Variations autour du théorème de Wilson

Le théorème de Wilson a été découvert à la fin du dixième siècle par le mathématicien arabe Ibn al-Haytham qu'on nomme aussi Alhazen. Le résultat ressurgit, sans démonstration, à la fin du dix-huitième siècle dans les écrits de Edward Waring qui l'attribue en 1770 à son élève John Wilson. L'année suivante, Lagrange en donne deux démonstrations dans son article [LAG] (voir la quatrième preuve présentée ici). En fait, Leibniz (1646-1716) connaissait déjà le résultat et sa démonstration mais ne les avait pas publiés (voir [RAS] pour de plus amples considérations historiques).

Dans cette note consacrée au théorème de Wilson, on propose dans une première partie quatre démonstrations de ce résultat. La deuxième partie étudie la réciproque du théorème de Wilson, quelques variantes autour de ce théorème ainsi que leurs applications à des tests de primalité (voir aussi [DMZ, exercice 2.16 et 2.19]). Dans une troisième partie, on donne une généralisation du théorème de Wilson due à Gauss. Enfin, la dernière partie étudie quelques propriétés de congruence pour les coefficients binomiaux (dont l'une peut s'obtenir comme conséquence du théorème de Wilson).

Remarquons que les tests de primalité qui se déduisent du théorème de Wilson reposent peu ou prou sur le calcul d'un factoriel et sont donc inefficaces en pratique. Ainsi le théorème de Wilson est plutôt anecdotique.

Notation 1 – Nombre premier. On note $\mathscr{P}$ l'ensemble des nombres premiers.

Théorème de Wilson.

Lemme 2 – Théorème de Wilson. Si $p \in \mathscr{P}$ alors
$$(p-1)! = -1\,[p]\,.$$

Preuve. On va donner quatre démonstrations de ce résultat de Wilson. L'idée directrice des deux premières démonstrations est de remplacer ce calcul de congruence par un calcul dans $\mathbb{F}_p$ ce qui va permettre d'utiliser les propriétés d'un corps. L'idée de la troisième démonstration est d'utiliser les théorèmes de Sylow dans le groupe symétrique $\mathfrak{S}_p$. La quatrième preuve est une adaptation en langage moderne d'une des deux preuves proposées par Lagrange dans son article [LAG]. On trouvera d'autres démonstrations sur la page

https://fr.wikipedia.org/wiki/Théorème_de_Wilson

Notation pour les deux premières démonstrations. On note $\pi : \mathbb{Z} \to \mathbb{F}_p$ la surjection canonique. On a
$$\pi((p-1)!) = \prod_{x \in {\mathbb{F}_p}^\times} x$$
Il s'agit donc de calculer le produit des éléments du groupe multiplicatif ${\mathbb{F}_p}^\times$.

Première démonstration : théorème de Lagrange et relation coefficients-racines. Le théorème de Lagrange appliqué au groupe multiplicatif ${\mathbb{F}_p}^\times$ montre que $x^{p-1} = 1$ pour tout $x \in {\mathbb{F}_p}^\times$. Ainsi tous les éléments de ${\mathbb{F}_p}^\times$ sont racines de $\mathrm{X}^{p-1} - 1 \in \mathbb{F}_p[\mathrm{X}]$. On en déduit que
$$\prod_{x \in {\mathbb{F}_p}^\times} (\mathrm{X} - x) \mid (\mathrm{X}^{p-1} - 1)\,.$$
Par raison de degré, on a
$$\prod_{x \in {\mathbb{F}_p}^\times} (\mathrm{X} - x) = \mathrm{X}^{p-1} - 1\,.$$
Les relation coefficient-racines donnent alors
$$\prod_{x \in {\mathbb{F}_p}^\times} x = (-1)^{p-1} \cdot (-1) = -1\,.$$
Attention au cas $p = 2$ dans la dernière égalité du calcul précédent.

Deuxième démonstration : produit des éléments d'un groupe abélien fini et nombre de racines d'un polynôme à coefficients dans un corps. Montrons au préalable le résultat suivant. Soit G un groupe abélien fini noté multiplicativement et G_2 l'ensemble de ses éléments d'ordre 2. On a
$$\prod_{x \in \mathrm{G}} x = \prod_{x \in \mathrm{G}_2} x\,. \qquad (*)$$
En distinguant dans le membre de gauche les éléments de G vérifiant $x \neq x^{-1}$, on obtient
$$\prod_{x \in \mathrm{G}} x = \left(\prod_{x = x^{-1}} x \right) \left(\prod_{x \neq x^{-1}} x \right).$$
En regroupant dans le facteur de droite, un élément et son inverse (ce qu'on peut bien faire puisqu'ils sont distincts), il reste
$$\prod_{x \in \mathrm{G}} x = \prod_{x = x^{-1}} x\,.$$

Or $x = x^{-1}$ si et seulement si $x \in \mathrm{G}_2 \sqcup \{1\}$. Comme le facteur 1 ne compte pas dans le produit, on obtient l'égalité $(*)$.

