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 $k = 6$.

Corrigé. Commençons par une observation : si $f \in \mathbb{F}_q[t]$ est un polynôme irréductible à coefficients dans $\mathbb{F}_q$, disons unitaire de degré k, alors il est complètement décomposé sur son corps de rupture $\mathbb{F}_{q^k}$ (i.e. : dès qu'il acquiert une racine, il les acquiert toutes) ; ceci découle immédiatement de l'unicité de $\mathbb{F}_{q^k}$ dans n'importe quel corps le contenant (autrement dit, n'importe quel élément algébrique de degré k sur $\mathbb{F}_q$, et en particulier toute racine de f, engendre le même corps $\mathbb{F}_{q^k}$).

Si f est un polynôme irréductible de degré k sur $\mathbb{F}_q$, ses racines dans $\mathbb{F}_{q^k}$ sont au nombre de k exactement (elles sont un ensemble de conjugués, c'est-à-dire une orbite pour l'action du groupe de Galois $G = \langle \mathrm{Fr}_q \rangle$ sur $\mathbb{F}_{q^k}$). De plus, tout élément de $\mathbb{F}_{q^k}$ qui est de degré précisément k sur $\mathbb{F}_q$, c'est-à-dire n'est pas dans un $\mathbb{F}_{q^{k_1}}$ pour $k_1 < k$ (diviseur strict), est racine d'un unique polynôme unitaire irréductible de degré k sur $\mathbb{F}_q$. Ainsi, si $M(\ell)$ désigne le nombre d'éléments de $\mathbb{F}_{q^k}$ (ou de $\mathbb{F}_{q^\ell}$) de degré ℓ sur $\mathbb{F}_q$, le nombre de polynômes unitaires irréductibles de degré k sur $\mathbb{F}_q$ est $\frac{1}{k} M(k)$, et on a $q^k = \sum_{\ell|k} M(\ell)$ (pour tout entier naturel non nul k).

On voit alors que le nombre $M(k)$ d'éléments de degré exactement k sur $\mathbb{F}_q$ est égal à q^k moins les $M(k/\ell)$ pour ℓ diviseur premier de k : c'est-à-dire q^k moins $q^{k/\ell}$ pour tout ℓ diviseur premier de k plus $q^{k/\ell\ell'}$ pour ℓ, ℓ' diviseurs premiers distincts de k (car on a décompté deux fois ces éléments) plus, etc., ce qui est la formule annoncée. Plus rigoureusement, comme

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

$q^k = \sum_{\ell|k} M(\ell)$, en appliquant la formule d'inversion de Möbius, on a $M(k) = \sum_{\ell|k} \mu(\ell)\, q^{k/\ell}$, d'où le résultat.

Enfin, le nombre de générateurs du groupe $\mathbb{F}_{q^k}^\times$ à $q^k - 1$ éléments est $\phi(q^k - 1)$. N'importe lequel de ces générateurs est de degré exactement k sur $\mathbb{F}_q$ (car s'il est dans un $\mathbb{F}_{q^{k_1}}$ pour $k_1 < k$ il est d'ordre multiplicatif au mieux $q^{k_1} - 1$). Le nombre de polynômes unitaires irréductibles primitifs de degré k est donc bien $\frac{1}{k}\,\phi(q^k - 1)$.

Pour $q = 2$ et $k = 6$, il y a $2^6 = 64$ polynômes unitaires de degré k sur $\mathbb{F}_q$, le nombre de ceux qui sont irréductibles est $\frac{1}{6}\,(2^6 - 2^3 - 2^2 + 2^1) = \frac{1}{6}\,54 = 9$, et le nombre de ceux-là qui sont primitifs est $\frac{1}{6}\,\phi(3^2 \cdot 7) = \frac{1}{6}\,(2 \times 3 \times 6) = 6$. ✓

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 $\mathbb{F}_{p^k}$.

