# feuille de TD/TP 1

Polynômes irréductibles sur les corps finis

Un polynôme de $\mathbb{F}_p[X]$ ($p$ premier) de degré $n$ est dit *primitif* s'il est irréductible et s'il est le polynôme minimal d'une racine primitive de l'unité dans $\mathbb{F}_{p^n}$. Dit autrement $P \in \mathbb{F}_p[X]$ est primitif s'il est irréductible et si le plus petit $r$ tel que $X^r \equiv 1 \mod P$ est $r = p^n - 1$, l'ordre du groupe $\mathbb{F}_{p^n}^*$.

Le *polynôme réciproque* d'un polynôme $P(X) = \sum_{i=0}^{n} a_i X^i$ de degré $n$, est le polynôme $P^*(X) = \sum_{i=0}^{n} a_{n-i} X^i$, et donc $P^*(X) = X^n P(\frac{1}{X})$. On a $P^{**} = P$ si le coefficient constant de $P$ est non nul ($P$ et $P^*$ de même degré).

**Exercice 1.**

**1.** Montrer que si $X \not| P$, le polynôme $P$ est irréductible, resp. primitif, si et seulement si son polynôme réciproque $P^*$ est irréductible, resp. primitif.

**2.** Calculer le nombre de polynômes primitifs de degré $n$ sur $\mathbb{F}_p$ (utiliser la fonction $\varphi$ d'Euler).

**3.** Montrer que le polynôme $\sum_{i=0}^{n} X^i$ ($n \geq 1$) de $\mathbb{F}_2[X]$ n'est primitif que si $n = 1$ ou $n = 2$.

**4.** Déterminer tous les polynômes irréductibles et primitifs de degré 2, 3 et 4 sur $\mathbb{F}_2$.

**5.** Montrer que tous les polynômes irréductibles de degré 5 sur $\mathbb{F}_2$ sont primitifs. Les déterminer.

**Exercice 2 (Un algorithme pour l'irréductibilité).** Soit $q$ un nombre premier, $n$ un entier naturel strictement positif, et $P$ un polynôme unitaire à coefficients dans $\mathbb{F}_q$. Le polynôme $X^{q^n} - X$ est à coefficients dans $\mathbb{F}_q$. On pose $\mathrm{K} = \mathbb{F}_q[X]/(P)$.

**1.** Montrer que si $P$ est irréductible de degré $d$, et si $d \mid n$, alors tout élément de K est racine de $X^{q^n} - X$ et en déduire que $P \mid X^{q^n} - X$.

**2.** Montrer que si l'entier naturel strictement positif $d$ est tel que $q^d - 1$ divise $q^n - 1$ alors $d$ divise $n$.

**3.** Montrer que si le polynôme $P$ est irréductible de degré $d$ et divise $X^{q^n} - X$, alors tout élément de K est racine de ce polynôme. En déduire que $d$ divise $n$.

**4.** Montrer que $X^{q^n} - X$ n'a pas de facteur multiple.

**5.** En déduire que dans $\mathbb{F}_q[X]$, $X^{q^n} - X$ est exactement le produit de tous les polynômes unitaires irréductibles dont le degré divise $n$.

**6.** En déduire qu'un polynôme $P$ de degré $n$ de $\mathbb{F}_q[X]$ est irréductible si et seulement si :

**a.** $P \mid X^{q^n} - X$ ;

**b.** pour tout diviseur premier $p$ de $n$, $P$ et $X^{q^{n/p}} - X$ sont premiers entre eux.

Proposer un algorithme dans le cas $q = 2$ pour décider si un polynôme de degré $n$ est irréductible, et évaluer sa complexité.

**7.** Soit $m_n(q)$ le nombre de polynômes irréductibles de degré $n$ sur $\mathbb{F}_q$. Montrer que :

$$q^n = \sum_{d|n} d\, m_d(q)$$

et en déduire que :

$$\frac{q^n - q^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq m_n(q) \leq \frac{q^n}{n}$$

puis que pour $n$ assez grand, parmi les polynômes de degré $n$, environ un sur $n$ est irréductible.

On déduit de l'inégalité précédente qu'il existe un polynôme irréductible sur $\mathbb{F}_p$, $p$ premier, et donc l'existence d'un corps fini de cardinal $p^n$, comme corps de rupture de ce polynôme sur $\mathbb{F}_p$.

**8.** La fonction $\mu$ étant la fonction de Möbius, montrer que :

$$m_n(q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

**9.** Montrer que $P$ est un polynôme primitif de degré $n$ de $\mathbb{F}_q[X]$ si et seulement s'il vérifie, en plus des deux conditions précédentes :

**c.** Pour tout diviseur premier $p$ de $q^n - 1$, $P \not| X^{\frac{q^n-1}{p}} - 1$.

Cette condition est en général beaucoup plus lourde à vérifier, que celles du test d'irréductibilité on doit calculer l'ensemble des diviseurs premiers de $q^n - 1$.

**Exercice 3.** Le but de cet exercice est de faire fonctionner les algorithmes de l'exercice précédent sur des exemples. Organisez vos calcul de façon efficace, par exemple en base 2 on peut utiliser que :

$$X^{\sum_{i=1}^{k} a_i 2^i} = \prod_{i=1}^{k} \left(X^{2^i}\right)^{a_i} = \prod_{1 \leq i \leq k,\ a_i \neq 0} X^{2^i}, \quad a_i \in \{0, 1\}$$

et $X^{2^i}$ se calcule par $i$ élévations au carré successives. Montrer que dans $\mathbb{F}_2[X]$ :

1. $X^6 + X + 1$ est irréductible et primitif ;
2. $P_{AES} = X^8 + X^4 + X^3 + X + 1$ (polynôme de l'AES) est irréductible, mais pas primitif.

