}-x^{13}+x^{11}-x^{10}+x^9-x^7+x^6-x^4+x^3-x+1$ )  
Clairement  $x^2+x+1$  revient partout.  
Regardons les polynômes cyclotomiques.  
> cyclotomic(3,x);  
 $x^2+x+1$   
Tiens donc.  
> seq(cyclotomic(3*p,x), p=seq(ithprime(i), i=3..5));  
 $x^8-x^7+x^5-x^4+x^3-x+1$ ,  $x^{12}-x^{11}+x^9-x^8+x^6-x^4+x^3-x+1$ ,  
 $x^{20}-x^{19}+x^{17}-x^{16}+x^{14}-x^{13}+x^{11}-x^{10}+x^9-x^7+x^6-x^4+x^3-x+1$   
Bon ça a l'air clair. Mais pourquoi cela ?  
> expand((x^(2*p)+x^p+1)*(x^p-1));  
( $x^p$ )3 - 1  
Ok : voir la propriété donnée dans l'énoncé.
```

Un peu d'arithmétique

```
Vérifions la propriété proposée pour de petites valeurs de n  
> seq(n*(n^6-1) mod 7, n=1..10);  
0, 0, 0, 0, 0, 0, 0, 0, 0, 0  
Tout va bien. On factorise donc :  
> Factor(n*(n^6-1) mod 7);  
n(n+6)(n+5)(n+2)(n+4)(n+3)(n+1)  
Ok. Le produit de 7 entiers consécutif est forcément divisible par 7.  
Bien noter l'utilisation de Factor et non pas de factor. Ici c'est 'mod' qui travaille.  
> factor(n*(n^6-1) mod 7);  
n(n+6)(n+1)(n^2+n+1)(n^2+6n+1)  
Ce n'est pas vraiment le résultat souhaité.  
Et avec msolve ?  
> msolve(n*(n^6-1)=0, 7);  
{ n = n }  
Ok : Tout entier est solution.
```

Racines rationnelles de polynômes de $\mathbb{Z}[X]$

```
si p/q irréductible est racine de  $an^*x^n+...+a_0$  alors :  
 $an^*p^n=-q*(a(n-1)*p^{n-1}+...+a_0*q^{n-1})$  c'est à dire :  
q divise  $an^*p^n$ . Or q est premier avec p et donc avec  $p^n$  et donc q divise  $an$ .  
De meme p divise  $a_0$ .  
Application : Faisons une fonction qui renvoie tous les nombres répondant à la condition nécessaire que l'on vient de démontrer.  
Un exemple :  
> poly:=27*(x-4/3)*(x-7/9);  
poly := 27  $\left(x-\frac{4}{3}\right)\left(x-\frac{7}{9}\right)$   
> expand(poly);  
27  $x^2-57x+28$   
> lcoeff(poly,x);  
27  
> tcoeff(poly,x);  
28  
> divisors(28);  
{ 1, 2, 4, 7, 14, 28 }  
D'où la fonction :  
> possibles:= (p,x) -> {seq(seq(i/j, j=divisors(lcoeff(p,x))), i=divisors(tcoeff(p,x)))};  
Warning, 'i' in call to 'seq' is not local  
Warning, 'j' in call to 'seq' is not local  
> possibles(poly,x);  
{  $\frac{28}{3}, \frac{28}{9}, 1, 2, 4, 7, 14, 28, \frac{28}{27}, \frac{1}{3}, \frac{1}{27}, \frac{1}{9}, \frac{4}{3}, \frac{4}{9}, \frac{2}{27}, \frac{2}{9}, \frac{4}{27}, \frac{7}{3}, \frac{7}{9}, \frac{7}{27}, \frac{14}{27}, \frac{14}{9}, \frac{14}{3}$  }  
Reste à ne sélectionner que les 'vraies' racines.  
On crée une fonction qui renvoie true (vrai) si 'v' est une racine du polynôme 'p' d'indéterminée 'x' :  
> estnul:=(v,p,x) -> subs(x=v,p)=0;  
Et on utilise select pour ne prendre dans les possibles (poss) que les vraies racines :  
> vraies:= (p,x,poss) -> select(estnul,poss,p,x);
```

```
[ On combine le tout :
> toutesracines := (p,x) -> vraies(p,x,possibles(p,x)):
[ Résultat :
> toutesracines(poly,x);
```

$$\left\{\frac{4}{3}, \frac{7}{9}\right\}$$

