Corps finis, cryptographie, tests de primalité

Exercice 1. (Corps finis avec sage - Manipulations de base). Dans `sage`, les corps finis se définissent à l'aide de la commande `GF`.

(1) Calculer les carrés des éléments de $\mathbb{F}_4$.

(2) Calculer les ordres (pour la multiplication) des éléments non nuls de $\mathbb{F}_9$.

(3) La méthode `polynomial` permet d'obtenir le polynôme unitaire et irréductible choisi automatiquement par `sage` pour définir un corps composé. Déterminer le polynôme choisi par `sage` pour définir $\mathbb{F}_4$. Vérifier que ce polynôme est irréductible dans $\mathbb{F}_2[x]$. Factoriser ce polynôme sur $\mathbb{F}_4$. Commenter.

(4) Déterminer la liste des polynômes irréductibles de degré 2 de $\mathbb{F}_2[x]$ et la liste des polynômes irréductibles de degré 3 de $\mathbb{F}_2[x]$. *On pourra utiliser la méthode* `polynomials` *des objets anneaux de polynômes.*

(5) L'option `modulus` de `GF` permet d'imposer un choix de polynôme unitaire irréductible dans la définition d'un corps composé. Définir $\mathbb{F}_8$ en utilisant deux polynômes irréductibles différents.

Exercice 2. (Effet du morphisme de Frobenius sur les racines). Soit $P = x^3 + x^2 + 2x + 1$.

(1) Factoriser P sur $\mathbb{F}_{17}$ et $\mathbb{F}_{289}$.

(2) Quel est l'effet du morphisme de Frobenius sur les racines de P dans $\mathbb{F}_{289}$? Expliquer.

(3) On écrit $\mathbb{F}_{289} = \mathbb{F}_{17}[x]/(Q)$ où $Q = x^2 - x + 3$. On note a la classe du polynôme x dans ce quotient. Déterminer un polynôme unitaire R de degré 3 de $\mathbb{F}_{17}[x]$ tel que 2 et $a+1$ soient des racines de R dans $\mathbb{F}_{289}$. Ce polynôme est-il unique ?

Exercice 3. (Irréductibilité et polynômes de degré 2). Dans cet exercice, on suppose $a \neq 0$.

(1) Soit $P = ax^2 + bx + c \in k[x]$ où k est un corps de caractéristique différente de 2. Montrer que P est irréductible sur k si et seulement si $b^2 - 4ac$ n'est pas un carré de k.

(2) Soit $P = ax^2 + bx + c \in k[x]$ où k est un corps de caractéristique de 2. On suppose $b \neq 0$. Montrer que P est irréductible sur k si et seulement si $x^2 + x + d$ est irreductible sur k pour $d = acb^{-2}$. Si P est réductible, exprimer ses racines en fonction d'une racine de $x^2 + x + d$. Que se passe-t-il si $b = 0$?

Exercice 4. (Sous-corps d'un corps fini). Dans $\mathbb{F}_{531441}$, conjecturer puis vérifier avec `sage` le cardinal des ensembles des racines des polynômes suivants $X^{81} - X$, $X^{729} - X$ et $X^{19683} - X$.

Exercice 5. On considère un corps fini $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où $P \in \mathbb{F}_p[X]$ est irréductible de degré n. On note $x = \overline{X}$. L'élément x est-il toujours un générateur de $\mathbb{F}_q^\times$? Expérimenter avec `sage` (attention, `sage` ne choisit pas ses polynômes irréductibles au hasard pour construire un corps fini).

Exercice 6. Soient $P_1 = X^3+X^2+1$ et $P_2 = X^3+X+1$ des polynômes de $\mathbb{F}_2[X]$. On note $k_1 = \mathbb{F}_2[X]/(P_1)$ et $k_2 = \mathbb{F}_2[X]/(P_2)$. Construire explicitement un isomorphisme de corps entre k_1 et k_2 (on demande une formule explicite et un argument théorique garantissant que la formule est bien un isomorphisme, on pourra utiliser `sage` pour effectuer d'éventuels calculs). Combien y a-t-il de tels isomorphismes ?

Exercice 7 (Factorisation par degré)**.** Soit p un nombre premier et n un entier positif.

(1) En étudiant les orbites des éléments de $\mathbb{F}_{p^n}$ sous l'action du morphisme de Frobenius, redémontrer que $X^{p^n} - X \in \mathbb{F}_p[X]$ est le produit des polynômes unitaires irréductibles de $\mathbb{F}_p[X]$ et dont le degré divise n (on admettra que $X^{p^n} - X$ est sans facteur carré).

(2) Déduire de la propriété précédente un algorithme de factorisation par degrés de complexité $O((\log(p) + \log(n))nM(n))$: un tel algorithme prend un entrée un polynôme sans carré P de degré n de $\mathbb{F}_p[X]$ et renvoie le n-uplet de polynômes $(Q_1, \ldots, Q_n)$ où Q_i est le produit des facteurs irréductibles de P de degré i. Implémenter cet algorithme.

