UNIVERSITÉ D'ANTANANARIVO

DOMAINE SCIENCES ET TECHNOLOGIES

MENTION MATHÉMATIQUES ET INFORMATIQUE

Année Universitaire 2023-2024

Semestre 5

Licence L3 - PAAC

ALGÈBRE ALGORITHMIQUE I

TD no. 1 - Algorithmes et Pseudo-codes

N.B. Soit $(R, +, \times)$ un anneau commutatif. On suppose que notre langage mathématique algorithmique permet d'effectuer les opérations dans cet anneau. Lorsque R est un corps, on utilise la notation K.
(1) Soit X une variable et $R[X]$ l'anneau des polynômes en X, à coefficients dans r. Un élément de $R[X]$ s'écrit f ou $f(X)$, avec

$$f(X) = f_0 + f_1X + \cdots + f_iX^i + \cdots + f_nX^n \text{ avec } \quad n \in \mathbb{N} \text{ et } f_i \in R \text{ pour } i = 0, \ldots, n. \tag{1}$$

S'il existe $i \in \{0, \ldots, n\}$ tel que $f_i \neq 0$, le degré de f est $\max\{i \mid 0 \leqslant i \leqslant n \text{ et } f_i \neq 0\}$. Sinon, $f = 0$ et on pose $\deg f = -\infty$. Le polynôme f est une constante non nulle ssi $f = f_0$, ce qui équivaut à $\deg f = 0$.
(2) Dans $\mathbb{F}[X]$, la *division euclidienne* de f par g où $f, g \in \mathbb{F}[X]$ avec $g \neq 0$, produit deux polynômes $q, r \in \mathbb{F}[X]$ tels que

$$f = gq + r \quad \text{avec} \quad r = 0 \quad \text{ou} \quad \deg r < \deg g. \tag{2}$$

Le polynôme q est noté par $f \text{ div } g$ et r par $f \bmod g$. Donc g divise f (on dit que g divise f et on note $g|f$) ssi $f \bmod g = 0$ et dans ce cas, on a $f = gq$.

Exercice 1. Faire un algorithme (organigramme +pseudo-code) pour
Calculer a^n pour $a \in R$ et $n \in \mathbb{N}$.

Exercice 2. Soit $p \geqslant 2$ un entier. Dans $\mathbb{Z}/p\mathbb{Z}$, l'addition et la multiplication sont effectuées mudulo p. Ces lois munissent $\mathbb{Z}/p\mathbb{Z}$ d'un structure d'anneau commutatif.
Faire la table d'addition et de multiplication pour les anneaux suivants :
(1) $\mathbb{Z}/2\mathbb{Z}$, (2) $\mathbb{Z}/3\mathbb{Z}$, (3) $\mathbb{Z}/4\mathbb{Z}$, (4) $\mathbb{Z}/5\mathbb{Z}$.

Exercice 3. Trouver, s'il existe, une racine des polynômes suivantes :

(1) $f(X) = X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$,

(2) $f(X) = X^3 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$,

(3) $f(X) = X^4 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$,

(4) $f(X) = X^2 + X + 1 \in (\mathbb{Z}/3\mathbb{Z})[X]$.

Exercice 4. Soit $f(X) \in R[X]$ avec

$$f(X) = f_0 + f_1 X + \cdots + f_i X^i + \cdots + f_n X^n$$

où $n \in \mathbb{N}$ et $f_i \in R$ pour $i = 0, \ldots, n$.

(1) Ecrire un algorithme (organigramme+pseudo-code) pour construire la liste f qui contient les coefficients de $f(X)$, suivant les puissances croissantes de X.

(2) Soit $a \in R$.

(a) Donnez l'expression de $f(a)$.

(b) Faire un algorithme (organigramme +pseudo-code) pour calculer $f(a)$.

Exercice 5. Faire un algorithme (organigramme+pseudo-code) pour trouver toutes les racines d'un polynôme $f(X)$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Vérifiez votre algorithme par un exemple simple non trivial.

