Licence de Mathématiques — Université de Nice-Sophia Antipolis
Algèbre effective — 2011-2012

Contrôle du 2 décembre 2011
durée 1h30

Sans document.
Les réponses aux questions théoriques doivent être rédigées rigoureusement.
Les réponses aux questions utilisant Maple doivent comporter les commandes tapées et vos commentaires sur leurs résultats.

Exercice 1

Ecrire une fonction qui calcule le pgcd de deux polynômes en la variable x par l'algorithme d'Euclide.
(vous aurez besoin de la fonction **rem**).

Solution

```
> pgcd:=proc(p1,p2)
  if p2=0 then p1 else pgcd(p2,rem(p1,p2,x)) fi
  end:
```

Exercice 2

Tester votre fonction avec les deux polynômes :

```
> p1:=x^8+98*x^5-23*x^4+10*x^3-61*x^2-8*x-29:
> p2:=79*x^5+37*x^4-23*x^3+87*x^2+44*x+29:
```

Amusant n'est-ce pas ?
Les polynômes p1 et p2 sont-ils premiers entre eux ? Pourquoi ?

Solution

```
> pgcd(p1,p2);
```

-1741606573912759449304919668403755055465976283382518660484304050\
16915296472512 / 7055525025233228945246067094212578028120646270\
99553795026573896580752013443

Oui, les polynômes p1 et p2 sont premiers entre eux puisque leur pgcd est une constante.
Comme le pgcd de polynômes est déterminé à la multiplication par une constante non nulle près on peut dire que pgcd(p1,p2)=1 mais la constante donnée par l'algorithme d'Euclide est très compliquée : c'est un nombre rationnel avec 77 chiffres au numérateur et 74 au dénominateur.

Exercice 3

On va essayer de comprendre d'où vient cette fraction monstrueuse.
Modifier votre fonction pour qu'elle affiche les restes calculés à chaque étape de l'algorithme d'Euclide.
Factoriser le dénominateur du premier reste calculé.
Expliquer ce résultat.

Solution

```
> pgcd:=proc(p1,p2)
  if p2=0 then p1 else print(p2);pgcd(p2,rem(p1,p2,x)) fi
  end:
> pgcd(p1,p2);
```

$$79\,x^5+37\,x^4-23\,x^3+87\,x^2+44\,x+29$$

$$-\frac{2509654925}{38950081}-\frac{2652487366}{38950081}\,x^4+\frac{1458029761}{38950081}\,x^3-\frac{6520640612}{38950081}\,x^2-\frac{2412848510}{38950081}\,x$$

$$-\frac{331340621810369259701}{703568922678961795 6}-\frac{1217162066514883209335}{7035689226789617956}\,x^3-\frac{3211309207748050316 25}{1758922306697404489}\,x^2-\frac{1827608328815952578 74}{1758922306697404489}\,x$$

$$-\frac{716490057211482900249009854531765592}{76070881401390717411391411046108 45}-\frac{1839847055141795886899103824983123248}{7607088140139071741139141104610845}\,x^2-\frac{1659211325283546050543974267117805 16}{152141762802781434822782822092 2169}\,x$$

$$-\frac{170351707048977005896506093100363866165664333254714073}{267290972355378020108136848707204543019182097570 43488}+\frac{5674786378811423812089373049281330518653117023918 24449}{5345819447107560402162736974144090860383641951408 6976}\,x$$

$$-174160657391275944930491966840375505546597628338251866048430405\backslash\; 16915296472512 \Big/ 70555250252332289452460670942125780281206462 7\backslash\; 99553795026573896580752013443$$

$$-174160657391275944930491966840375505546597628338251866048430405\backslash\; 16915296472512 \Big/ 70555250252332289452460670942125780281206462 7\backslash\; 99553795026573896580752013443$$

```
> ifactor(38950081);
```

$$(79)^4$$

On voit que le dénominateur vaut 38950081 dans tous les coefficients du premier reste calculé. Ce nombre est le coefficient de tête du diviseur à la puissance 4 qui est le nombre d'étapes de la première division : on divise p1 de degré 8 par p2 de degré 5, il faut 4 étapes pour arriver à un reste de degré 4, à chaque étape le reste r_i a un dénominateur 79^i, pour calculer r_{i+1} on doit faire $r_i-\frac{\textit{un coefficient entier} * p2}{79^{(i+1)}}$, donc sauf simplification miraculeuse on divise une fois de plus par 79 :
première étape de la division, il reste

```
> r1:=sort(expand(p1-1/79*x^3*p2));
```