Lorsqu'on applique ce calcul au groupe multiplicatif ${\mathbb{F}_p}^\times$, on obtient

$$\prod_{x \in {\mathbb{F}_p}^\times} x \quad = \prod_{x^2=1, x \neq 1} x \,.$$

Il s'agit donc de calculer les racines de $\mathrm{X}^2 - 1$ distinctes de 1 dans $\mathbb{F}_p$. Lorsque $p = 2$, on a $\mathrm{X}^2 - 1 = (\mathrm{X} - 1)^2$. Ainsi, il n'y a pas de racines de $\mathrm{X}^2 - 1$ distinctes de 1. Le produit est donc égal à $1 = -1$. Lorsque p est impair, les éléments -1 et 1 sont distincts et racines de $\mathrm{X}^2 - 1$. Comme un polynôme de degré n à coefficients dans un corps (en fait un anneau intègre) a au plus n racines dans ce corps, on en déduit que les seuls racines de $\mathrm{X}^2 - 1$ dans $\mathbb{F}_p$ sont $\{-1, 1\}$. Finalement

$$\prod_{x \in {\mathbb{F}_p}^\times} x = \prod_{x^2=1, x \neq 1} x = -1 \,.$$

Troisième démonstration : théorème de Sylow et groupe de permutations. Étudions les p-Sylow du groupe symétrique $\mathfrak{S}_p$ (à propos des théorèmes de Sylow, on pourra consulter [PER, Chapitre 1.5]). Comme $|\mathfrak{S}_p| = p! = p(p-1)!$ avec $p \nmid (p-1)!$, les p-Sylow de $\mathfrak{S}_p$ sont d'ordre p et donc cycliques. De plus, ils sont engendrés par n'importe lequel de leurs éléments non trivial qui est alors un élément d'ordre p. Réciproquement, si x est un élément d'ordre p de $\mathfrak{S}_p$ alors $\langle x \rangle$ est d'ordre p et donc un p-Sylow de G. Les p-Sylow de $\mathfrak{S}_p$ sont donc les groupes engendrés par un élément d'ordre p de $\mathfrak{S}_p$.

Déterminons à présent les éléments d'ordre p de $\mathfrak{S}_p$. Pour calculer l'ordre d'un élément de $\mathfrak{S}_p$, on utilise sa décomposition en cycles à support disjoint : l'ordre est le ppcm des longueurs des cycles de cette décomposition. Ainsi si σ est d'ordre p, les cycles intervenant dans sa décomposition en cycle à support disjoint sont de longueur un diviseur de p c'est-à-dire 1 ou p. De plus, s'ils sont tous de longueur 1 alors $\sigma = \mathrm{id}_{[\![1\,,p]\!]}$ n'est pas d'ordre p. Il existe donc dans la décomposition en cycles à support disjoint de σ un cycle de longueur p. Comme la somme des longueurs des cycles qui interviennent dans la décomposition de σ est p, il n'y a pas d'autres cycles et σ est un cycle d'ordre p. Finalement les éléments d'ordre p de $\mathfrak{S}_p$ sont les p-cycles.

Or, il y a $(p-1)!$ p-cycles dans $\mathfrak{S}_p$ puisqu'il s'agit de choisir l'image de 1 (qui doit être différente de 1) puis l'image de l'image de 1 (qui doit être différente des deux premiers éléments) et ainsi de suite. Par ailleurs, si S_1 et S_2 sont deux p-Sylow de $\mathfrak{S}_p$ distincts alors $\mathrm{S}_1 \cap \mathrm{S}_2 = \{1\}$ (ce résultat n'est pas vrai en général, ici il est vrai parce que les p-Sylow sont d'ordre p). En effet, comme $\mathrm{S}_1 \neq \mathrm{S}_2$, on peut supposer (quitte à échanger S_1 et S_2) qu'il existe $x \in \mathrm{S}_1$ tel que $x \notin \mathrm{S}_2$. Ainsi $\mathrm{S}_1 \cap \mathrm{S}_2$ est un sous-groupe de S_1 ne contenant pas x. C'est donc un sous-groupe strict de S_1. L'ordre de $\mathrm{S}_1 \cap \mathrm{S}_2$ est donc un diviseur strict de $|\mathrm{S}_1| = p$. Ainsi $|\mathrm{S}_1 \cap \mathrm{S}_2| = 1$ et $\mathrm{S}_1 \cap \mathrm{S}_2 = \{1\}$. Finalement, tout élément x d'ordre p de $\mathfrak{S}_p$ appartient à un unique p-Sylow de $\mathfrak{S}_p$ qui est $\langle x \rangle$. Comme chaque p-Sylow est cyclique d'ordre p, il contient exactement $p-1$ éléments d'ordre p. Ainsi le nombre s_p de p-Sylow de $\mathfrak{S}_p$ vérifie $s_p(p-1) = n_p$ où n_p est le nombre d'élément d'ordre p de $\mathfrak{S}_p$. Finalement $s_p = (p-1)!/(p-1) = (p-2)!$.

Comme le nombre de p-Sylow d'un groupe est congru à 1 modulo p, on en déduit que

$$(p-2)! \equiv 1 \,[p] \,.$$

En multipliant par $p - 1 \equiv -1 \,[p]$, on obtient le théorème de Wilson.

Quatrième démonstration (dues à Lagrange) : formule du binôme et polynôme. Le cas où $p = 2$ est trivial. On considère à présent que p est un nombre premier impair. Soit P le polynôme donné par

$$\mathrm{P}(\mathrm{X}) = \prod_{i=1}^{p-1} (\mathrm{X} + i) \in \mathbb{Z}[\mathrm{X}] \,.$$

On a alors $$(\mathrm{X}+1)\mathrm{P}(\mathrm{X}+1) = (\mathrm{X}+1)\prod_{i=1}^{p-1}(\mathrm{X}+1+i) = (\mathrm{X}+1)\prod_{i=2}^{p}(\mathrm{X}+i) = (\mathrm{X}+p)\mathrm{P}(\mathrm{X}) \,. \qquad (\star)$$

