Master CSI 2 2013-2014

Cryptanalyse — M1MA9W06
Responsable : G. Castagnos

Rappels sur les corps finis

On donne quelques rappels rapides sans démonstration.

Définition 1 (caractéristique d'un anneau $(A, +, \times)$ d'unité 1 $(1 \times a = a)$)**.** Soit

$$\Phi : \begin{array}{ccc} \mathbf{N} & \to & A \\ n & \mapsto & 1+1+1+\ldots 1 \; (n \text{ fois}) \end{array}$$

On note Car(A) le plus petit n, s'il existe, tel que $\Phi(n) = 0$. Sinon Car(A) $= 0$. On a par exemple $\mathrm{Car}(\mathbf{Z}) = \mathrm{Car}(\mathbf{Q}) = 0$).

Soit K un corps fini, c'est à dire que K a un nombre fini d'éléments et c'est un anneau (unitaire, commutatif) tel que tous les éléments non nuls sont inversibles : $K^* = K \setminus \{0\}$ est un groupe pour $\times$ appelé groupe multiplicatif. La caractéristique Car(K) est un nombre premier.

Proposition 1. Soit K un corps fini de caractéristique p premier. K a nécessairement $q = p^n$ éléments, pour $n \geqslant 1$. K contient $\mathbf{Z}/p\mathbf{Z}$ appelé le sous-corps premier de K. K est un espace vectoriel de dimension n sur $\mathbf{Z}/p\mathbf{Z}$.

Il existe donc une base de n éléments de K, $(e_1, \ldots, e_n)$ telle que pour tout x dans K il existe un unique $(\alpha_1, \ldots, \alpha_n)$ dans $\mathbf{Z}/pZ$ tel que

$$x = \sum_{i=1}^{n} \alpha_i e_i.$$

Réciproquement, pour tout nombre premier p et tout $n \geqslant 1$, $q = p^n$, il existe un corps fini et un seul (à isomorphisme près) à q éléments. On le note $\mathbf{F}_q$, ou GF(q).

Remarque 1. Soit $\mathbf{F}_q$ un corps fini avec $q = p^n$, alors on a $(x+y)^p = x^p + y^p$ pour tout $x, y \in \mathbf{F}_q$. L'application $f : x \mapsto x^p$ est un automorphisme dit de Frobenius : $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et f est une bijection. Les éléments tels que $f(x) = x$ sont exactement les éléments de $\mathbf{F}_p \subset F_q$.

Réalisation

Soit P un polynôme irréductible (c'est à dire qu'il n'a pas d'autres diviseurs que les constantes et lui même fois une constante) à coefficients dans $\mathbf{F}_p$ de degré n, $\mathbf{F}_p[X]/(P(X))$ est un corps avec $q = p^n$ éléments.

Réciproquement, pour tout p premier, et $n \geqslant 1$, $q = p^n$ il existe un polynôme P irréductible de degré n sur $\mathbf{F}_p$ permettant de construire $\mathbf{F}_q$ comme $\mathbf{F}_p[X]/(P(X))$.

En pratique plusieurs P sont possibles et donnent des représentations différentes (mais isomorphes) de $\mathbf{F}_q$. On choisit un polynôme P qui rend l'arithmétique plus performante.

On note $\alpha = X \pmod{P(X)}$, $\alpha \in \mathbf{F}_q$ par identification de $\mathbf{F}_q$ et $F_p[X]/(P(X))$. On a $P(\alpha) = 0$. La famille $(1, \alpha, \alpha^2, ..., \alpha^{n-1})$ est une base de $\mathbf{F}_q$ vu comme espace vectoriel sur $\mathbf{F}_p$.

En Sage si `F` est un corps fini, `V=F.vector_space()` définit l'espace vectoriel correspondant au corps fini `F`, et si `a` est un élément de `F`, `V(a)` renvoie les coordonnées de `a` dans la base de `V`. Réciproquement, si `v` est un vecteur, `F(v)` renvoie l'élément de `F` correspondant.

Ordres

Si β est un élément non nul de $\mathbf{F}_q$, on a $\beta^{q-1} = 1$: car $q-1$ est l'ordre (le cardinal) du groupe multiplicatif $\mathbf{F}_q^*$. L'ordre de β est le plus petit entier e tel que $\beta^e = 1$. Cet ordre e divise $q-1$ (c'est le théorème de Lagrange, e étant aussi l'ordre du sous-groupe engendré par β).

Si e divise $q-1$, il y a $\phi(e)$ éléments (indicatrice d'Euler) d'ordre e. En particulier, il existe $\phi(q-1)$ éléments d'ordre $q-1$: ce sont les générateurs de $\mathbf{F}_q^*$, on les appelle éléments primitifs et on dit que $\mathbf{F}_q^*$ est cyclique (d'ordre $q-1$). Si $\alpha \in F_q$ est primitif, on a alors $\mathbf{F}_q$ constitué de $0, \alpha, \alpha^2, ... \alpha^{q-1} = 1$: c'est une autre représentation possible plus adaptée pour faire des multiplications mais pas des additions.

Remarque 2. Si β est d'ordre e, alors β^i $(1 \leqslant i \leqslant e)$ est d'ordre $\operatorname{ppcm}(e,i)/i$. En particulier les éléments d'ordre e sont les β^i tels que $\operatorname{pgcd}(e,i) = 1$ (on a alors $\operatorname{ppcm}(e,i) = e \times i$). On en a bien $\phi(e)$.

Polynôme minimal

Soit $\beta \in F_q^\times$, $q = p^n$, le polynôme P unitaire de plus petit degré sur $\mathbf{F}_p$ tel que $P(\beta) = 0$ est son polynôme minimal. Il est irréductible sur $\mathbf{F}_p$.

Si P est irréductible de degré n sur $\mathbf{F}_p$ et α est racine de P alors ses racines sont les conjugués de α par l'action du Frobenius, c'est à dire : $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$. De plus toutes les racines ont le même ordre.

Le polynôme minimal d'un élément primitif est dit primitif (toutes ces racines sont donc primitives).

Les sous-corps de $\mathbf{F}_p^n$ sont les $\mathbf{F}_p^s$ où $s \mid n$. Les éléments de $\mathbf{F}_p^s$ sont les racines de $X^{p^s} - X$.