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 à la puissance d, soit $\mathrm{Fr}^d : x \mapsto x^q$.

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 $G = \langle \mathrm{Fr}^d \rangle$ 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 (théorème de Chevalley-Warning). Soit $\mathbb{F} = \mathbb{F}_q$ un corps fini (de caractéristique p), et $P \in \mathbb{F}[X_0, \ldots, X_n]$ un polynôme homogène de degré $d > 0$ en $n+1$ variables avec $d \leq n$: on cherche à montrer que P 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 P dans $\mathbb{F}^{n+1}$ est multiple de p, en considérant la somme des $P(x_0, \ldots, x_n)^{q-1}$ où $(x_0, \ldots, x_n)$ parcourt tous les $(n+1)$-uplets d'éléments de $\mathbb{F}$.

3 (« 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 $|\Phi_n(q)| > q - 1$.

4 (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

([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 $\phi(n) = \mathrm{card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

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* :

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

5 (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) ?

6 (addition et multiplication de Conway). Lorsque E est un ensemble d'entiers naturels (non égal à $\mathbb{N}$ tout entier), on notera $\operatorname{mex} E = \min(\mathbb{N} \setminus E)$ le plus petit naturel qui n'est pas dans E. On définit par récurrence des opérations binaires $\#$ et $@$ sur $\mathbb{N}$ (et à valeurs dans $\mathbb{N}$), appelées respectivement somme de Conway et produit de Conway (ou somme de nim et produit de nim), en posant :

$$a\#b = \operatorname{mex}(\{a'\#b : a' < a\} \cup \{a\#b' : b' < b\})$$

$$a@b = \operatorname{mex}\{(a'@b)\#(a'@b')\#(a@b') : a' < a \text{ et } b' < b\}$$

(†) Montrer successivement, par des récurrences : que $\#$ est commutative, que $a\#0 = a$ pour tout naturel a, que $a\#b = 0$ si et seulement si $a = b$, que $\#$ est associative (supposer $e < a\#(b\#c)$ et prouver $e \neq (a\#b)\#c$ par exemple), que $@$ est commutative, que $a@0 = 0$ pour tout naturel a, que $a@1 = a$ pour tout naturel a, que $@$ est distributive sur $\#$, que $@$ est associative, et que $a@b = 0$ si et seulement si $a = 0$ ou $b = 0$. Expliquer comment l'écriture binaire de $a\#b$ (c'est-à-dire son unique décomposition en puissances de 2 distinctes) se calcule à partir de celles de a et de b. Calculer $2^{2^r}@2^{2^s}$ pour $r \neq s$ et $2^{2^r}@2^{2^r}$ et prouver que l'ensemble des entiers naturels entre 0 et $2^{2^r} - 1$ est stable par les lois $\#$ et $@$ et forme un corps (isomorphe, donc, à $\mathbb{F}_{2^{2^r}}$).

On considère le jeu suivant, appelé jeu de nim de dimension 2 : un damier rectangulaire de dimensions arbitraires est complètement rempli de pions, blancs d'un côté et noirs de l'autre (de sorte qu'une et une seule de ces couleurs est visible pour chaque pion), dans une certaine configuration initiale (non précisée). Chacun des deux joueurs, à son tour, doit retourner un pion de façon à le faire passer de noir à blanc, et il peut aussi retourner (quelle que soit sa couleur à ce moment-là) un pion quelconque plus haut dans la même colonne, ou un pion quelconque plus à gauche dans la même ligne, ou encore les deux à la fois à condition dans ce cas de retourner aussi le quatrième sommet du rectangle défini par les trois pions retournés. Le jeu se termine quand tous les pions sont blancs, de sorte que le joueur dont c'est le tour ne peut plus jouer, et ce joueur a alors perdu. Montrer que le jeu se termine toujours en temps fini, et que le second joueur a une stratégie gagnante si et seulement si la somme de Conway des $a@b$ est nulle, où (a, b) parcourt tous les couples ligne/colonne (comptées à partir de 1) où le pion est noir.

(‡) Montrer que, si on étend les lois $\#$ et $@$ à des ordinaux quelconques avec exactement les même définitions ($\operatorname{mex} E$ signifiant : le plus petit ordinal n'appartenant pas à E) alors ω^ω est stable pour les lois $\#$ et $@$ et est une clôture algébrique de $\mathbb{F}_2$. Tout cardinal régulier indénombrable est également stable pour les lois en question et est un corps algébriquement clos de caractéristique 2, et l'ordinal ω^ω est le plus petit transcendant.

Motivations : L'exercice 1 est classique et à connaître. Il faut d'ailleurs remarquer la similarité entre le fait que la fraction des polynômes unitaires de degré k sur $\mathbb{F}_q$ qui sont irréductible soit environ $\frac{1}{k}$ et le théorème classique des nombres premiers. L'exercice 2 est lui aussi un grand classique. Il exprime le fait, dans la terminologie introduite par Lang, que les corps finis sont des corps C_1. Le théorème 3 n'est pas moins classique. Il exprime le fait que le groupe de Brauer d'un corps fini est nul. En principe, il devrait être possible de déduire directement un résultat de l'autre (tout corps C_1 a un group de Brauer nul), mais, en pratique, cela donne une démonstration probablement plus compliquée. L'exercice 4 est ultra-classique, et Gauß (qui en a trouvé pas moins de douze démonstrations différentes) l'appelait le « théorème d'or ». L'exercice 5 n'est pas très classique, mais il est amusant. L'exercice 6 n'est pas classique du tout, c'est un craquage de ma part. On trouvera tout plein de choses dans cette ligne d'idées dans le livre *On Numbers and Games* de J. H. Conway.