Par ailleurs, comme $\deg \mathrm{P} = p-1$ et est unitaire, on peut écrire

$$\mathrm{P}(\mathrm{X}) = \sum_{i=0}^{p-1} a_i \mathrm{X}^{p-i-1}$$

avec $a_0 = 1$ et $a_{p-1} = \mathrm{P}(0) = (p-1)!$. Il s'agit à présent de montrer que pour $1 \leqslant k \leqslant p-2$, on a $p \mid a_k$. Pour cela, on réécrit la relation $(\star)$ sous la forme : $p\mathrm{P}(\mathrm{X}) = (\mathrm{X}+1)\mathrm{P}(\mathrm{X}+1) - \mathrm{X}\mathrm{P}(\mathrm{X})$ et on calcule le coefficient en X^{p-1-k} dans cette relation. Pour $p\mathrm{P}(\mathrm{X})$, on obtient pa_k, pour $\mathrm{X}\mathrm{P}(\mathrm{X})$, on obtient a_{k+1} et pour $(\mathrm{X}+1)\mathrm{P}(\mathrm{X}+1)$, on écrit

$$(\mathrm{X}+1)\mathrm{P}(\mathrm{X}+1) = (\mathrm{X}+1)\sum_{i=0}^{p-1} a_i (\mathrm{X}+1)^{p-1-i} = \sum_{i=0}^{p-1} a_i (\mathrm{X}+1)^{p-i} \,.$$

En développant avec la formule du binôme de Newton $(\mathrm{X}+1)^{p-i}$, on obtient comme terme en X^{p-1-k},

$$\binom{p-i}{p-1-k} = \binom{p-i}{k+1-i}.$$

Ainsi, on obtient l'égalité $$pa_k = \sum_{i=0}^{p-1} a_i \binom{p-i}{k+1-i} - a_{k+1} \,.$$

Or pour $i > k+1$, le terme $\binom{p-i}{k+1-i}$ est nul (le degré de $(X+1)^{p-i}$ n'est pas suffisant pour fournir un terme en X^{p-1-k}. Pour $i = k+1$, on obtient $a_{k+1}\binom{p-i}{k+1-i} = a_{k+1}$. Finalement, on obtient la relation

$$pa_k = \sum_{i=0}^{k} a_i \binom{p-i}{k+1-i}.$$

En isolant les termes pour $i = 0$ et $i = k$ qui donne respectivement, $\binom{p}{k+1}$ et $(p-k)a_k$, on peut réécrire la relation précédente sous la forme

$$ka_k = \binom{p}{k+1} + \sum_{i=1}^{k-1} a_i \binom{p-i}{k+1-i}. \qquad (\star\star)$$

En particulier, cela donne $a_1 = p(p-1)/2$ qui est divisible par p puisque $(p-1)/2$ est un entier (p est impair). La relation $(\star\star)$ permet alors de montrer par récurrence que, pour tout $1 \leqslant k \leqslant p-2$, on a $p \mid a_k$. En effet, on vient d'effectuer l'initialisation grâce à la valeur de a_1 et la relation $(\star\star)$ assure par hypothèse de récurrence forte que ka_k est divisible par p grâce au fait que $\binom{p}{k+1}$ l'est puisque $2 \leqslant k+1 \leqslant p-1$ et que $p \mid \binom{p}{i}$ pour $1 \leqslant i \leqslant p-1$ (voir le lemme 13). Mais comme $1 \leqslant k \leqslant p-1$, le lemme d'Euclide assure que $p \mid a_k$ [1]. Il ne reste plus qu'à conclure en calculant $P(1)$ de deux façons différents :

$$P(1) = \prod_{i=1}^{p-1}(1+i) = \prod_{i=2}^{p} i = p! \qquad \text{et} \qquad P(1) = \sum_{i=0}^{p-1} a_i = 1 + \sum_{i=1}^{p-2} a_i + (p-1)!\,.$$

Comme $p!$ et les a_i pour $1 \leqslant i \leqslant p-2$ sont divisibles par p, on obtient que $p \mid ((p-1)!+1)$. C'est le résultat souhaité. ∎

Réciproque du théorème de Wilson et test de primalité.

Dans cette partie, on montre la réciproque du théorème de Wilson pour obtenir ainsi une caractérisation des nombres premiers. On obtient ainsi un test de primalité qui s'avère inefficace puisque nécessitant le calcul d'une factorielle (voir la remarque 4). On donne ensuite quelques généralisations du théorème de Wilson et de son critère de primalité (voir les corollaires 5 et 7 et la remarque 6).

Remarque 3 – Réciproque du théorème de Wilson. Soit n un entier non premier. Montrons que

$$(n-1)! = 0\,[n] \quad \text{si} \quad n \neq 4 \qquad \text{et} \qquad (n-1)! = 2\,[n] \quad \text{si} \quad n = 4\,.$$

Si on peut écrire $n = dd'$ avec $1 < d < n'$ et $1 < d' < n$ et $d \neq d'$ alors les facteurs d et d' apparaissent dans $(n-1)!$. Ainsi $n = dd' \mid (n-1)!$ c'est-à-dire $(n-1)! = 0\,[n]$. Or tout entier non premier qui n'est pas le carré d'un nombre premier peut s'écrire sous une telle forme. En effet,

– si la décomposition en facteur premier de n fait intervenir plusieurs nombres premiers :

$$n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k} \qquad \text{avec} \qquad \alpha_i > 0, \quad p_i \in \mathscr{P}, \quad k > 1 \quad \text{et} \quad p_i \neq p_j \text{ si } i \neq j\,,$$

on choisit $d = p_1$ et $d' = n/d \neq d$;

– sinon $n = p^\alpha$ avec $\alpha \geqslant 3$ et on choisit $d = p$ et $d' = p^{\alpha-1} \neq d$

Il reste à étudier le cas $n = p^2$ avec $p \in \mathscr{P}$. Si $p > 2$ alors $1 < p < n$ et $1 < 2p < p^2 = n$ et $p \neq 2p$. Ainsi les facteurs p et $2p$ apparaissent dans $(n-1)!$ et donc $n = p^2 \mid (n-1)!$ c'est-à-dire $(n-1)! = 0\,[n]$. Enfin, le cas $p = 2$ aboutit à $n = 4$ et donc $(n-1)! = 6 = 2\,[4]$.

