Anneaux $\mathbb{Z}/n\mathbb{Z}$

Exercice 1. Échauffement.

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

Exercice 2. 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

$$x \equiv a_i \,(\mathrm{mod}\, m_i)\,,\ 1 \leq i \leq r$$

   en supposant que les m_i sont des entiers naturels 2 à 2 premiers entre eux.
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 3. 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 4. 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 $a^{t2^{j-1}} \equiv -1 (\bmod p)$.

(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 $a^t \equiv 1 (\bmod n)$, la procédure s'arrête et renvoie « vrai ».
   - Pour i de 0 à $s-1$: si $a^{t2^i} \equiv -1 (\bmod n)$ 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.

Exercice 5. Exercice bonus – Quelques propriétés des nombres de Carmichael.

On appelle *nombre de Carmichael* un entier $n \geq 2$ composé vérifiant néanmoins le résultat du théorème de Fermat, c'est-à-dire $a^n \equiv a (\bmod n)$ pour tout $a \in \mathbb{Z}$.

1. Déterminer avec `Sage` le plus petit nombre de Carmichael.

On cherche à déterminer de grands nombres de Carmichael.

2. Montrer que si n est un nombre de Carmichael, alors :
   - n est sans facteur carré (indication : on pourra utiliser que $p^n \equiv p (\bmod n)$).
   - pour tout facteur premier p de n, $(p-1) \mid (n-1)$ (indication : on pourra utiliser que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique).

3. Montrer que réciproquement, un nombre composé n qui est sans facteur carré et avec $(p-1) \mid (n-1)$ pour tout facteur premier p de n est un nombre de Carmichael (on pourra utiliser le théorème chinois).

4. Déduire de la question 2 qu'un nombre de Carmichael est toujours impair et possède au moins trois facteurs premiers.

5. Montrer que si pour un entier $k \geq 1$, les nombres $p_1 = 6k+1$, $p_2 = 12k+1$, $p_3 = 18k+1$ sont premiers, alors $p_1 p_2 p_3$ est un nombre de Carmichael. En utilisant cette question, trouver grâce à `Sage` de « grands » nombres de Carmichael.

6. Illustrer les questions 2 et 3 avec le nombre déterminé à la question 1.