Corrigé. Considérons $x_1, \ldots, x_k$ les racines de f dans $\bar{\mathbb{F}}_q$ (avec multiplicité). Tout d'abord, f est irréductible si et seulement si il existe un i, et par suite tout i, tel que x_i soit de degré k sur $\mathbb{F}_q$: en effet, s'il existe un tel i alors f divise le polynôme minimal de x_i, lequel est de degré k, donc ils sont égaux (à constante près) et f est bien irréductible, et réciproquement si f est irréductible alors toutes ses racines sont de degré k (sinon le polynôme minimal d'une racine serait un diviseur de f de degré strictement plus petit, contredisant l'irréductibilité). Si f est irréductible, comme toutes ses racines sont de degré k exactement, (a) il divise $t^{q^k} - t$ (dont les racines sont *tous* les éléments de degré divisant k sur $\mathbb{F}_q$) et (b) n'a aucune racine commune avec $t^{q^\ell} - t$ si ℓ est un diviseur strict de k (car les racines de $t^{q^\ell} - t$ sont de degré divisant ℓ donc certainement pas k). Réciproquement, si f n'est pas irréductible, c'est qu'il a une racine x_i d'un degré ℓ différent de k (strictement plus petit) : si ℓ divise k (strictement, donc), alors f n'est pas premier avec $t^{q^\ell} - t$, contredisant (b), et si ℓ ne divise pas k alors x_i n'est pas racine de $t^{q^k} - t$, contredisant (a).

Il est bien nécessaire de supposer à la fois (a) et (b) pour avoir l'irréductibilité : par exemple, $f(t) = t^2 - t$ est de degré 2 et vérifie (a) mais pas (b), et si g et h sont irréductibles de degrés 2 et 3 alors $f = gh$ est de degré 5 et vérifie (b) (puisque le seul diviseur strict de 5 est 1 et que f n'a pas de racine de degré 1) mais pas (a).

Pour déterminer algorithmiquement (et efficacement) si un polynôme $f \in \mathbb{F}_q[t]$ est irréductible, on veut donc notamment tester si f divise $t^{q^k} - t$: *a priori* cela peut sembler difficile car q^k peut être très grand. En fait, il s'agit simplement de calculer $\bar{t}^{q^k}$ dans l'anneau quotient $\mathbb{F}_q[t]/(f)$, ce qui se fait ainsi : si on représente les éléments de $\mathbb{F}_q[t]/(f)$ sur la base $1, \bar{t}, \ldots, \bar{t}^{d-1}$, les additions se font terme à terme, et les multiplications se font en multipliant les polynômes puis en réduisant modulo f, et pour élever $\bar{t}$ à la puissance q^k on peut par exemple représenter q^k en binaire et utiliser l'exponentiation rapide (i.e., on calcule $\bar{t}^2$, $\bar{t}^4$, $\bar{t}^8$, etc., par élévations au carré successives, et on multiplie celles dont le chiffre correspondant dans l'écriture binaire de q^k est 1), donc vérifier si $\bar{t}^{q^k} = \bar{t}$ dans $\mathbb{F}_q[t]/(f)$ se fait en $O(k^3)$ opérations dans $\mathbb{F}_q$ (voire mieux si on utilise une multiplication intelligente). La condition (b) est semblable : pour savoir si f est premier avec $t^{q^\ell} - t$, on commence par calculer $\bar{t}^{q^\ell} - \bar{t}$ dans $\mathbb{F}_q[t]/(f)$, ce qui donne le reste de la division euclidienne de $t^{q^\ell} - t$ par f, et ceci est la première étape de l'algorithme d'Euclide pour calculer le pgcd de $t^{q^\ell} - t$ et f.

En pratique, pour faire des calculs dans $\mathbb{F}_{p^k}$, il suffit de le représenter comme $\mathbb{F}_p[t]/(f)$ avec f irréductible de degré k. La question est donc de trouver un tel f : pour cela, on se contente bêtement de tirer au hasard un polynôme unitaire de degré k (il y en a p^k), de tester l'irréductibilité comme on vient de le voir, et de recommencer tant qu'on n'a pas trouvé un polynôme irréductible : l'exercice 1 montre que la probabilité qu'un polynôme de degré k sur $\mathbb{F}_p$ soit irréductible est environ $\frac{1}{k}$ (le « environ » étant à un $O(p^{-k/2})$ près, qui est négligeable). Donc en $O(k)$ essais on finit par en trouver un. ✓

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 $\mathbb{F}$.