Finalement, on a la disjonction de cas

$$(n-1)! = \begin{cases} -1\,[n] & \text{si } n \in \mathscr{P} \\ 2\,[n] & \text{si } n = 4 \\ 0\,[n] & \text{sinon} \end{cases}$$

Comme $2 \neq -1[4]$, on en déduit ainsi la caractérisation suivante de la primalité : soit n un entier supérieur ou égal à 2 alors

$$n \in \mathscr{P} \qquad \Longleftrightarrow \qquad (n-1)! = -1\,[n].$$

Cette caractérisation fournit alors un test de primalité de la façon suivante : soit $n \in \mathbb{N}^*$ l'entier dont on cherche à déterminer la primalité, calculer $(n-1)!$ modulo n. Si on trouve -1 alors n est premier ; sinon n n'est pas premier. ∎

Remarque 4 – Intérêt du test de primalité de Wilson. En pratique pour déterminer la primalité d'un nombre, le test de Wilson est inefficace : le calcul du factoriel étant beaucoup trop long (c'est un temps de calcul exponentiel) alors qu'on dispose d'algorithme de primalité en temps polynomial (par exemple l'algorithme AKS,

1. La nullité modulo p des coefficients a_k pour $1 \leqslant k \leqslant p-2$ peut être obtenue directement en réduisant modulo p le polynôme P et en utilisant la relation que la réduction modulo p de P est $X^{p-1} - 1$ comme on l'a vu dans la première démonstration.

voir [BOR]) ou encore d'algorithmes probabilistes extrèmement rapides (par exemple les tests de Miller-Rabin ou Solovay-Strassen [DMZ, 5.3.4]).

Par ailleurs, si on souhaite quand même mettre en place le test de Wilson, on effectuera toutes les multiplications modulo n (c'est-à-dire dans $\mathbb{Z}/n\mathbb{Z}$) plutôt que de calculer l'entier $(n-1)!$ et de considérer ensuite son résidu modulo n. Cela permet de borner à l'avance la taille des nombres manipulés. ■

Corollaire 5 Soit $p \in \mathscr{P}$ et $1 \leqslant n \leqslant p$. On a

$$(n-1)!(p-n)! = (-1)^n \,[p]$$

Preuve. Pour $n = 1$ et $n = p$, il s'agit du théorème de Wilson. Supposons le résultat vrai pour n vérifiant $1 \leqslant n < p-1$ et montrons qu'il est vrai pour $n+1$. Dans $\mathbb{Z}$, on a

$$n!(p-n-1)!(p-n) = n(n-1)!(p-n)!$$

En réduisant cette égalité modulo p, on a

$$n!(p-n-1)!(-n) = n(n-1)!(p-n)!\,[p]\,.$$

Comme $1 \leqslant n < p-1$, l'entier n est inversible modulo p et donc

$$n!(p-n-1)!(-1) = (n-1)!(p-n)!\,[p]\,.$$

Ainsi $$n!(p-n-1)! = (-1)(n-1)!(p-n)! = (-1)^{n+1}\,[p]\,.$$ ■

Remarque 6 – Une autre caractérisation de la primalité. Soit $n \in \mathbb{N} \setminus \{0,1\}$. On a

$$\forall\, m \in [\![\,1\,,\,n\,]\!],\quad (m-1)!(n-m)! = (-1)^m\,[n] \qquad \Longleftrightarrow \qquad n \in \mathscr{P}\,.$$

(⇒) Si $m = 1$ alors $(n-1)! = -1\,[n]$. La remarque 3 assure que n est premier.
(⇐) Il s'agit du corollaire 5. ■

Corollaire 7 Soit n un entier impair supérieur ou égal à 3. On a

$$n \in \mathscr{P} \qquad \Longleftrightarrow \qquad \left(\left(\frac{n-1}{2}\right)!\right)^2 = (-1)^{\frac{n+1}{2}}\,.$$

Preuve. L'entier n est impair, on peut donc écrire $n = 2m+1$ c'est-à-dire $m = (n-1)/2$. On a donc

$$(n-1)! = 1 \cdots (m-1) \cdot m \cdot (m+1) \cdot (m+2) \cdots (2m)\,.$$

Or $$m+1 = -m\,[n],\quad m+2 = -(m-1)\,[n],\quad \ldots,\quad 2m = -1\,[n]\,.$$

On a donc $$(n-1)! = 1 \cdots (m-1) \cdot m \cdot (-m) \cdot (-(m-1)) \cdots (-1) = (-1)^m (m!)^2\,.$$

Comme -1 est inversible dans $\mathbb{Z}/n\mathbb{Z}$, on en déduit que

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 = (-1)^{\frac{n+1}{2}}\,[n] \quad \Longleftrightarrow \quad (-1)^{\frac{n-1}{2}}(n-1)! = (-1)^{\frac{n+1}{2}}\,[n] \quad \Longleftrightarrow \quad (n-1)! = -1\,[n]\,.$$

La remarque 4 permet de conclure. ■

Remarque 8 On aurait pu montrer le sens direct du corollaire 7 en appliquant le corollaire 5 pour $n = (p+1)/2$. Par ailleurs, le corollaire 7 montre que si p est un nombre premier congru à 1 modulo 4 alors -1 est un carré modulo p puisque

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = (-1)^{\frac{p+1}{2}} = -1\,[p]\,.$$ ■

Un résultat de Gauss.

Dans cette partie, on aborde une généralisation, due à Gauss, du théorème de Wilson bien différente de celles qui précèdent. Avant d'aborder ce résultat de Gauss, on va affiner l'égalité $(*)$ sur le produit des éléments d'un groupe abélien fini . On commence pour cela par un calcul dans un $\mathbb{F}_2$-espace vectoriel de dimension finie.