Exercice 8 (Test d'irréductibilité)**.** Soit p un nombre premier et $P \in \mathbb{F}_p[X]$, non constant, de degré n. On rappelle que les assertions suivantes sont équivalentes

— P est irréductible

— $\text{pgcd}(P, X^{p^j} - X) = 1$ pour $j = 1, 2, \ldots, \lfloor n/2 \rfloor$

— $X^{p^n} \equiv X[P]$ et $\mathrm{pgcd}(P, X^{p^{n/i}} - X) = 1$ pour tout premier i divisant n.

(1) En déduire un test d'irreductibilité sur $\mathbb{F}_p$. L'implanter avec `sage`.

(2) Implanter avec `sage` un algorithme probabiliste prenant en entrée un nombre premier p et un entier n et renvoyant un polynôme irréductible unitaire de degré n. Modifier votre algorithme pour renvoyer également le nombre d'essais effectués. Illustrer.

Exercice 9 (Algorithme de Cantor-Zassenhaus)**.** Soit p un nombre premier impair.

(1) Écrire une procédure basée sur l'algorithme de Cantor-Zassenhaus permettant de trouver un facteur non trivial d'un polynôme $P \in \mathbb{F}_p[X]$ produit de polynômes irréductibles deux à deux distincts tous de même degré d (donné en entrée).

(2) Déduire une procédure récursive donnant la factorisation complète d'un polynôme $P \in \mathbb{F}_p[X]$ unitaire non constant, sans facteur carré en produit de ses facteurs irréductibles (on pourra utiliser la factorisation par degré).

Exercice 10 (Crible)**.** Déterminer tous les nombres premiers inférieurs à 10 000 en utilisant un crible.

Exercice 11 (Test de Fermat)**.** Écrire une procédure implémentant le test de primalité de Fermat pour un entier impair n donné. Vérifier expérimentalement que le test de Fermat renvoie la bonne réponse dans plus de la moitié des cas si l'entier n n'est pas un nombre de Carmichael.

Exercice 12 (Nombres de Carmichael)**.**

(1) Écrire un test permettant de déterminer si un entier impair n est un nombre de Carmichael. Tester cette procédure pour les entiers : 663, 867, 935, 1105, 1547, 1729, 2077, 2465, 2647, 2821, 172081.

(2) Soient $p_1 = 6m + 1$, $p_2 = 12m + 1$ et $p_3 = 18m + 1$ trois entiers dont on suppose qu'ils sont premiers pour une certaine valeur de m. Montrer que pour cette valeur de m l'entier $p_1p_2p_3$ est un nombre de Carmichael.

(3) Déterminer les 5 plus petits nombres de Carmichael de la forme donnée à la question précédente (on pourra utiliser `is_prime`).

Exercice 13 (Test de primalité de Rabin–Miller)**.**

(1) Écrire une procédure implémentant le test de primalité de Miller–Rabin pour un entier impair.

(2) Tester cette procédure pour $n = 561$ et $n = 9\,746\,347\,772\,161$. Comparer avec la réponse du test de Fermat.

(3) Écrire un raffinement de la procédure précédente prenant en entrée un entier impair $n \geqslant 1$ et un entier $k \geqslant 1$ et détectant correctement la primalité de n, ou sa non primalité avec probabilité d'erreur inférieure à $1/2^k$.

(4) Comparer les vitesses d'exécution de votre procédure et `is_prime` pour de « grands » entiers impairs.

(5) Écrire un nouveau raffinement du test de primalité de Miller-Rabin qui renvoie également un facteur non trivial de n lorsque c'est possible.

Exercice 14 (Certificat de primalité)**.**

(1) Soit $n > 1$ un entier impair tel que l'on connaisse tous les facteurs premiers de $n - 1$. Montrer que les affirmations suivantes sont équivalentes

(a) n est premier

(b) il existe a tel que $a^{(n-1)} \equiv 1 \pmod{n}$ et $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ pour tout facteur premier q de $n-1$.

(2) Expliquer comment utiliser ce critère pour fournir des informations permettant de vérifier qu'un entier est premier. On parle de *certificat de Pratt*.

(3) Expliciter un certificat de primalité pour 229.

Exercice 15 (Test de Fibonacci)**.** Écrire une procédure implémentant le test de primalité de Fibonacci. On rappelle que ce test est basé sur la propriété suivante : si n est premier, alors

$$u_{n-\epsilon_n} \equiv 0 \pmod{n},$$

où (u_n) est la suite de Fibonacci de condition initiales $u_0 = 0$ et $u_1 = 1$, $\epsilon_n = 1$ quand $n \equiv \pm 1 \pmod{5}$, $\epsilon_n = -1$ quand $n \equiv \pm 2 \pmod{5}$ et $\epsilon_n = 0$ quand $n \equiv 0 \pmod{5}$.

Exercice 16 (RSA)**.**

(1) Écrire une procédure `rsa(p,q)` prenant en entrée deux nombres premiers $p \neq q$ et renvoyant un couple clé publique/clé privée RSA : $(n = pq, e)$, (n, d).

(2) Écrire des procédures `chiffre` et `dechiffre` illustrant le fonctionnement du cryptosystème RSA.