Corrigé. Remarquons que pour $t \in \mathbb{F}$ on a $t^{q-1} = 1$ sauf si $t = 0$ auquel cas $t^{q-1} = 0$. Ainsi, la somme des $f(x_0, \ldots, x_n)^{q-1}$ est congrue modulo p au nombre de $(x_0, \ldots, x_n)$ tels que $f(x_0, \ldots, x_n) \neq 0$, donc si on prouve qu'elle est nulle (dans $\mathbb{F}$) le nombre de zéros de f dans $\mathbb{F}^{n+1}$ sera multiple de p (le cardinal de tout $\mathbb{F}^{n+1}$ étant lui-même multiple de p), et, comme il existe toujours le zéro trivial, il y en aura au moins un autre.

En développant $f(x_0, \ldots, x_n)^{q-1}$ comme somme de monômes chacun de degré $d(q-1)$, on est ramené à prouver que si $x_0^{s_0} \cdots x_n^{s_n}$ est un monôme de degré $s_0 + \cdots + s_n = d(q-1) < (n+1)(q-1)$ alors la somme sur tous les $(x_0, \ldots, x_n)$ de $x_0^{s_0} \cdots x_n^{s_n}$ est nulle dans $\mathbb{F}$. Cette somme se factorise comme le produit des $\sum_{x \in \mathbb{F}} x^{s_i}$ et il suffit donc de prouver qu'au moins l'un de ces facteurs est nul. Or au moins un des s_i vérifie $s_i < q-1$. Finalement, il suffit donc prouver que si $s < q-1$ alors $\sum_{x \in \mathbb{F}} x^s = 0$ (dans $\mathbb{F}$).

Lorsque $s = 0$, le résultat est clair (le nombre d'éléments de $\mathbb{F}$ est multiple de p), on peut donc supposer $s > 0$ et la somme peut être faite sur $\mathbb{F}^\times$, qui est un groupe cyclique d'ordre $q-1$: en appelant g un générateur de celui-ci, on a $\sum_{x \in \mathbb{F}^\times} x^s = \sum_{i=0}^{q-2} g^{si} = \frac{g^{s(q-1)}-1}{g^s-1}$ (puisque $g^s \neq 1$ dans $\mathbb{F}$) et comme $g^{s(q-1)} = 1$, cette somme est bien nulle, ce qui conclut. ✓

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 $|\Phi_n(q)| > q-1$.

Corrigé. Pour tout $x \in D$, soit $Z_x = \{y \in D : xy = yx\}$ le centralisateur de x : manifestement, Z_x est un $\mathbb{F}$-espace vectoriel, et même une algèbre à divisions sur $\mathbb{F}$. Soit $d(x)$ sa dimension (comme $\mathbb{F}$-espace vectoriel) : alors $Z_x \cap D^\times$ a pour cardinal $q^{d(x)} - 1$, où $d(x)$ divise n (par exemple parce que D est un Z_x-espace vectoriel à gauche, ou simplement parce que $q^{d(x)} - 1$ ne peut diviser $q^n - 1$ que si $d(x)$ divise n). L'orbite de x sous l'action de $D^\times$ a pour cardinal $\frac{q^n-1}{q^{d(x)}-1}$, et l'équation aux classes (le cardinal de $D^\times$ est la somme des cardinaux des orbites) s'écrit

$$q^n - 1 \;=\; q - 1 \;+\; \sum_{x \in S} \frac{q^n - 1}{q^{d(x)} - 1}$$

(où S est un ensemble de représentants des orbites ayant strictement plus d'un seul élément et $q-1$ est le cardinal de $\mathbb{F}^\times$, ensemble des orbites à un élément).

