Arithmétique 2

Exercice 1.

Pour une suite de réels (le plus souvent entiers) $(a_n)_{n\in\mathbb{N}}$, on définit la fraction continue $[a_0, a_1, ..., a_n]$ par

$$[a_0, a_1, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

Soit $x \in \mathbb{R}$. Le développement en fractions continue d'un réel x est défini par récurrence par $a_n = \lfloor x_n \rfloor$, $x_0 = x$, et tant que x_n n'est pas entier, $x_{n+1} = \frac{1}{x_n - a_n}$ (si x_n est entier, les deux suites s'arrêtent). On démontre que l'on a alors

$$x = \lim_{n\to+\infty} [a_0, a_1, \ldots, a_n]$$

(1) Soit $x \in \mathbb{R}$.
   (a) Vérifier que $x = [a_0, a_1, \ldots, a_p, x_p]$ pour tout p tel que la suite est définie.
   (b) Vérifier que la suite (x_n) est bien définie pour tout n si et seulement si x est irrationnel.

(2) Écrire un programme qui étant donné un nombre x, calcule les n premiers termes de la suite (a_n) ci-dessus.

(3) Vérifier expérimentalement que $x = \lim[a_0, ;a_n]$ pour une valeur de x de votre choix.

(4) Donner le développement en fraction continue de $\sqrt{2}$ et de $\varphi = \frac{1+\sqrt{5}}{2}$. Donner les 20 premiers termes du développement en fraction continue de π.

Exercice 2.

Une approximation d'un nombre x par un nombre rationnel $\frac{p}{q}$ est bonne si l'on atteint une erreur $\varepsilon = |x - \frac{p}{q}|$ petite avec un dénominateur q qui n'est pas trop grand. Le développement en fraction continue permet d'obtenir les meilleures approximations d'un nombre x en général. Pour un nombre irrationnel x, soit $u_n = [a_0, a_1, ..., a_n] = \frac{p_n}{q_n}$ son $n^{\text{ème}}$ développement en fractions continues. Soit $C_n = |x - \frac{p_n}{q_n}| q_n^2$.

(1)

(2) Écrire un programme qui, étant donné un développement en fraction continue $[a_0, a_1, ..., a_n]$, calcule le numérateur et le dénominateur de u_n.

(3) Pour le nombre d'or $x = \phi = \frac{1+\sqrt{5}}{2}$ et pour $x = \pi$, calculer les premières valeurs de u_n, p_n, q_n et C_n.

(4) Vérifier expérimentalement le théorème d'approximation de Dirichlet : pour un nombre irrationnel x, il existe une infinité de nombres rationnels $\frac{p}{q}$, tels que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2}$$

Exercice 3.

Etant donné un polynôme réel P, on définit sa suite de Sturm $(P_n)_{n\in\mathbb{N}}$ par $P_0 = P$, $P_1 = P'$, $P_i = -P_{i-2} \bmod P_{i-1}$ pour $i \leq 2$, jusqu'au polynôme P_k qui est constant (et alors la suite s'arrête).

Pour tout nombre réel x, on note $V(x)$ le nombre de changements de signe dans la suite des signes de $P_0(x), P_1(x), ..., P_k(x)$, en supprimant les zéros éventuels. Par exemple, le nombre de changements de signe de la suite de signes $0, +, -, -, 0, +, +, -$ est égal à 3. On rappelle :

Théorème. Soit P un polynôme sans racine multiple, et soient $a, b \in \mathbb{R}$ tels que $P(a) \neq 0$ et $P(b) \neq 0$. Alors le nombre de racines réelles de P dans l'intervalle $[a, b]$ est égal à $V(a) - V(b)$.

(1) Écrire une procédure qui prend en entrée un polynôme rationnel sans racine multiple P et deux nombres a et b, et qui renvoie le nombre de racines de P dans l'intervalle $[a, b]$.

(2) En utilisant la procédure précédente, et en procédant par dichotomie, écrire une procédure récursive qui prend en entrée un polynôme rationnel sans carré P et un paramètre d'erreur $\varepsilon > 0$ et renvoie un ensemble de couples (I, m) constitués :
— D'un intervalle I strictement inférieure à ε
— D'un entier m, nombre de racines de P dans I
tels que la réunion des intervalles recouvre toutes les racines de P.

1. Algorithme de Berlekamp

Exercice 4.

Soit k un corps fini de cardinal q. Nous allons programmer l'algorithme de Berlekamp pour factoriser un polynôme $P \in k[X]$ sans facteur carré.

(1) Étant donné un polynôme $P \in k[X]$, considérons Φ l'application linéaire de $k[X]/(P)$ dans lui même définie par $\Phi : f \mapsto f^q - f$.
Écrire une fonction qui prend en argument un polynôme $P(X) \in k[X]$ et qui renvoie la matrice de Φ dans la base $\{1, X, X^2, ...\}$.
Que s'attend-t-on à trouver pour la 1ère colonne ?
Quelle matrice obtient-on pour le polynôme $P = X^4 + X^3 + X^2 + X + 1$ de $\mathbb{Z}/19\mathbb{Z}[X]$?

(2) Écrire une fonction qui, étant donné un polynôme P, détermine une base du noyau de cette matrice.

(3) Écrire une fonction qui prend en argument deux polynômes P et Q, et qui recherche un $s \in k$ tel que le PGCD de P et de $Q - s$ soit non trivial, en renvoyant le diviseur de P ainsi trouvé, et en renvoyant `None` s'il n'y en a pas.

(4) Programmer une fonction qui prend un polynôme sans facteur carré à coefficients dans un corps fini et qui donne un diviseur non trivial de ce polynôme (éventuellement le polynôme lui-même, ou plutôt `None` (c'est a dire rien du tout), s'il est irréductible).

(5) Tester avec $X^4 + 1$ puis avec $X^{12} + X^2 + 1 \in \mathbb{F}_p[X]$ pour les nombres premiers $2 \leq p \leq 19$. On pourra vérifier les résultats avec la méthode `.is_ irreducible()` ou `.factor()`.
Que se passe-t-il pour $X^4 + 1$ et $p = 2$?

(6) Programmer la fonction `Berlekamp` qui prend un polynôme sans facteur carré à coefficients dans un corps fini, et qui renvoie sa décomposition en produit d'irréductibles.
Tester avec $X^{12} + X^2 + 1$ sur $\mathbb{F}_{19}$.