TD n° 1 — Arithmétique

Exercice 1
L'objectif de cet exercice est de rafraîchir votre mémoire arithmétique. Le petit théorème de Fermat affirme que, si p est un nombre premier, alors

$$\forall b \in \mathbb{Z}, \quad b^p \equiv b \pmod{p}.$$

1. Justifier brièvement ce théorème.
2. Montrer, en utilisant ce théorème, que $n = 10^5 + 7$ n'est pas un nombre premier.
3. Retrouver ce résultat en utilisant la commande `isprime` et la commande `ispseudoprime`. Comparer ces deux commandes à l'aide de la documentation.
4. Trouver la décomposition de n en facteurs premiers à l'aide de la commande `factor`.
5. Étudier expérimentalement la réciproque du petit théorème de Fermat, *i.e.* si

   $$\forall b \in \mathbb{Z}, \quad b^n \equiv b \pmod{n}$$

   alors n est un nombre premier.
6. Un **nombre de Carmichael** est un entier n qui n'est pas premier, mais qui satisfait quand même la conclusion du petit théorème de Fermat. Dresser la liste de tous les nombres de Carmichael inférieurs à 10000 à l'aide de gp.

Exercice 2
La **méthode de cryptographie** RSA est devenue un standard dans le monde. Les lettres RSA signifient Rivest-Shamir-Adleman du nom de ses inventeurs, qui l'ont mis au point en 1977. RSA est un algorithme dit « à clef publique » qui sert aussi bien au chiffrement de documents qu'à l'identification.

Le principe d'un algorithme à clef publique est que la méthode pour chiffrer le message est connue de tout le monde, mais qu'une seule personne sait déchiffrer. Dans le cas du codage RSA, tous les agents reçoivent la clef publique, un couple (n, e) où n est un nombre qui est le produit de deux facteurs premiers p et q (très grands en général), et e est un nombre premier à $(p-1)(q-1)$. La clef privée du décodeur est l'entier d tel que $1 < d < (p-1)(q-1)$ et

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

La sécurité de ce code vient du fait qu'il est *a priori* très difficile de trouver la décomposition en facteurs premiers $n = pq$ du nombre n. Par conséquent, il est difficile de déterminer la clef privée (n, d) à partir de la clef publique (n, e).

Le message est exprimé à l'aide des entiers choisis dans $\Sigma = \{0, 1, \ldots, n-1\}$. Pour chiffrer un caractère, on utilise l'application

$$\Theta : \sigma \in \Sigma \mapsto \sigma^e \pmod{n}.$$

Pour déchiffrer, on effectue

$$\Xi : \sigma \in \Sigma \mapsto \sigma^d \pmod{n}.$$

Cette technique est justifiée par le petit théorème de Fermat, qui a la conséquence suivante : pour tout entier x et pour tout entier ℓ,

$$x^{\ell(p-1)(q-1)+1} \equiv x \pmod{n}.$$

Ainsi la propriété $de \equiv 1 \pmod{(p-1)(q-1)}$ garantit que $\Xi \circ \Theta = \mathrm{Id}$.

1. Écrivez une procédure de chiffrement RSA qui chiffre l'entier s avec la clef publique (n, e).
2. Chiffrez le message 1234567890 en utilisant la clef publique $n = 21556703041$ et $e = 7$.
3. Déchiffrez le message 8509780874 en utilisant la clef privée $n = 34675796329$ et $d = 30595937633$.
4. Dans les deux cas précédents, cassez le cryptosystème, *i.e.* retrouvez $\{p, q\}$, d et e.
5. Écrivez une procédure `GenClef` qui génère aléatoirement une clef publique (n, e) et une clef privée (n, d) où n est le produit de deux nombres premiers p, q choisis au hasard parmi les 10^7 premiers nombres premiers et d est choisi uniformément entre 2 et $(p-1)(q-1)-2$.

Exercice 3

L'objectif de cet exercice est de pouvoir manipuler de façon pratique les corps finis et les polynômes à coefficients dans les corps finis.

