TD 6 : Arithmétique

Antoine Frénoy Pierre Gruet

5 et 12 janvier 2011

Introduction : Test de primalité (rappel)

Écrivez une procédure qui prend en argument un entier naturel et renvoie `true` s'il est premier, `false` sinon.

Exercice 1 : PGCD et identité de Bezout dans $\mathbb{Z}$

Écrivez une procédure prenant deux entiers a et b et renvoyant leur PGCD p et les deux coefficients de Bezout associés (u et v tels que $a * u + b * v = p$).

Exercice 2 : Algorithme d'exponentiation rapide

On cherche à calculer les grandes puissances d'un entier naturel d'une manière rapide. On va voir une méthode qui limite le nombre de multiplications.

- Méthode naïve : Écrivez une procédure intuitive qui prend en argument deux entiers naturels a et n et qui renvoie a^n en n'effectuant que des additions et des multiplications.
- Méthode plus intelligente : Commencez par décomposer n en base deux (vous pouvez utiliser la fonction `expand`) :

  $$n = \sum n_k * 2^k$$

  avec $\forall k, n_k = 0$ ou 1. On a alors

  $$a^n = \prod_{k \in \mathrm{I}} a^{2^k}$$

  avec $\mathrm{I} = \{k / n_k = 1\}$. Utilisez cette relation pour écrire une procédure plus rapide.
- Comparez la rapidité des deux méthodes en calculant 415^{10341}.

Exercice 3 : Se familiariser avec les polynômes

Définissez ainsi deux polynômes P et Q :

```
> P:=X^2+2*X+1;
> Q:=(X+3)^7;
```

Testez et comprenez les commandes `degree`, `expand`, `simplify`, `diff`, `factor` et `coeff`. Servez vous de l'aide si nécessaire.

Exercice 4 : Évaluation rapide d'un polynôme par la méthode de Horner

Vous avez vu en cours la méthode de Hörner permettant l'évaluation rapide d'un polynôme. Servez vous de cette méthode pour écrire une procédure `eval_horner` prenant deux arguments P et a et renvoyant $\mathrm{P}(a)$.

Exercice 5 : PGCD de deux polynômes

Soient A et B deux polynômes, B non nul : il existe un unique couple (Q, R) tel que $\mathrm{A} = \mathrm{B}*\mathrm{Q}+\mathrm{R}$ avec $deg(\mathrm{R}) < deg(\mathrm{B})$. Ce couple est donné par les fonctions `quo` et `rem`.

Utilisez cette propriété pour écrire une procédure `euclide_pol` renvoyant le PGCD de deux polynômes.

Exercice 6 : Algorithme de multiplication rapide de polynômes

Soit n un entier supérieur à 1. On cherche à écrire une procédure relativement efficace de multiplication de deux polynômes de degrés $n-1$

- Écrivez une procédure prenant en argument deux polynômes de degrés $n-1$ et renvoyant leur produit, en multipliant les coefficients deux à deux.
  Cette procédure est relativement coûteuse en calculs : elle nécessite n^2 multiplications.
- Il est possible de faire mieux. Pour multiplier $a_0 + a_1 * \mathrm{X}$ par $b_0 + b_1 * \mathrm{X}$, il est possible, au lieu d'effectuer quatre multiplications en suivant la méthode naïve, d'en effectuer seulement trois :
  Posons $q_0 = a_0 * b_0$, $q_1 = (a_0 + a_1) * (b_0 + b_1)$ et $q_2 = a_1 * b_1$, on a alors :

  $$(a_0 + a_1 * \mathrm{X}) * (b_0 + b_1 * \mathrm{X}) = q_0 + (q_1 - q_0 - q_2) * \mathrm{X} + q_2 * \mathrm{X}^2$$

  On fait donc seulement trois multiplications, et un certain nombre d'additions dont le coût est très faible comparé à celui de la multiplication.
  Ce principe peut s'appliquer récursivement à la multiplication de polynômes de degrés $n-1$: soient A et B deux polynômes de degrés $n-1$, posons

  $$m = \lceil n/2 \rceil$$

  et écrivons les divisions euclidiennes de A et de B par X^m. Il existe A_0, A_1, B_0, B_1 de degrés inférieurs ou égaux à $m-1$ tels que

  $$\mathrm{A} = \mathrm{A}_0 + \mathrm{A}_1 * \mathrm{X}^m$$

  et

  $$\mathrm{B} = \mathrm{B}_0 + \mathrm{B}_1 * \mathrm{X}^m$$

  On peut alors généraliser la formule précédente : en posant $\mathrm{Q}_0 = \mathrm{A}_0 * \mathrm{B}_0$, $\mathrm{Q}_1 = (\mathrm{A}_0 + \mathrm{A}_1) * (\mathrm{B}_0 + \mathrm{B}_1)$ et $\mathrm{Q}_2 = \mathrm{A}_1 * \mathrm{B}_1$, on a

  $$\mathrm{A} * \mathrm{B} = \mathrm{Q}_0 + (\mathrm{Q}_1 - \mathrm{Q}_0 - \mathrm{Q}_2) * \mathrm{X}^m + \mathrm{Q}_2 * \mathrm{X}^{2m}$$

  Écrivez une procédure récursive qui multiplie deux polynômes de degrés $n-1$ en utilisant cette méthode.
- Comparez la rapidité des deux méthodes en multipliant $(\mathrm{X}+3)^{400}$ par $(\mathrm{X}^2 - 7 * x + 3)^{200}$.