Lemme 9 – $\mathbb{F}_2$-espace vectoriel de dimension finie. Soit V un $\mathbb{F}_2$-espace vectoriel de dimension finie. Si $\dim_{\mathbb{F}_2} \mathrm{V} \neq 1$ alors

$$\sum_{x \in \mathrm{V}} x = 0\,.$$

Si $\dim_{\mathbb{F}_2} \mathrm{V} = 1$ alors $\sum_{x \in \mathrm{V}} x$ est l'unique vecteur non nul de V.

Preuve. Si $\dim \mathrm{V} = 0$, le résultat est évident. On suppose à présent $\dim \mathrm{V} \geqslant 1$. Commençons par le cas où $\mathrm{V} = {\mathbb{F}_2}^n$. On a donc

$$\sum_{x\in \mathrm{V}} x = \sum_{(\varepsilon_1,\dots,\varepsilon_n)\in {\mathbb{F}_2}^n} (\varepsilon_1,\dots,\varepsilon_n)\,.$$

Lorsque $x=(\varepsilon_1,\dots,\varepsilon_n)$ décrit ${\mathbb{F}_2}^n$, les valeurs 0 et 1 apparaissent 2^{n-1} fois sur chacune des n composantes, (les solutions de l'équation $\varepsilon_i=0$ (resp. $\varepsilon_i=1$) forment un hyperplan vectoriel (resp. affine) de ${\mathbb{F}_2}^n$). Ainsi si $n\geqslant 2$ alors 2^{n-1} est pair et la i^{e} composante de la somme est nulle. Si $n=1$ alors

$$\sum_{x\in \mathrm{V}} x = \sum_{x\in \mathbb{F}_2} x = 0+1=1$$

qui est le seul vecteur non nul de $\mathbb{F}_2$.

Considérons à présent le cas général. Il existe un isomorphisme (de $\mathbb{F}_2$-espace vectoriel) $f:{\mathbb{F}_2}^n\to \mathrm{V}$. Comme f est bijective, on a

$$\sum_{x\in \mathrm{V}} x = \sum_{y\in {\mathbb{F}_2}^n} f(y)\,.$$

Par ailleurs, comme f est linéaire, on a

$$\sum_{x\in \mathrm{V}} x = f\left(\sum_{y\in {\mathbb{F}_2}^n} y\right).$$

Ainsi, si $\dim \mathrm{V}\geqslant 2$, on obtient bien une somme nulle. Si $\dim \mathrm{V}=1$ alors, par linéarité et bijectivité, f envoie le seul vecteur non nul de $\mathbb{F}_2$ sur le seul vecteur non nul de V et on obtient le résultat souhaité. ∎

Comme la structure de $\mathbb{F}_2$-espace vectoriel est automatique sur un groupe abélien dont les éléments sont d'ordre 1 ou 2 (voir l'exemple 6.29 de [BPM]), le résultat du lemme 9 s'étend de la façon suivante à un groupe abélien fini.

Corollaire 10 – Somme des éléments d'un groupe abélien fini. Soit G un groupe abélien fini (noté additivement). Si G admet un unique élément d'ordre 2 alors

$$\sum_{x\in \mathrm{G}} x = y\,.$$

Dans le cas contraire, on a

$$\sum_{x\in \mathrm{G}} x = 0\,.$$

Preuve. D'après la relation $(*)$, on a

$$\sum_{x\in \mathrm{G}} x = \sum_{x\in \mathrm{G}_2} x = \sum_{x\in \mathrm{G}_2\sqcup\{0\}} x$$

Montrons que $\mathrm{G}_2\sqcup\{0\}$ est un sous-groupe de G dont tous les éléments (sauf 0) est d'ordre 2. La deuxième propriété est évident par définition de G_2. Il s'agit donc de montrer que $\mathrm{G}_2\sqcup\{0\}$ est un groupe. On a $0\in \mathrm{G}_2\sqcup\{0\}$. De plus, si $x\in \mathrm{G}_2\sqcup\{0\}$ alors $-x=x\in \mathrm{G}_2\sqcup\{0\}$. Enfin, pour $x,y\in \mathrm{G}_2\sqcup\{0\}$, on a $2(x+y)=2x+2y=0$ (puisque G est abélien). Ainsi $x+y\in \mathrm{G}_2\sqcup\{0\}$.

L'exemple 6.29 de [BPM] assure alors que $\mathrm{G}_2\sqcup\{0\}$ est un $\mathbb{F}_2$-espace vectoriel (de dimension finie puisque G est fini). Le lemme 9 donne alors le résultat puisque $\dim_{\mathbb{F}_2}(\mathrm{G}_2\sqcup\{0\})=1$ si et seulement si G_2 est réduit à un singleton. ∎

On peut à présent énoncer et démontrer la généralisation du théorème de Wilson due à Gauss. Sa démonstration repose de façon essentielle sur la structure des groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ (où p est premier et $\alpha\in\mathbb{N}$).