1. Soit p un nombre premier. On note $\mathbb{F}_p$ le corps fini à p éléments. Pour tout entier $n \geq 1$, on note $\mathbb{F}_{p^n}$ le corps fini à p^n éléments, qui est une extension de degré n de $\mathbb{F}_p$. Tous ces corps sont **uniques à isomorphisme près**.
   (a) Montrer que, pour tout x dans $\mathbb{F}_p$,
   $$x^p = x.$$
   (b) Écrire les tables d'addition et de multiplication de $\mathbb{F}_7$ en s'aidant de gp.
2. Soit $P(X) = X^5 + X^4 + 2X^3 - 2X^2 - 4X - 3$.
   (a) Factoriser P à l'aide de gp dans $\mathbb{C}[X]$ puis dans $\mathbb{Z}[X]$.
   (b) Calculer à l'aide de gp le discriminant de P.
   (c) Factoriser à l'aide de gp ce polynôme dans $\mathbb{F}_2[X]$, $\mathbb{F}_{11}[X]$, $\mathbb{F}_{13}[X]$, $\mathbb{F}_{23}[X]$, $\mathbb{F}_{31}[X]$, $\mathbb{F}_{37}[X]$. Que remarquez-vous ?
3. Montrer que $\mathbb{F}_4$ est isomorphe en tant que corps à
   $$\mathbb{F}_2[X]/(X^2 + X + 1).$$
   Écrire les tables d'addition et de multiplication de ce corps en s'aidant de gp.
4. On cherche à décrire explicitement $\mathbb{F}_8$.
   (a) Soit x dans $\mathbb{F}_8 \setminus \mathbb{F}_2$. Montrer que $\mathbb{F}_8 = \mathbb{F}_2[x]$.
   (b) En déduire que $\mathbb{F}_8$ est isomorphe en tant que corps à $\mathbb{F}_2[X]/(Q(X))$ où $Q(X)$ est le polynôme minimal de x sur $\mathbb{F}_2$. Rappelez les propriétés d'un tel polynôme.
   (c) Combien existe-t-il de polynômes de degré 3 à coefficients dans $\mathbb{F}_2$? Dressez la liste des polynômes de degré 3 à coefficients dans $\mathbb{F}_2$ et $\mathbb{F}_2$-irréductibles en s'aidant de gp.

(d) En déduire que $\mathbb{F}_8$ est isomorphe en tant que corps à

$$\mathbb{F}_2[X]/(X^3+X+1) = \mathbb{F}_{8,1}$$

et à

$$\mathbb{F}_2[X]/(X^3+X^2+1) = \mathbb{F}_{8,2}.$$

(e) Écrire les tables d'addition et de multiplication de $\mathbb{F}_{8,1}$ et $\mathbb{F}_{8,2}$ en s'aidant de gp.

(f) Soit α une racine de X^3+X+1. Montrer à l'aide de gp que α^2 et α^4 sont les autres racines de X^3+X+1. Montrer également à l'aide de gp que α^3, α^5 et α^6 sont les racines de X^3+X^2+1.

(g) Écrire un isomorphisme explicite entre $\mathbb{F}_{8,1}$ et $\mathbb{F}_{8,2}$.

5. Soient p un nombre premier et $Q(X)$ un polynôme à coefficients dans $\mathbb{F}_p$, de degré $n \geqslant 1$ et $\mathbb{F}_p$-irréductible.

(a) Montrer que $\mathbb{F}_p[X]/(Q(X))$ est le corps fini de cardinal $q = p^n$, noté $\mathbb{F}_q$.

(b) Montrer que pour tous x et y dans $\mathbb{F}_q$ et pour tout entier naturel t,

$$(x+y)^{p^t} = x^{p^t} + y^{p^t}.$$

(c) En déduire que l'application

$$\begin{array}{rccc} \mathrm{Frob}_p : \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & x^p \end{array}$$

est un automorphisme [1] de $\mathbb{F}_q$, dont l'ensemble des points fixes est exactement $\mathbb{F}_p$.

(d) En déduire que pour tout élément x de $\mathbb{F}_q$ et tout entier naturel t,

$$(Q(x))^{p^t} = Q\left(x^{p^t}\right).$$

(e) En déduire également que si α est une racine de $Q(X)$ alors les autres racines de $Q(X)$ sont $\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$.

6. Comment trouver un polynôme à coefficients dans $\mathbb{F}_p$, de degré $n \geqslant 1$ et $\mathbb{F}_p$-irréductible ?

(a) Écrire une procédure permettant de tirer aléatoirement un polynôme de degré n à coeffcients dans $\mathbb{F}_p$.

(b) Tester l'irréductibilité d'un tel polynôme de plusieurs façons.

(c) Donner une estimation du nombre d'essais à faire par rapport à n pour que le polynôme aléatoire fourni par la procédure précédente soit $\mathbb{F}_p$-irréductible.

7. Tester sur des gros exemples tout ce qui a été vu dans cet exercice *i.e.* $n > 10^3$ et/ou $p > 10^{10}, 10^{100}$. Qu'en pensez-vous ?

1. Frob_p est le **morphisme de Frobenius** de $\mathbb{F}_q$