Exercice 6. Soit $(G, *)$ un groupe fini, i.e $\mathsf{card}(G) = |G| = n$ est fini. Soit e l'élément neutre de G.

(1) Soit $g \in G$. Soit

$$A = \{\underbrace{g * g * \cdots * g}_{k\text{fois}} \mid k \in \mathbb{N}\}. \tag{3}$$

(a) Comment s'écrit l'égalité (3) si la loi de G et notée multiplicativement ?

(b) Comment s'écrit l'égalité (3) si la loi de G et notée additivement ?

(2) Que peut-on dire de $\mathsf{card}\, A$?

(3) Montrer qu'il existe un plus petit entier $h \in \mathbb{N}^*$ tel que

$$\underbrace{g * g * \cdots * g}_{h\text{fois}} = e. \tag{4}$$

Terminologie. L'entier h de la question (2) est appelé l'ordre de g et est noté par $o(g)$.

Exercice 7. Trouver l'ordre de g dans G dans chacun des cas suivants :

(1) $G = (\mathbb{Z}/6\mathbb{Z}, +), g = 1, 2, 3, 4, 5$

(2) $G = (\mathbb{Z}/7\mathbb{Z}^*, \times), g = 2, 3, 4$.

Exercice 8. Soit $(G,+)$ un groupe fini de cardinal n et $g \in G$. Faire un algorithme (organigramme +pseudo-code) pour trouver $o(g)$.

Exercice 9. Même question que l'exercice 8, mais la loi de G est notée multiplicativement.

Exercice 10. Soit $(G,\times)$ un groupe fini, avec $G = \{g_1,\dots,g_n\}$ où $g_1 = 1$. Montrer qu'il existe un plus petit entier $N \in \mathbb{N}^*$ tel que

$$(\forall g \in G) \quad [g^N = 1].$$

(*Indication* : utiliser l'exercice 6). L'entier N est appelé l'*exposant* de G.

Exercice 11. Soient $a,b \in \mathbb{N}$ avec $a > b \neq 0$. La *division euclidienne* de a par b trouve l'unique couple d'entiers $(q,r) \in \mathbb{N}^2$ vérifiant

$$a = bq + r \quad \text{avec} \quad 0 \leqslant r < b.$$

On peut calculer r par la méthode suivante : On soustraie b à a. Si le nombre obtenu est plus petit que b, c'est le reste r et on arrête le processus. Sinon on recommence le processus en remplaçant a par la différence obtenue.
Faire un algorithme (organigramme +pseudo-code) correspondant à cette méthode.

Exercice 12. Soient $f(X), g(X) \in R[X]$. Soient la somme $S(X) = f(X) + g(X)$ et le produit $P(X) = f(X) \cdot g(X)$.
(1) Ecrire l'expression qui donne S.
(2) Ecrire l'expression qui donne P.
(3) On représente les polynômes $A(X)$ de $R[X]$ par la liste A de ses coefficients selon l'exercice 4.

(a) Faire un algorithme (organigramme +pseudo-code) pour trouver S.
(b) Faire un algorithme (organigramme +pseudo-code) pour calculer P.

Exercice 13. Soit le corps fini à 5 éléments $\mathbb{F}_5$. Soient les polynômes

$$f(X) = 2X^4 + 4X^2 + 3X + 2, \quad g(X) = 3X^2 + 4 \in \mathbb{F}_5[X].$$

Effectuer la division euclidienne de $f(X)$ par $g(X)$.

Exercice 14. On suppose que l'écriture usuelle (1) d'un polynôme de $\mathbb{F}[X]$ est une structure de donnée acceptable pour notre langage mathématique algorithmique. Soient $f,g \in \mathbb{F}[X]$ avec $g \neq 0$. Ecrire un algorithme (organigramme +pseudo-code) qui donne le quotient de f par g.