Applications de l'algorithme d'Euclide sur les entiers et les polynômes — Correction des exercices —

Exercice 1 -

1. Un anneau commutatif A est *euclidien* s'il est unitaire, intègre et s'il existe une application $\nu : A-\{0\} \to \mathbb{N}$ vérifiant la propriété de *division euclidienne* : pour tout couple (a,b) d'éléments de A tel que $b \neq 0$, il existe $(q,r) \in A \times A$ tel que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$. Sur l'anneau $\mathbb{Z}$, l'application $\nu : \mathbb{Z} - \{0\} \to \mathbb{N}$, $\nu(m) = |m|$ vérifie la propriété de division euclidienne (pourquoi ?), donc $\mathbb{Z}$ est euclidien. Sur l'anneau $k[X]$, l'application $\nu : k[X] - \{0\} \to \mathbb{N}$, $\nu(P) = \deg(P)$ vérifie la propriété de division euclidienne (pourquoi ?), donc $k[X]$ est euclidien. L'unicité de la division euclidienne n'est pas dans la définition : par exemple sur $\mathbb{Z}$, $19 = (-5)(-3) + 4$ avec $|4| < |-5|$ et $19 = (-5)(-4) + (-1)$ avec $|-1| < |-5|$. Toutefois, on peut l'obtenir en demandant $r \geq 0$. Sur $k[X]$, l'unicité se démontre facilement.
2. Partant de $(a,b) \in A \times A$ avec $b \neq 0$ et $\nu(a) \geq \nu(b)$ on calcule les restes (r_i) par récurrence :
   - $r_0 = a$, $r_1 = b$;
   - Tant que $r_i \neq 0$, r_{i+1} est le reste de la division euclidienne de r_{i-1} par r_i : $r_{i-1} = r_i q + r_{i+1}$.
   Tant que $r_i \neq 0$, la suite $\nu(r_i)$ décroît strictement. Puisque $\mathrm{pgcd}(r_{i-1}, r_i) = \mathrm{pgcd}(r_i, r_{i+1})$, dès que $r_{i+1} = 0$, r_i est un p.g.c.d. de (a,b).
3. Pour $i \geq 0$, tant que $r_i \neq 0$, on construit (u_i, v_i) ayant la propriété que $r_i = u_i a + v_i b$. A la fin de l'algorithme, on obtient ainsi un couple de Bézout. De la relation $r_{i+1} = r_{i-1} - q r_i$ on déduit facilement les récurrences : $u_{i+1} = u_{i-1} - q u_i$, $v_{i+1} = v_{i-1} - q v_i$. On initialise alors avec $(u_0, v_0) = (1,0)$ et $(u_1, v_1) = (0,1)$.

Exercice 2 -

1. Soit d un p.g.c.d. de a et b. Si d ne divise pas c, il n'y a pas de solution. Sinon, posons $a' = a/d$, $b' = b/d$, $c' = c/d$ et soit (u,v) un couple de Bézout de (a,b). Une solution particulière est $x_0 = uc'$, $y_0 = vc'$ et l'ensemble des solutions est $x = kb' + x_0$, $y = y_0 - ka'$ pour $k \in \mathbb{Z}$.
2. Soit $e = \mathrm{pgcd}(a,b,c)$. Si e ne divise pas d, il n'y a pas de solution. Sinon, en remarquant que $e = \mathrm{pgcd}(\mathrm{pgcd}(a,b),c)$, on pose $e' = \mathrm{pgcd}(a,b)$. On a $e = \mathrm{pgcd}(e',c)$ et on choisit des couples de Bézout $e' = au' + bv'$ et $e = e'u + cv$. Alors $e = au'u + bv'u + cv$. On en déduit une solution. Pour la description de *toutes* les solutions, regarder par exemple sur :

   `http://wims.unice.fr/wims/fr_U1~algebra~docmodarith.fr.html`
3. Écrivons l'action de chaque marin comme une fonction : il part d'un tas de x noix, en jette une, puis cache le cinquième du tas restant. Il reste donc un tas de $f(x) := \frac{4}{5}(x-1)$ noix. Le lendemain, après que chacun des cinq marins ait fait cette action, il reste un nombre de noix multiple de 5. L'équation est donc $f^5(x) = 5y$, dont on cherche les solutions entières. Nous finirons le calcul sur Maple.