**Exercice 4.**
1. Calculer $X^9$ modulo $1 + X^3 + X^6$. Le polynôme $1 + X^3 + X^6$ est-il irréductible ? Est-il primitif ?
2. Déterminer tous les polynômes primitifs de degré 6 dont 3 coefficients sont non nuls.
3. Calculer $X^{21}$ modulo $1 + X + X^2 + X^4 + X^6$. Ce polynôme est-il irréductible ? Est-il primitif ?

**Exercice 5.** Un nombre de Mersenne est un nombre de la forme $2^m - 1$ avec $m$ premier. Un exposant de Mersenne est un nombre $m$ tel que $2^m - 1$ est un nombre de Mersenne premier.

1. Montrer que $m$ est un exposant de Mersenne si et seulement si $2^m - 1$ est premier.
2. Soit $\mathbb{F}_2$ le corps à deux éléments. Montrer que si $m$ est un exposant de Mersenne, tous les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré $m$ sont primitifs (et réciproquement).
3. Combien y-a-t-il de polynômes primitifs de $\mathbb{F}_2[X]$ de degré $m$ si ce dernier est un exposant de Mersenne ?
4. Montrer que si $m$ est un exposant de Mersenne, le polynôme $P$ de degré $m$ est primitif si et seulement si $X^{2^{m-1}} \equiv 1 \mod P$.
5. Application : vérifier que 7 est un exposant de Mersenne. Combien y-a-t-il de polynômes primitifs de degré 7 ? Vérifier que $X^7 + X + 1$ est un polynôme primitif.

   Montrer qu'un polynôme primitif de degré 7 possède 3, 5 ou 7 coefficients non nuls, et qu'il en existe bien dont exactement 5 coefficients sont non nuls.

## Calcul sur les corps finis de caractéristique 2

Vous avez à réaliser en C une petite bibliothèque pour le calcul dans les corps finis de caractéristique 2. Les polynômes sur F2 de degré au plus 63 sont représentés par des entiers de 64 bits, chaque bit de poids $i$ étant le coefficient du monôme de même poids. par exemple `0x65` représente le polynôme $X^7 + X^5 + X^2 + 1$. Le corps fini $\mathbb{F}_{2^n}$ est vu comme le quotient $\mathbb{F}_2[X]/(P)$, où $P$ est un polynôme irréductible de degré $n$, ses éléments sont représentés de façon univoque par des polynômes de degré au plus $n-1$.

Les calculs se font grâce aux opérations bit à bit, en particulier si le polynôme $P$ est représenté par l'entier machine `P` :
— le xor (`^`) donne la somme de deux polynômes ;
— `P&(1<<i)` donne le coefficient de degré $i$ de $P$ ;
— le décalage à gauche (`P <<= n`) donne $X^n P$ (s'il n'y a pas de débordement) ;
— le décalage à droite (`P >>= n`) donne le quotient de $P$ par $X^n$

Les opérations de multiplication et de division peuvent se réaliser par des algorithmes analogues à ceux de l'école primaire (avec seulement 2 chiffres 0 et 1 et sans retenue !).

**Exercice 6.** Décrire des algorithmes linéaires (en la taille, soit le degré des entrées !) pour :

1. la multiplication de deux polynômes $P$ et $Q$ (sans tenir compte des débordements) ;
2. la division euclidienne d'un polynôme de $P$ par un polynôme $Q$ ;
3. la multiplication de deux polynômes $P$ et $Q$ modulo un polynôme $M$ (sans débordement). Sachant que $\deg(P) < \deg(M)$ le calcul du reste de la dvision de $X \cdot P$ par $M$ demande un test et au plus une addition polynomiale.

**Exercice 7.** Déduire de l'estimation du nombre de polynômes irréductibles et de polynômes primitifs de degré donné que l'on a un algorithme « raisonnable » pour produire aléatoirement un polynôme irréductible ou un polynôme primitif de degré donné.

Un fichier `f2_poly.h` est distribué, qui détaille les fonctions à réaliser. Toutes doivent être testées. Le produit et l'élévation à la puissance sont à réaliser modulo un polynôme donné, cas où les questions de débordement se gèrent simplement, et qui fournit le calcul.

Les tests d'irréductibilité et de primitivité doivent être implémentés de façon suffisamment efficace pour que par exemple le calcul de tous les polynômes irréductibles de degré $n$ soit très rapide, voire quasi-instantané pour $n = 20$), de même pour les polynômes primitifs (bien que l'algorithme soit moins efficace).

Une façon de vérifier les tests d'irréductibilité et de primitivité est de compter à l'aide de ces tests le nombre de polynômes irréductibles et de polynômes primitifs d'un degré donné. Ces nombres se calculent plus rapidement à l'aide de la fonction de Möbius pour les polynômes irréductibles (voir la formule démontrée à l'exercice 2), et de la fonction d'Euler pour les polynômes primitifs (voir exercice 1).

Vous pouvez utiliser le logiciel `Sage` pour les calculs utilisant ces deux fonctions (la fonction indicatrice d'Euler se note `euler_phi`, la fonction de Möbius `moebius`), ou bien calculer directement ces fonctions en C.