Corollaire 11 – Un résultat de Gauss. Soit $n\in\mathbb{N}^*$. On a alors

$$\prod_{\substack{1\leqslant x<n\\ x\wedge n=1}} x \quad = \begin{cases} -1\,[n] & \text{si } n\in\{4,p^\alpha,2p^\alpha,\quad \text{où } p\in\mathscr{P}\smallsetminus\{2\} \text{ et } \alpha\in\mathbb{N}^*\}\\ 1\,[n] & \text{sinon}\,. \end{cases}$$

Preuve. On note $\pi:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Comme un élément $x\in[\![\,1\,,\,n-1\,]\!]$ vérifie $x\wedge n=1$ si et seulement si $\pi(x)$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ admet un unique représentant dans $[\![\,1\,,\,n-1\,]\!]$ (voir [PER, proposition 7.1]), il s'agit en fait de calculer

$$\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x\,.$$

Commençons par les cas $n\in\{1,2\}$. Dans chacun des deux cas, $(\mathbb{Z}/n\mathbb{Z})^\times$ est réduit au singleton $\{1\}$. Le résultat est alors évident. Considérons à présent $n\notin\{1,2\}$. Dans ce cas, -1 est un élément d'ordre 2 de $(\mathbb{Z}/n\mathbb{Z})^\times$ puisque $(-1)^2=1$ et $-1\neq 1$ (si $n\in\{1,2\}$, on a $-1=1$). D'après le corollaire 10, il suffit de montrer que -1 est le seul élément d'ordre 2 de $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $n\in\{4,p^\alpha,2p^\alpha,\quad \text{où } p\in\mathscr{P}\smallsetminus\{2\} \text{ et } \alpha\in\mathbb{N}^*\}$. Cela va résulter de la structure des groupes $(\mathbb{Z}/n\mathbb{Z})^\times$ (voir [PER, proposition 7.4 à 7.11]).

Dans un premier temps, on va montrer que si $(\mathbb{Z}/n\mathbb{Z})^\times$ a un unique élément d'ordre 2 alors

$$n\in\{2^\alpha,p^\alpha,2p^\alpha,\quad \text{où } p\in\mathscr{P}\smallsetminus\{2\}\,,\ \alpha\in\mathbb{N}^* \text{ et } \beta\geqslant 3\}\,.$$

Cette implication nécessite très peu de résultats sur la structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$: on utilise juste le théorème chinois (voir [BPM, Théorème 5.29]) et le cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ pour p premier et $\alpha\in\mathbb{N}^*$. L'implication réciproque, quant à elle, nécessite l'étude précise de la structure des $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ pour p premier et $\alpha\in\mathbb{N}^*$ et permettra d'éliminer les cas 2^β avec $\beta\geqslant 3$

On suppose donc que $(\mathbb{Z}/n\mathbb{Z})^\times$ a un unique élément d'ordre 2. On considère la décomposition de n en nombre premier

$$n = {p_1}^{\alpha_1} \cdots {p_s}^{\alpha_s} \qquad \text{avec} \qquad p_i \in \mathscr{P},\ p_i \neq p_j \text{ si } i \neq j \text{ et } \alpha_i \in \mathbb{N}^*.$$

Grâce au théorème chinois, on obtient que

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/{p_1}^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/{p_s}^{\alpha_s}\mathbb{Z})^\times$$

Supposons qu'il existe deux nombres premiers impairs $p_i \neq p_j$ qui apparaissent dans la décomposition de n en facteur premier. Dans ce cas, $(\mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z})^\times$ et $(\mathbb{Z}/{p_j}^{\alpha_j}\mathbb{Z})^\times$ sont deux groupes abéliens d'ordre respectif ${p_i}^{\alpha_i-1}(p_i-1)$ et ${p_j}^{\alpha_j-1}(p_j-1)$ qui sont des nombres pairs. En particulier, ils contiennent chacun un élément d'ordre deux (qu'on note respectivement u et v). Le produit

$$(\mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z})^\times \times (\mathbb{Z}/{p_j}^{\alpha_j}\mathbb{Z})^\times$$

contient donc au moins trois éléments d'ordre 2 (les couples $(1,v)$ et $(u,1)$ et (u,v)) et donc $(\mathbb{Z}/n\mathbb{Z})^\times$ aussi. On aboutit à une contradiction. On en déduit que $n = 2^\beta p^\alpha$ avec $\beta, \alpha \in \mathbb{N}$ et p nombre premier impair. Supposons alors $\beta \geqslant 2$ et $\alpha \geqslant 1$. Dans ce cas, $(\mathbb{Z}/2^\beta\mathbb{Z})^\times$ et $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ sont deux groupes abéliens d'ordre respectif $2^{\beta-1}$ et $p^{\alpha-1}(p-1)$ qui sont des nombres pairs (puisque $\beta \geqslant 2$). En particulier, ils contiennent chacun un élément d'ordre deux. Comme ci-dessus, on en déduit que $(\mathbb{Z}/n\mathbb{Z})^\times$ contient au moins trois éléments d'ordre 2. On en déduit que n est de la forme 2^β (cas $\alpha = 0$) ou p^α ou $2p^\alpha$ (cas $\beta < 2$) avec $\beta \geqslant 2$ (on a éliminé le cas $n = 2$), p nombre premier impair et $\alpha \geqslant 1$.

Étudions à présent la réciproque. Supposons que $n = p^\alpha$ avec p nombre premier impair et $\alpha \geqslant 1$. D'après la proposition 7.6 de [PER], $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique d'ordre $p^{\alpha-1}(p-1)$ qui est pair. Ainsi $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ admet un unique élément d'ordre 2. Supposons que $n = 2p^\alpha$ avec p nombre premier impair et $\alpha \geqslant 1$. D'après le théorème chinois, on a $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times = (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ qui est cyclique d'ordre pair (comme on vient de le voir) et admet donc un unique élément d'ordre 2. Enfin, si $n = 2^\beta$ avec $\beta \geqslant 2$ alors, d'après la proposition 7.10 de [PER], on a $(\mathbb{Z}/2^\beta\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\beta-2}\mathbb{Z}$ qui a au moins (et même exactement) trois éléments d'ordre 2 si $\beta \geqslant 3$ puisqu'alors $2^{\beta-2}$ est pair et $\mathbb{Z}/2^{\beta-2}\mathbb{Z}$ contient donc un élément d'ordre 2. Si $\beta = 2$ alors $n = 4$ et $(\mathbb{Z}/4\mathbb{Z})^\times = \{-1, 1\}$ a bien un unique élément d'ordre 2. ∎

Remarque 12 – Lorsque n est premier. Lorsque n est un entier premier, le corollaire 11 redonne exactement le théorème de Wilson. ∎

Congruence et coefficients binomiaux.

