Rappels : Pour tout naturel q, il existe un corps fini ayant q éléments *si et seulement si* q s'écrit de la forme p^d avec p un nombre premier et $d \geq 1$; dans ce cas, le corps en question est unique à isomorphisme près et on le note $\mathbb{F}_q$: il est de caractéristique p et a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ comme corps premier, sur lequel il est de degré d. Le corps $\mathbb{F}_q$, avec $q = p^d$, peut être vu comme un sous-corps de $\mathbb{F}_{q'}$, avec $q' = p'^{d'}$, si et seulement si $p' = p$ et $d|d'$, auquel cas ce sous-corps est unique (et $\mathbb{F}_q$ se voit comme l'ensemble des racines du polynôme $t^q - t$ dans $\mathbb{F}_{q'}$; inversement, $\mathbb{F}_{q'}$ se voit comme un corps de décomposition de $t^{q'} - t$ dans $\mathbb{F}_q$). Le groupe multiplicatif $\mathbb{F}_q^\times$ de $\mathbb{F}_q$ — comme tout groupe multiplicatif fini d'un corps — est cyclique, c'est le groupe des racines $(q-1)$-ièmes de l'unité dans $\mathbb{F}_q$. Le groupe des automorphismes de $\mathbb{F}_{q'}$ laissant fixe $\mathbb{F}_q$, ou groupe de Galois de $\mathbb{F}_{q'}$ sur $\mathbb{F}_q$, est cyclique d'ordre d'/d engendré par le frobenius « élévation à la puissance q », soit $\mathrm{Fr}_q\colon x \mapsto x^q$. Pour tout élément x de $\bar{\mathbb{F}}_q$ il existe un plus petit d tel que $x \in \mathbb{F}_{q^d}$, qui divise tous les autres, et ce d s'appelle le degré de x sur $\mathbb{F}_q$ — c'est aussi l'ordre de Fr_q opérant sur x (c'est-à-dire le cardinal de l'orbite) et c'est aussi le degré de l'unique polynôme irréductible unitaire sur $\mathbb{F}_q$ dont x est racine (le polynôme minimal de x, dont les autres racines sont justement l'orbite de x par Galois).

1. Soit $q = p^d$ (où p est un nombre premier et $d \geq 1$) et soit $k \geq 1$ un entier naturel. Le nombre de polynômes unitaires de degré k dans $\mathbb{F}_q$ est manifestement q^k. Montrer que le nombre de polynômes unitaires de degré k sur $\mathbb{F}_q$ qui sont irréductibles est

$$\frac{1}{k} \sum_{\ell | k} \mu(\ell)\, q^{k/\ell}$$

où ℓ parcourt les diviseurs de k et $\mu(\ell)$ désigne la fonction de Möbius[1]. (Indication : compter les éléments de $\mathbb{F}_{q^k}$ en fonction de leur degré sur $\mathbb{F}_q$, ou bien regarder les orbites par l'action du groupe de Galois $G = \langle \mathrm{Fr}_q \rangle$ sur $\mathbb{F}_{q^k}$.) On dit qu'un tel polynôme est *primitif* lorsque, de plus, une de ses racines (et donc n'importe laquelle de ses racines) est un générateur du groupe multiplicatif $\mathbb{F}_{q^k}^\times$: montrer que le nombre de polynômes unitaires irréductibles de degré k sur $\mathbb{F}_q$ qui sont primitifs est

$$\frac{1}{k}\, \phi(q^k - 1)$$

où $\phi(n)$ désigne la fonction indicatrice d'Euler[2]. Calculer ces valeurs pour $q = 2$ et $k = 6$.

2 (test d'irréductibilité de Rabin). Soit $f \in \mathbb{F}_q[t]$ un polynôme de degré k à coefficients dans $\mathbb{F}_q$. Montrer que f est irréductible si et seulement si il vérifie les deux conditions suivantes : (a) f divise $t^{q^k} - t$, et (b) f est premier à $t^{q^\ell} - t$ pour tout diviseur strict ℓ de k. (On signalera si oui ou non il est nécessaire de mettre les deux conditions.) Expliquer pourquoi ceci fournit un algorithme efficace permettant de déterminer si f est irréductible (en supposant qu'on sache déjà faire des calculs dans $\mathbb{F}_q$) ; puis expliquer pourquoi la connaissance d'un tel algorithme permet de faire des calculs dans $\mathbb{F}_{p^k}$.