Soit $\Phi_n(t) = \prod(t-\zeta)$ (le produit portant sur les racines primitives n-ièmes de l'unité) le n-ième polynôme cyclotomique : rappelons que $\Phi_n \in \mathbb{Z}[t]$. Alors $\Phi_n(q)$ divise $q^n - 1$, et même divise $\frac{q^n-1}{q^{d(x)}-1} = \prod_{d(x)|\ell|n,\, \ell>d(x)} \Phi_\ell(q)$ pour $d(x) < n$ (soit x non central). On en déduit que $\Phi_n(q)$ divise $q-1$ et en particulier $|\Phi_n(q)| \leq |q-1|$. Mais comme $|q-\zeta| > |q-1|$ pour tout complexe $\zeta \neq 1$ sur le cercle unité, ce n'est possible que si $n = 1$, et $D = \mathbb{F}$, ce qu'on voulait prouver. ✓

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* :

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

Corrigé. Expliquons d'abord pourquoi $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod p$: si g est un élément primitif modulo p, c'est-à-dire un générateur de $\mathbb{F}_p^\times$, alors un élément n de $\mathbb{F}_p^\times$ est un carré si et seulement si il s'écrit $n = g^{2i}$ pour un certain i, et alors $n^{(p-1)/2} = g^{i(p-1)} = 1$ dans $\mathbb{F}_p^\times$ tandis que si à l'inverse $n = g^{2i+1}$ alors $n^{(p-1)/2} = g^{i(p-1)}\, g^{(p-1)/2} = -1$ (car $g^{(p-1)/2}$ a pour carré 1 dans $\mathbb{F}_p$ et ne vaut pas lui-même 1). En particulier, on peut remarquer $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, dans $\mathbb{Z}$ cette fois. Le fait que $\left(\frac{mn}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p}\right)$ est également clair.

On a $S^2 = \sum_{x,y\in\mathbb{F}_p^\times} \left(\frac{xy}{p}\right)\zeta^{x+y}$, soit, en posant $t = y/x$ (dans $\mathbb{F}_p^\times$), $\sum_{x,t\in\mathbb{F}_p^\times} \left(\frac{t}{p}\right)\zeta^{x(1+t)}$ (où on a utilisé le fait que $\left(\frac{x}{p}\right)^2 = 1$). Or $\sum_{x\in\mathbb{F}_p^\times} \zeta^{xu}$ vaut (toujours dans $\mathbb{F}_q$) -1 si $u \in \mathbb{F}_p^\times$ et $p-1$ si $u = 0$: appliquant ce fait dans ce qui précède à $u = 1+t$, on trouve $S^2 = \left(\frac{-1}{p}\right)p - \sum_{x,t\in\mathbb{F}_p^\times}\left(\frac{t}{p}\right)$ et le second terme est nul (il y a autant d'éléments de $\mathbb{F}_p^\times$ qui sont des carrés que qui n'en sont pas) d'où $S^2 = \left(\frac{-1}{p}\right)p$.

Par ailleurs, $S^q = \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)\zeta^{qx}$ (le frobenius $x \mapsto x^q$ étant un automorphisme de corps) donc $S^q = \sum_{z\in\mathbb{F}_p^\times}\left(\frac{q}{p}\right)\left(\frac{z}{p}\right)\zeta^z$ (en posant $z = qx$ et en utilisant de nouveau le fait que $\left(\frac{q}{p}\right)$ est son inverse), soit $S^q = \left(\frac{q}{p}\right)S$.

De ces deux formules on déduit d'une part $S^{q-1} = \left(\frac{q}{p}\right)$ et de l'autre $S^{q-1} = (S^2)^{(q-1)/2} = \left[\left(\frac{-1}{p}\right)p\right]^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$, d'où la loi de réciprocité quadratique (l'égalité ayant lieu dans $\mathbb{F}_q$ donc dans $\mathbb{Z}$). ✓

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) ?

Corrigé. (1) Manifestement, si g est un générateur du groupe multiplicatif $\mathbb{F}_{q^k}^\times$, les éléments $1, g, \ldots, g^{k-1}$ sont libres sur $\mathbb{F}_q$, donc sont une $\mathbb{F}_q$-base de $\mathbb{F}_{q^k}$. Pour tout $i \in \mathbb{Z}$, posons $g^i = \alpha_0^{(i)} + \alpha_1^{(i)} g + \cdots + \alpha_{k-1}^{(i)} g^{k-1}$. Montrons que la suite $(\alpha_0^{(i)})_i$ (périodique de période $p^k - 1$) est un « presque » bracelet de De Bruijn, en ce sens qu'il s'y trouve chaque k-uplet d'éléments de $\mathbb{F}_q$ à l'exception du k-uplet nul.