Le théorème de Wilson étudie la congrence d'une factorielle. Que se passe-t-il pour les coefficients binomiaux ? On donne une réponse très partielle dans le lemme 13 qui suit. Bien que sans rapport avec le théorème de Wilson, on donne l'égalité (**1**) car elle est fondamentale dans tous les calculs en caractéristique p (voir la remarque 14). Malgré sa moindre importance, on mentionne aussi l'égalité (**2**) puisqu'on en donne une démonstration reposant sur le théorème de Wilson.

Lemme 13 – Congruence et coefficients binomiaux. Soit p un nombre premier. On a alors

$$\forall\, k \in [\![1\,,\, p-1]\!], \qquad \binom{p}{k} = 0\,[p] \tag{1}$$

et

$$\forall\, k \in [\![0\,,\, p-1]\!], \qquad \binom{p-1}{k} = (-1)^k\,[p]\,. \tag{2}$$

Preuve. Commençons par l'égalité (**1**). On en donne trois preuves.

Première preuve. Il s'agit de la preuve la plus commune : elle repose sur de l'arithmétique élémentaire : le lemme de Gauss. On a

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!}\,.$$

Ainsi $k!\mathrm{C}_p^k = p(p-1)\cdots(p-k+1)$. Comme $k > 0$, on a $p \mid p(p-1)\cdots(p-k+1)$ (c'est un produit de k facteurs avec $k > 0$ et qui « commence » par p). Comme $k \leqslant p-1$, $p \nmid k!$ puisque p ne divise aucun des entiers inférieurs ou égaux à k. Comme p est premier, le lemme de Gauss assure que $p \mid \mathrm{C}_p^k$.

Deuxième preuve. Il s'agit de la preuve proposée dans le corollaire 2.8 de [DMZ]. Dans la première démonstration du théorème de Wilson, on a montré l'égalité suivante dans $\mathbb{F}_p[\mathrm{X}]$

$$\prod_{x \in {\mathbb{F}_p}^\times} (\mathrm{X} - x) = \mathrm{X}^{p-1} - 1\,.$$

En multipliant par $\mathrm{X} = \mathrm{X} - 0$, on obtient alors l'égalité

$$\prod_{x \in \mathbb{F}_p} (\mathrm{X} - x) = \mathrm{X}^p - \mathrm{X}\,.$$

Par ailleurs, l'application $x \mapsto x - 1$ est une bijection de $\mathbb{F}_p$ (d'inverse $x \mapsto x + 1$). On en déduit que

$$\prod_{x\in\mathbb{F}_p}(\mathrm{X}-x)=\prod_{x\in\mathbb{F}_p}(\mathrm{X}-(x-1))=\prod_{x\in\mathbb{F}_p}((\mathrm{X}+1)-x)=(\mathrm{X}+1)^p-(\mathrm{X}+1)\,.$$

On obtient donc $(\mathrm{X}+1)^p-\mathrm{X}-1=\mathrm{X}^p-\mathrm{X}$ c'est-à-dire $(\mathrm{X}+1)^p=\mathrm{X}^p+1$. En développant $(\mathrm{X}+1)^p$ avec la formule du binôme de Newton, on obtient que $\mathrm{C}_p^k=0$ dans $\mathbb{F}_p$ c'est-à-dire $p\mid\mathrm{C}_p^k$.

Troisième preuve. Par définition, C_p^k est le nombre de parties à k éléments d'un ensemble à p éléments. Pour démontrer l'égalité souhaité, on va choisir un « bon » ensemble à p éléments (en fait $\mathbb{Z}/p\mathbb{Z}$) et faire agir un p-groupe (en fait $\mathbb{Z}/p\mathbb{Z}$) sur l'ensemble des parties à k éléments de notre ensemble à k éléments. Comme le cardinal d'une orbite divise le cardinal du groupe qui agit (voir [PER, Chapitre 1 proposition 4.7]), on en déduit que les orbites ont pour cardinal une puissance de p et donc si aucune orbite n'est réduite à un point, elles ont toutes un cardinal divisible par p et le nombre totale de partie à k éléments est divisible par p.

On considère donc l'ensemble à p éléments $\mathbb{Z}/p\mathbb{Z}$ et on note $\mathscr{P}_k$ l'ensemble des parties à k éléments de $\mathbb{Z}/p\mathbb{Z}$. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur $\mathscr{P}_k$ de la façon suivante

$$m\colon\begin{cases}\mathbb{Z}/p\mathbb{Z}\times\mathscr{P}_k\longrightarrow\mathscr{P}_k\\ \quad(x,\mathrm{E})\quad\longmapsto x+\mathrm{E}=\{x+y,\quad y\in\mathrm{E}\}\ .\end{cases}$$

L'application m est bien définie puisque $x+\mathrm{E}$ a le même nombre d'éléments que E (puisque l'application $y\mapsto x+y$ est une bijection de $\mathbb{Z}/p\mathbb{Z}$). De plus, on a $0+\mathrm{E}=\mathrm{E}$ et $(x+x')+\mathrm{E}=x+(x'+\mathrm{E})$ pour tout $x,x'\in\mathbb{Z}/p\mathbb{Z}$ et $\mathrm{E}\in\mathscr{P}_k$. On va montrer qu'il n'existe pas d'orbites ponctuelles pour cette action lorsque $k\in[\![1\,,\,p-1]\!]$. Soit $\mathrm{E}\in\mathscr{P}_k$. Comme $k\in[\![1\,,\,p-1]\!]$, il existe $i\in\mathrm{E}$ et $j\notin\mathrm{E}$. On a donc $j\in(j-i)+\mathrm{E}$ et $j-i+\mathrm{E}\neq\mathrm{E}$. Ainsi l'orbite de E sous $\mathbb{Z}/p\mathbb{Z}$ n'est pas ponctuelle. Comme le cardinal de l'orbite de E est un diviseur de celui de $\mathbb{Z}/p\mathbb{Z}$ (voir [PER, Chapitre 1 proposition 4.7]), on obtient que le cardinal de l'orbite de E est p. On a donc découpé $\mathscr{P}_k$ en partie à p éléments. Ainsi $|\mathscr{P}_k|=\mathrm{C}_p^k$ est divisible par p.