```
[ Great !
```

☐ Fractions rationnelles

☐ Décomposition en éléments simples

```
> q:=(x^3+x^2-x+1)/(-3*x+7*x^2-3*x^3+7*x^4);
```

$$q := \frac{x^3 + x^2 - x + 1}{-3x + 7x^2 - 3x^3 + 7x^4}$$

```
> convert(q, parfrac, x);
```

$$-\frac{1}{3} \frac{1}{x} + \frac{143}{87} \frac{1}{7x-3} + \frac{1}{29} \frac{3+7x}{1+x^2}$$

```
[ Avouons le : la décomposition en éléments simple n'est pas un sujet très passionnant.
> convert(q, fullparfrac, x);
```

$$-\frac{1}{3} \frac{1}{x} + \left(\sum_{\alpha=\%1} \frac{\frac{595}{2523} - \frac{3}{58} - \alpha + \frac{581}{5046} - \alpha^2}{x - \alpha} \right)$$

```
%1 := RootOf(-3+7_Z-3_Z^2+7_Z^3)
> convert(", radical);
```

$$-\frac{1}{3} \frac{1}{x} + \frac{143}{609} \frac{1}{x - \frac{3}{7}} + \frac{\frac{7}{58} - \frac{3}{58}I}{x - I} + \frac{\frac{7}{58} + \frac{3}{58}I}{x + I}$$

☐ Suites de Sturm

```
[ Question 1 : Il suffit de diviser par le PGCD de P et P'
Prenons un exemple :
> poly:=(x-1)^3*(x-2)^4*(x-3)^5;
```

$$poly := (x-1)^3 (x-2)^4 (x-3)^5$$

```
[ La fonction simples divise un polynome P par le PGCD de P et P'
> simples:=(p,x) -> expand(p/gcd(p,diff(p,x)));
> factor(simples(poly,x));
```

$$(x-1)(x-2)(x-3)$$

```
[ Question 2 : Il s'agit de l'agorithme d'Euclide (300 av JC).
Question 3 : Exprimer la relation de récurrence sans modulo et remplacer Pk(x) par 0.
Question 4 : Sturm(P,x) ne change de valeur que pour un x pour lequel un des Pk s'annule.
Mais comme quand un Pk s'annule, pour k>0, Pk-1 et Pk+1 ont un signe différent, peu importe comment Pk se comporte autour de x, Sturm(P,x) ne change pas de valeur. Ainsi le seul changement possible est pour P0(x)=P(x)=0
Question 5 : Quand x croît, au moment où P(x) s'annule, Sturm(P,x) décroît de 1 (quelque soit le signe de P'). D'où la propriété cherchée.
Appliquons :
D'abord, une fonction recursive renvoyant la suite de sturm a partir d'un certain rang :
> SuiteDeSturmAPCR:=proc(p0,p1,x);if p1=0 then p0 else p0,SuiteDeSturmAPCR(p1,-rem(p0,p1,x),x)
fi;end:
Puis son initialisation :
> SuiteDeSturm:=(p,x) -> [SuiteDeSturmAPCR(simples(p,x),diff(simples(p,x),x),x)]:
Un exemple :
> SuiteDeSturm(poly,x);
```

$$\left[x^3 - 6x^2 + 11x - 6, 3x^2 - 12x + 11, -\frac{4}{3} + \frac{2}{3}x, 1 \right]$$

```
[ Une version légèrement modifiée pour avoir les changements de signe :
> SignesSturmAPCR:=proc(p0,p1,x); if p1=0 then 0 else
abs(signum(p0)-signum(p1))+SignesSturmAPCR(p1,-rem(p0,p1,x),x) fi;end:
> SignesSturm:=(p,x) -> SignesSturmAPCR(simples(p,x),diff(simples(p,x),x),x)/2:
Exemple :
> SignesSturm(poly,x);
```

$$\frac{1}{2} \left| \text{signum}(x^3 - 6x^2 + 11x - 6) - \text{signum}(3x^2 - 12x + 11) \right| + \frac{1}{2} \left| \text{signum}(3x^2 - 12x + 11) - \text{signum}(x - 2) \right| + \frac{1}{2} \left| \text{signum}(x - 2) - 1 \right|$$

```
> spoly:=unapply(",x):
> spoly(-10);
```

$$3$$

```
> spoly(3/2);
```

$$2$$

```
> spoly(5/2);
```

$$1$$

```
> spoly(10);
```

$$0$$

```
[ Calculons le nombre de racines réelles :
> limit(spoly(x),x=-infinity)-limit(spoly(x),x=infinity);
```

$$3$$

```
[ The End.
```