Exercice 3 -

1. Soit A un anneau euclidien et $a, b \in A$ tels que $\text{pgcd}(a, b) = 1$. Alors $A/(a) \times A/(b) \cong A/(ab)$. L'application $A/(ab) \to A/(a) \times A/(b)$ est (bien !) définie par $\alpha \mapsto (\alpha \mod (a), \alpha \mod (b))$. Elle est injective car si $a|\alpha$ et $b|\alpha$, alors $ab|\alpha$ puisque a et b sont premiers entre eux. Pour la surjectivité, partant de (α, β) on cherche x tel que $x \equiv \alpha \mod (a)$ et $x \equiv \beta \mod (b)$. Soit un couple de Bézout (u, v) de (a, b) : $au + bv = 1$. Alors $x = au\beta + bv\alpha$ convient.
2. On se ramène à une équation diophantienne (Exercice 2). Posons $d = \text{pgcd}(a, n)$. Si d ne divise pas b, il n'y a pas de solution. Sinon, avec les mêmes notations, les solutions sont de la forme $x = kn' + ub'$, $k \in \mathbb{Z}$. Mais on ne s'intéresse qu'aux solutions distinctes modulo n. Pour k_1, k_2, les valeurs associées de x modulo n sont égales si et seulement si d divise $k_1 - k_2$. Donc il y a d solutions données par $k = 0, \ldots, d - 1$.
3. On résout $ax \equiv 1 \mod (n)$ comme ci-dessus. Si $d = 1$, l'inverse est u, sinon a n'est pas inversible.

Exercice 4 -

1. Pour la multiplication : soit $f, g \in k[X]/(P)$ représentés par des polynômes F, G. On fait la division euclidienne $FG = PQ + R$ et on a $f \cdot g = R$. Dans $\mathbb{Q}(\alpha)$, soit P le polynôme minimal de α sur $\mathbb{Q}$. Alors $\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(P)$. Le polynôme P est irréductible. Il reste à comprendre la division (calcul d'inverse). Pour $f \in k[X]/(P)$ représenté par un polynôme F avec $\deg(F) < \deg(P)$, on a $\text{pgcd}(F, P) = 1$ car P est irréductible. Soit un couple de Bézout $1 = UF + VP$. On fait la division euclidienne $U = PQ + R$. Alors $f^{-1} = R$.
2. Il reste à calculer la dimension : la dimension vectorielle est k, donc il y a p^k éléments.

Exercice 5 - On doit calculer les degrés dans l'algorithme d'Euclide étendu (Exercice 1). Partant de $\deg(a) \geq \deg(b)$, la suite $\deg(r_i)$ décroît strictement pour $i \geq 1$, et $\deg(q_i) = \deg(r_{i-1}) - \deg(r_i)$. On montre aisément par récurrence que les suites $\deg(u_i)$ et $\deg(v_i)$ sont croissantes pour $i \geq 1$ et que $\deg(u_i) \leq \deg(b) - \deg(r_i)$ et $\deg(v_i) \leq \deg(a) - \deg(r_i)$ pour $i \geq 2$.
On applique avec $a := F(x)$ le développement limité de f à l'origine à l'ordre $p + q$, $\deg(F) = p + q$, et $b := x^{p+q}$. On se ramène facilement au cas où $f(0) \neq 0$, donc $\text{pgcd}(a, b) = 1$. Soit j le premier indice tel que $\deg(r_j) \leq p$. Posons $P := r_j$ et $Q := u_j$. On a $\deg(P) \leq p$ et $\deg(Q) \leq q$ d'après ce qui précède. De l'égalité $P = QF + v_j x^{p+q}$ on déduit $F = \frac{P}{Q} + O(x^{p+q})$ et si $Q(0) = 0$ on a aussi $P(0) = 0$ donc on peut simplifier la fraction (ce qui réduit le degré des polynômes : certains auteurs excluent cette possibilité.)