Passons à l'égalité (**2**). On en donne aussi trois preuves.

Première preuve. Dans la deuxième preuve de l'égalité (**1**), on a vu l'identité $(\mathrm{X}+1)^p=\mathrm{X}^p+1$ dans $\mathbb{F}_p[\mathrm{X}]$. Lorsqu'on connait l'égalité (**1**), cette identité s'obtient de façon immédiate en développant grâce à la formule du binôme de Newton. Lorsque p est impair, en divisant l'identité précédente par $(\mathrm{X}+1)$, on obtient alors

$$(\mathrm{X}+1)^{p-1}=\mathrm{X}^{p-1}+(-1)\mathrm{X}^{p-2}+\cdots+(-1)^{p-1}.$$

En développant le premier terme avec la formule du binôme de Newton, on obtient alors $\mathrm{C}_{p-1}^k=(-1)^k$ dans $\mathbb{F}_p$ c'est-à-dire $\mathrm{C}_{p-1}^k=(-1)^k\,[p]$.

Deuxième preuve. On a $(p-1-k)!k!\mathrm{C}_{p-1}^k=(p-1)!$. En réduisant cette égalité modulo p, le théorème 2 de Wilson et le corollaire 5 donne $(-1)^{k+1}\mathrm{C}_{p-1}^k=-1$.

Troisième preuve. D'après le triangle de Pascal, on a $\mathrm{C}_{p-1}^k+\mathrm{C}_{p-1}^{k+1}=\mathrm{C}_p^{k+1}$ pour tout $k\in[\![0\,,\,p-2]\!]$. Comme $k+1\in[\![1\,,\,p-1]\!]$, l'égalité (**1**) assure que $\mathrm{C}_{p-1}^k+\mathrm{C}_{p-1}^{k+1}=0\,[p]$. Ainsi $\mathrm{C}_{p-1}^k=-\mathrm{C}_{p-1}^{k+1}\,[p]$ pour tout $k\in[\![0\,,\,p-2]\!]$. Comme $\mathrm{C}_{p-1}^0=1$, on en déduit que $\mathrm{C}_{p-1}^k=(-1)^k\,[p]$. ∎

Remarque 14 – Morphisme de Frobenius. L'égalité (**1**) du lemme 13 est extrêmement importante parce que c'est elle qui assure le fait que le morphisme de Frobenius soit bien un morphisme.

De façon précise, soient p un nombre premier et A un anneau commutatif unitaire de caractéristique p. L'application

$$\mathrm{F}\colon\begin{cases}\mathrm{A}\longrightarrow\mathrm{A}\\ x\longmapsto x^p\end{cases}$$

est un morphisme d'anneaux unitaires qu'on appelle *morphisme de Frobenius de* A. On a bien sûr $\mathrm{F}(1)=1$. On a aussi $\mathrm{F}(xy)=(xy)^p=x^py^p=\mathrm{F}(x)\mathrm{F}(y)$ pour tous $x,y\in\mathrm{A}$ puisque A est commutatif. Ainsi pour montrer que F est un morphisme d'anneaux, il suffit de montrer que $\mathrm{F}(x+y)=\mathrm{F}(x)+\mathrm{F}(y)$ pour tous $x,y\in\mathrm{A}$. Or, d'après la formule du binôme de Newton (qu'on peut appliquer puisque A est un anneau commutatif) et l'égalité (**1**), on peut écrire

$$\mathrm{F}(x+y)=\sum_{k=0}^{p}\binom{p}{k}x^ky^{p-k}=x^p+y^p+\sum_{k=1}^{p-1}\binom{p}{k}x^ky^{p-k}=x^p+y^p+\sum_{k=1}^{p-1}pu_k\,x^ky^{p-k}=\mathrm{F}(x)+\mathrm{F}(y)+\sum_{k=1}^{p-1}pu_k\,x^ky^{p-k}$$

où $pu_k=\mathrm{C}_p^k$. Or dans un anneau de caractéristique p, on a $px=0$ pour tout x (puisque $px=(p1_\mathrm{A})x$ et que $p1_\mathrm{A}=0$ par définition de la caractéristique d'un anneau). Ainsi $\mathrm{F}(x+y)=\mathrm{F}(x)+\mathrm{F}(y)$. ∎

Références

[BPM] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K, 2005.

[BOR] Folkmar Bornemann. Primes is in p, une avancée accessible à « l'homme ordinaire ». *Gazette des mathématiciens*, 98 :p.14–29, 2003.

[DMZ] M. Demazure. *Cours d'algèbre. Primalité, divisibilité, codes.* Cassini, 1997.

[LAG] J.-L. Lagrange. Démonstration d'un théorème nouveau concernant les nombres premiers. *Lu à l'académie de Berlin*, 1771.

[PER] Daniel Perrin. *Cours d'algèbre*. Ellipse, 1996.

[RAS] R. Rashed. Ibn al-haytham et le théorème de wilson. *Archive for History of exact Sciences*, 22 :p.305–321, 1980.