$$r1 := -\frac{37}{79}\,x^7+\frac{23}{79}\,x^6+\frac{7655}{79}\,x^5-\frac{1861}{79}\,x^4+\frac{761}{79}\,x^3-61\,x^2-8\,x-29$$

deuxiéme étape de la division, il reste

```
> r2:=sort(expand(r1+37/79^2*x^2*p2));ifactor(6241);
```

$$r2 := \frac{3186}{6241}x^6 + \frac{603894}{6241}x^5 - \frac{143800}{6241}x^4 + \frac{61747}{6241}x^3 - \frac{379628}{6241}x^2 - 8x - 29$$

$$(79)^2$$

troisième étape de la division, il reste

```
> r3:=sort(expand(r2-3186/79^3*x*p2));ifactor(493039);
```

$$r3 := \frac{47589744}{493039}x^5 - \frac{11286922}{493039}x^4 + \frac{4600831}{493039}x^3 - \frac{30130796}{493039}x^2 - \frac{4036706}{493039}x - 29$$

$$(79)^3$$

quatrième et dernière étape de la division, il reste

```
> sort(expand(r3-47589744/79^4*p2));
```

$$-\frac{2652487366}{38950081}x^4 + \frac{1458029761}{38950081}x^3 - \frac{6520640612}{38950081}x^2 - \frac{2412848510}{38950081}x - \frac{2509654925}{38950081}$$

De manière générale si on divise $p_1 = a_n x^n + ... + a_0$ par $p_2 = b_m x^m + ... + b_0$ on introduira des fractions de dénominateur $b_m^{(n-m+1)}$

Exercice 4

On va modifier la fonction pgcd pour éviter l'apparition de fraction.
A chaque étape par quoi faut-il multiplier le polynôme divisé pour que le reste soit à coefficients entiers ?
Cela change-t-il le pgcd des deux polynômes ?
Modifier votre fonction pour que les restes successifs soient à coefficients entiers
(vous aurez besoin des fonctions **lcoeff** et **degree**).

Solution

A chaque étape au lieu de diviser $p_1 = a_n x^n + ... + a_0$ par $p_2 = b_m x^m + ... + b_0$ on divisera $b_m^{(n-m+1)} p_1$ par p_2 ce qui évitera l'apparition de fraction.
Le pgcd de polynômes est défini à une constante multiplicative non nulle près donc le pgcd d p_1 et p_2 est *le même* que celui d'un multiple de p_1 et p_2 .

```
> pgcd:=proc(p1,p2)
  if p2=0 then p1 else
  print(p2);pgcd(p2,rem(lcoeff(p2)^(degree(p1)-degree(p2)+1)
  *p1,p2,x)) fi
  end:
> pgcd(p1,p2);
```

$$79x^5 + 37x^4 - 23x^3 + 87x^2 + 44x + 29$$

$$-2509654925 - 2652487366x^4 + 1458029761x^3 - 6520640612x^2 - 2412848510x$$

$$-331340621810369259701 - 121716206651488320933 5x^3$$

$$- 128452368309922012650 0x^2 - 731043331526381031496x$$

$$-543496689002998313338170146685296386340235937424556 0$$

$$- 1395624088118130435125499864055314509277008413415064 0x^2$$

$- 62930102977110210357444984841023427613855975091369\,00\, x$

$-87338506327729696222772849126290253493161032059888904053393305\backslash$
$59574549378909851516476473413599260747075924466649752738696 00 + 1\backslash$
$4547179322125617738900969732809772482319536829864454718270929390\backslash$
$79636439018175136104069632636233612612144439739690268555 2400\, x$

$-3014279267540720249308071266755210846759147176866094334053 29336\backslash$
$5031841352736824749841245779023035812544076591001690760870210961\backslash$
$3141794171910328948608087875996781455658481630310986484705555360\backslash$
$2275058595125990920622586323675913592280478410260805136656718444\backslash$
$7060940146064457000741056872085830059264000000$

$-3014279267540720249308071266755210846759147176866094334053 29336\backslash$
$5031841352736824749841245779023035812544076591001690760870210961\backslash$
$3141794171910328948608087875996781455658481630310986484705555360\backslash$
$2275058595125990920622586323675913592280478410260805136656718444\backslash$
$7060940146064457000741056872085830059264000000$

Par exemple le pgcd(p1,p2) est une constante maintenant entière au lieu d'une fraction et on peut encore dire que pgcd(p1,p2) vaut 1.
L'entier calculé par l'algorithme est très grand, on peut encore améliorer cet algorithme.