Travaux Pratiques numéro 6 - Maple - L1-Arithmétique

Nhung PHAM

February 27, 2014

pham@math.unistra.fr

1 Rappeler quelques notations

1.1 Division Euclidenne

On rappelle que pour tout couple d'entiers (a, b) tels que $b > 0$, il existe un unique couple d'entier (q, r) vérifiant $a = bq + r, \quad 0 \leq r \leq b - 1$. On dit q le quotient de la division euclidienne de a par b et r est appelé le reste.
La commande

- $> iquo(a, b)$: permet calculer le quotient de a divise par b $(a, b \in \mathbb{Z}, b \neq 0)$.
- $> iquo(a, b,' r')$: permet calculer le quotient de a divise par b et envoyer la valeur du reste dans r.
- $> irem(a, b)$: permet calculer le reste de a divise par b $(a, b \in \mathbb{Z}, b \neq 0)$.
- $> irem(a, b,' q')$: permet calculer le reste de a divise par b et envoyer la valeur du quotient dans q.

Exercice 1 :
Écrire une procéndure qui prend en entreés deux entiers a et b et qui renvoie une liste contenant le quotient et le reste de la division euclidienne de a par b.

1.2 Plus grand diviseur commun (PGCD)

Le plus grand diviseur commun ou PGCD de deux entiers strictement postifs a et b est le plus grand nombre entier positif qui divise a et b. On le note $PGCD(a, b)$. Pour le calculer, on utilise généralement l'algorithme d'Euclide.
L'algorithme d'Euclide:
Soient a et b deux entiers naturels non nuls, avec $a > b$

1.2.1 On calcule le reste r de la division de a par b.

1.2.2 Si le reste est non nul, a prend la valeur de b et b prend la valeur de r et on va au point 1.2.1

1.2.3 Si le reste est nul, on a trouve le $pgcd$ qui vaut b.

La commande

- $> igcd(a, b, c, d, ...)$ envoie le $pgcd$ de a,b,c, d,... avec $a, b, c, d, ... \in \mathbb{Z}$.
- $> gcd(a, b)$ envoie le $pgcd$ de a,b avec a, b deux polynômes.
- $> gcd(a, b,' u',' v')$ envoie le $pgcd$ de a,b avec a, b deux polynômes,et $u := \frac{a}{pgcd(a,b)}, v := \frac{b}{pgcd(a,b)}$.

Exercice 2 :
Grâce à l'algorithme d'Euclide, écrire une procédure prenant en entr´des deux entiers a et b et renvoyant leur $PGCD$.

1.3 L'indicatrice d'Euler.

L'Indicatrice d'Euler est une fonction φ qui associe à n le nombre des positifs inférieurs ou égaux à n qui sont premiers avec n. On a φ vérifie les propriétés suivantes :

- $\varphi(p) = p - 1$ si et seulement si p est premier,
- $\varphi(p^k) = (p-1)p^{k-1}$ pour tout nombre premier p,
- $\varphi(uv) = \varphi(u)\varphi(v)$ si u et v sont deux nombre premiers entre eux,
- $\sum_{d\backslash n} \varphi(d) = n$.

Exercice 3:

Écrire une procédure qui, donné n, calcule $\varphi(n)$. Vérifier sur des exemples numériques les égalités précédentes.

1.4 Test de Primalité

(Test naïf) Pour savoir si un nombre p est premier , on essaye de le diviser par tous les nombres entiers de 2 à p. Si on a pas trouvé de diviseur, on sait qu'il est premier.

Exercice 4 :

Ecrire une procédure permettant de tester si un nombre p est premier?

Exercice 5 :

Réfléchissez à des moyens d'améliorer la méthode précédente afin de diminuer sensiblement le temps de calcul pour les procédures précédentes. Ecrire la procédure permettant de tester si un nombre est premier avec la méthode améliorer.

(Idée: Si $p = uv$ alors soit $u \leq \sqrt{p}$ soit $v \leq \sqrt{p}$ ...)

La commande $>$ *time* permet de tester la vitesse d'éxécution d'une procédure. Comparez les vitesses des deux procédures précédentes.

1.5 Le crible d'Eratosthène

Soit N un entier fixé. Pour déterminer tous les nombres premiers entre 2 et N, on prend une liste des entiers de 2 à N, on entoure le premier nombre, en l'occurrence 2, puis on parcourt la liste en barrant tous ses multiples. On poursuit ensuite avec la liste restante à partir du nombre après 2, on entoure le nombre suivant c'est à dire 3 puis on barre tous ses multiples. On continue avec $5, 7, 11, ...$ jusqu'à parcourir l'ensemble de la liste.

Dans Maple, la commande $subsop(i = NULL, L)$ permet de supprimer l'élément en position i de la liste L. La commande $nops(L)$ permet de connaître le nombre d'élément de la liste L.

Exercice 6 :

Ecrivez le crible d'Eratosthène pour les entiers de 2 à 100. En utilisant le crible d'Eratosthène, créez une procédure qui prend comme argument un entier N et qui renvoie une liste des nombres premiers inférieurs à N. Testez la procédure sur des nombres N pas trop élevés.

Vérifier que le résultat est correct en utilisant la commande *ithprime* (La commande *ithprime* permet donner le $i^{ème}$ premier).

2 Arithmétique et polynômes

Exercice 7 :

Soient p et q deux polynômes.

Le *pgcd* s'obtient par la commande *gcd* et le *ppcm* par la commande *lcm*. Par exemple

$> a := 2 * x * *3 - 2 : b := x * *2 - 1 :$

$> gcd(a, b); lcm(a, b);$

Vérifier que $ab = pgcd(a, b) \cdot ppcm(a, b)$ pour cet exemple.

Le quotient et le reste de la division euclidienne s'obtiennent par les commandes *quo* et *rem*. $> q := quo(a, b, x);$

$> r := rem(a, b, x);$

Vérifier que l'on a bien $a = bq + r$, avec $degre(r) < degre(b)$, sur l'exemple.

Exercice 8 :

Reprendre l'algorithme d'Euclide dans les cas de deux polynômes et vérifier le résultat pour a et b polynômes la forme $(x-i)(x^2-j)$, avec $0 \leq i, j \leq 2$ en comparant avec *gcd*.

Remarque:

De manière générale, il faut tester vos procédures sur beaucoup d'exemples, de rédiger sur UNE FEUILLE ce que vous constatez concernant leur fonctionnement et leur temps d'éxécution ainsi que les résultats que vous obtenez. On rappelle que le bouton stop (main blanche sur fond rouge) permet d'arrêter l'éxécution d'une procédure.