Remarquons d'abord que tout k-uplet à l'exception du k-uplet nul est la valeur pour un certain i de $(\alpha_0^{(i)}, \alpha_1^{(i)}, \ldots, \alpha_{k-1}^{(i)})$ (puisqu'il existe bien un i pour lequel $g^i = \alpha_0^{(i)} + \alpha_1^{(i)} g + \cdots + \alpha_{k-1}^{(i)} g^{k-1}$). Reste à expliquer pourquoi l'application $\mathbb{F}_q$-linéaire $\varphi\colon \mathbb{F}_{q^k} \to (\mathbb{F}_q)^k$ qui envoie $x \in \mathbb{F}_{q^k}$ sur les coordonnées respectives sur l'élément 1 (de la base $1, g, \ldots, g^{k-1}$) de $gx, g^2x, \ldots, g^k x$ (autrement dit, de façon peut-être plus claire, φ envoie $g^i = \alpha_0^{(i)} + \alpha_1^{(i)} g + \cdots + \alpha_{k-1}^{(i)} g^{k-1}$ sur $(\alpha_0^{(i+1)}, \ldots, \alpha_0^{(i+k)})$), est bijective. Or la matrice de φ sur la base $g^{k-1}, \ldots, g, 1$ (au départ, et la base canonique à l'arrivée) est $(\alpha_0^{(k-j+i)})_{ji}$, donc triangulaire (car $\alpha_0^{(i)} = 0$ si $0 < i < k$) de diagonale $(\alpha_0^{(k)}, \ldots, \alpha_0^{(k)})$, donc inversible ($\alpha_0^{(k)}$ ne peut pas être nul, sinon $\alpha_0^{(i)}$ serait nul pour tout $i > 0$ et on ne pourrait pas avoir $g^{p^k-1} = 1$).

Une fois obtenu un tel « presque » bracelet de De Bruijn, auquel il ne manque que le k-uplet $(0, \ldots, 0)$, il suffit d'insérer une perle 0 supplémentaire dans une des séquences de $k-1$ perles 0 (il y a $q-1$ tels endroits). La longueur du bracelet passe alors de $p^k - 1$ à p^k, et on se convainc immédiatement que tout k-uplet qui se trouvait dans l'ancien bracelet se trouve aussi dans le nouveau, et que le k-uplet nul s'y trouve maintenant. On a donc obtenu le bracelet recherché.

(2) Soient $q_1, \ldots, q_s$ des puissances de nombres premiers distincts, et soient $b_1, \ldots, b_s$ des bracelets de De Bruijn d'ordre k sur des alphabets $A_1, \ldots, A_s$ à $q_1, \ldots, q_s$ éléments : cherchons à obtenir un bracelet de De Bruijn b d'ordre k sur un alphabet (quelconque) à $q = q_1 \cdots q_s$ lettres, mettons $A = A_1 \times \cdots \times A_s$. Pour cela, on définit simplement $b(i) = (b_1(i_1), \ldots, b_s(i_s))$, où $i_1, \ldots, i_s$ sont les réductions de $i \in \mathbb{Z}/q^k\mathbb{Z}$ respectivement modulo $q_1^k, \ldots, q_s^k$. Le théorème chinois assure que pour tous éléments $i_1, \ldots, i_s$ de $\mathbb{Z}/q_1^k\mathbb{Z}, \ldots, \mathbb{Z}/q_s^k\mathbb{Z}$ respectivement, il existe un (unique) $i \in \mathbb{Z}/q^k\mathbb{Z}$ congru à $i_1, \ldots, i_s$ modulo $q_1^k, \ldots, q_s^k$ respectivement. Or ceci signifie précisément que pour tout k-uplet $(a_0, \ldots, a_{k-1}) \in A^k$, une fois trouvés (comme $b_1, \ldots, b_s$ sont des bracelets de De Bruijn) des indices $i_1, \ldots, i_s$ dans les périodes respectives de $b_1, \ldots, b_s$ où les k-uplets composantes de $(a_0, \ldots, a_{k-1})$ dans $A_1^k, \ldots, A_s^k$ se situent, on peut trouver un indice i modulo q^s où $(a_0, \ldots, a_{k-1})$ se situe dans b. C'est-à-dire que b est bien un bracelet de De Bruijn. ✓