3 (théorème de Chevalley-Warning). Soit $\mathbb{F} = \mathbb{F}_q$ un corps fini (de caractéristique p), et $f \in \mathbb{F}[X_0, \ldots, X_n]$ un polynôme homogène de degré $d > 0$ en $n+1$ variables avec $d \leq n$: on cherche à montrer que f a un zéro non trivial (c'est-à-dire autre que $(0, \ldots, 0)$). (En termes géométriques : une hypersurface de degré $d \leq n$ dans $\mathbb{P}^n$ sur un corps fini $\mathbb{F}$ a toujours un point sur $\mathbb{F}$.) Pour cela, on montrera que le nombre de zéros de f dans $\mathbb{F}^{n+1}$ est multiple de p, en considérant la somme des $f(x_0, \ldots, x_n)^{q-1}$ où $(x_0, \ldots, x_n)$ parcourt tous les $(n+1)$-uplets d'éléments de $\mathbb{F}$.

([1]) Soit $\mu(n) = 0$ si n est divisible par un carré et $\mu(n) = (-1)^s$ sinon, avec s le nombre de facteurs premiers — évidemment distincts — de n.
([2]) Soit $\phi(n) = \mathrm{card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

4 (« petit » théorème de Wedderburn). Soit D une algèbre à divisions (= corps gauche) finie (de cardinal fini). On se propose de montrer que D est, en fait, un corps. Soit $\mathbb{F}$ le centre de D (c'est-à-dire l'ensemble des $x \in D$ tels que $(\forall y \in D)(xy = yx)$), qui est un corps fini, et q son cardinal, et soit n la dimension de D comme $\mathbb{F}$-espace vectoriel. Écrire l'équation aux classes pour l'action de $D^\times$ sur lui-même par conjugaison. En notant $\Phi_n \in \mathbb{Z}[t]$ le n-ième polynôme cyclotomique, en déduire que $\Phi_n(q)$ divise $q - 1$. Obtenir une contradiction si $n > 1$ en prouvant que $|\Phi_n(q)| > q - 1$.

5 (loi de réciprocité quadratique). Si p est un nombre premier impair, et n un entier non multiple de p (ou un élément de $\mathbb{F}_p^\times$), on définit le symbole de Legendre $\left(\frac{n}{p}\right)$ comme $+1$ si n est un carré dans $\mathbb{F}_p$, et -1 sinon. Remarquer que $\left(\frac{mn}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p}\right)$ et que $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod p$. Soient maintenant p et q deux nombres premiers impairs distincts, et soit ζ une racine primitive p-ième de l'unité dans une extension de $\mathbb{F}_q$. Posons $S = \sum_{x\in\mathbb{F}_p^\times} \left(\frac{x}{p}\right) \zeta^x \in \mathbb{F}_q$: montrer que $S^2 = \left(\frac{-1}{p}\right) p$ et que $S^q = \left(\frac{q}{p}\right) S$. En déduire la *loi de réciprocité quadratique* :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

6 (bracelets de De Bruijn). On appelle *bracelet de De Bruijn* d'ordre $k \geq 1$ sur un alphabet (ensemble) fini A à $q \geq 1$ éléments une application b de $\mathbb{Z}/q^k\mathbb{Z}$ vers A telle que pour tout k-uplet $(a_0, \ldots, a_{k-1})$ d'éléments de A il existe un $i \in \mathbb{Z}/q^k\mathbb{Z}$ (manifestement unique) pour lequel $a_0 = b(i)$, $a_1 = b(i + 1)$ et ainsi de suite jusqu'à $a_{k-1} = b(i + k - 1)$. Autrement dit, il s'agit d'un bracelet de longueur q^k sur les q perles de l'alphabet, qui contient toute combinaison possible de k perles consécutives. On se propose de montrer que pour tout k et tout q il exite un bracelet de De Bruijn.

(1) Dans le cas où $q = p^d$ est une puissance d'un nombre premier p, montrer en utilisant le corps fini $\mathbb{F}_{q^k}$ qu'il existe un bracelet de De Bruijn. On pourra considérer g un générateur du groupe multiplicatif $\mathbb{F}_{q^k}^\times$ et décomposer les g^i dans la base $1, g, \ldots, g^{k-1}$ de $\mathbb{F}_{q^k}$ sur $\mathbb{F}_q$. (Commencer par obtenir un « presque » bracelet de De Bruijn, de longueur $q^k - 1$, qui contient toutes combinaison de k perles sauf une.)

(2) Comment peut-on obtenir un bracelet de De Bruijn lorsque q n'est pas une puissance d'un nombre premier mais un produit de telles puissances (c'est-à-dire un entier naturel non nul quelconque) ?