Quotients et restes chinois

Exercice 1. Révisions

1. Déterminer une solution $(A, B) \in \mathbb{Q}[X]^2$ de l'équation $A \times (X^4+2X+1)+B \times (X^3-X+2) = 1$.
2. Déterminer la liste de tous les nombres premiers p inférieurs à 100 tels que les polynômes $X^4 - 23X^3 + 113X^2 - 22X + 112$ et $X^3 - X^2$ ne soient pas premiers entre eux dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

Exercice 2. Nombre d'or et quotients

On rappelle que le nombre d'or ϕ est la racine positive de $X^2 = X + 1$.

1. Soit $K \subset L$ deux corps et $x_0 \in L$.
   (a) On note $\mathrm{ev}_{x_0} : K[X] \to L$ l'application qui envoie P sur $P(x_0)$. Montrer que ev_{x_0} est un morphisme d'anneau.
   (b) Soit $P_0 \in K[X]$. À quelle condition le morphisme ev_{x_0} passe-t-il au quotient $K[X]/(P_0)$?
   (c) On suppose maintenant que P_0 est irréductible et que $P_0(x_0) = 0$. Montrer que $K[X]/(P_0)$ est isomorphe à $\mathrm{ev}_{x_0}(K[X])$.
2. Dans `Sage`, la méthode `quotient` des anneaux de polynômes permet de définir un quotient d'un anneau de polynômes par un idéal. En utilisant un quotient judicieux, simplifier les expressions suivantes
$$\phi^7 + 2\phi^6 + \phi^4 + 1, \quad \frac{1}{\phi^7 - 1}, \quad \frac{\phi^4 - \phi + 1}{\phi^7 - 1}.$$
On expliquera soigneusement les fondements de cette méthode, en s'appuyant sur la première question.

Exercice 3. Restes chinois

1. Écrire une fonction `systeme_chinois(a, m)` qui, à partir de listes d'entiers `a` et `m` de longueur r, renvoie une solution x du système de congruences
$$x \equiv a_i \,(\mathrm{mod}\, m_i)\,,\ 1 \leqslant i \leqslant r$$
en supposant que les m_i sont des entiers naturels 2 à 2 premiers entre eux. On pourra essayer d'abord d'évaluer `zip([1,2], [3, 4])` et lire l'aide de `sum` et `prod`.
2. Comparer avec la commande `crt`.
3. A l'aide du théorème des restes chinois, déterminer un polynôme $P \in \mathbb{Q}[X]$ de degré au plus 3 tel que $P(0) = 1$, $P'(0) = 1$, $P(1) = 1$ et $P'(1) = -1$ (indication : interpréter les identités en termes de résidus modulo X^2 et $(X-1)^2$).

Exercice 4. Quotients et développements limités

1. À l'aide de `Sage`, définir $A = \mathbb{Q}[X]/(X^{10})$.
2. Déterminer les inversibles de A (on demande un argument théorique).
3. À l'aide de `Sage`, déterminer l'inverse de la classe de $1 - X$ dans A.

4. (Bonus) On note $\mathbb{Q}[[X]]$ l'anneau des séries formelles à coefficients rationnels. Ses éléments sont des séries $\sum_{n\geqslant 0} a_n X^n$, sans condition de convergence. Il est muni de l'addition terme à terme et du produit de Cauchy, de sorte que l'inclusion $\mathbb{Q}[X] \to \mathbb{Q}[[X]]$ est un morphisme d'anneaux. Montrer que cette inclusion descend en isomorphisme de A sur $\mathbb{Q}[[X]]/(X^{10})$. Montrer que $1-X$ est inversible dans $\mathbb{Q}[[X]]$, d'inverse $\sum_{n\geqslant 0} X^n$, et retrouver le résultat de la question précédente.

Exercice 5. Petit théorème de Fermat

1. Écrire une fonction `fermat(p)` qui confirme ou infirme qu'un nombre entier p donné vérifie la conclusion du *petit théorème de Fermat* : « si p est un nombre premier, alors $a^p \equiv a \,(\mathrm{mod}\, p)$ pour tout entier a ».
2. Vérifier le théorème pour les entiers premiers inférieurs à 1000.
3. Montrer, en utilisant `Sage`, que la condition « être premier » n'est pas nécessaire pour vérifier la conclusion du petit théorème de Fermat.

Exercice 6. Test de primalité de Miller–Rabin

1. Soit p un nombre premier. Montrer que si $a^2 \equiv 1 \,(\mathrm{mod}\, p)$, alors $a \equiv 1 \,(\mathrm{mod}\, p)$ ou $a \equiv -1 \,(\mathrm{mod}\, p)$.
2. On veut montrer que si p est un nombre premier impair et $p-1 = 2^s t$ avec t impair alors, pour tout a premier avec p
   - soit $a^t \equiv 1 \,(\mathrm{mod}\, p)$,
   - soit il existe $i \in \{0, ..., s-1\}$ tel que $a^{2^i t} \equiv -1 \,(\mathrm{mod}\, p)$.

   Soit a premier avec p. On pose $b = a^t$.
   (a) Justifier que b est inversible modulo p. On notera α l'ordre de b en tant qu'élément de $(\mathbb{Z}/p\mathbb{Z})^\times$.
   (b) Montrer que α divise 2^s. Dans la suite on notera $\alpha = 2^j$.
   (c) Montrer que si $j \neq 0$ alors $a^{t2^{j-1}} \equiv -1 (\,\mathrm{mod}\, p)$.
   (d) Conclure.
3. On considère le pseudo code suivant qui décrit le test de Miller–Rabin.
   ⋆ Entrée : un nombre impair n, et un nombre entier a premier avec n.
   - Calculer s et t tels que $n-1 = 2^s t$, avec t impair.
   - Si $a^t \equiv 1 (\,\mathrm{mod}\, n)$, la procédure s'arrête et renvoie « vrai ».
   - Pour i de 0 à $s-1$: si $a^{t2^i} \equiv -1 (\,\mathrm{mod}\, n)$ alors la procédure s'arrête et renvoie « vrai ».
   - Si l'on ne s'est pas arrêté avant, la procédure renvoie « faux ».

   Que conclure si l'algorithme renvoie « vrai » ? Et s'il renvoie « faux » ? Justifier.
4. Implanter le pseudo code ci-dessus en une fonction `miller_rabin(n, a)`, et le tester sur quelques valeurs de a et n.
5. Déterminer expérimentalement un couple (n, a) avec n composé (*i.e.*, non premier) et tel que `miller_rabin(n, a)` renvoie « vrai ». Vérifier expérimentalement que cette situation se produit pour moins de la moitié des a.