Christophe Bertault

Une identité remarquable au service de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$

Si le résultat suivant est classique, la preuve élémentaire qu'on en propose dans cette courte note l'est sans doute moins. Il est même possible qu'elle soit inédite.

Théorème **(Structure du groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$)** Pour tout nombre premier p, le groupe multiplicatif $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est cyclique.

Plusieurs démonstrations simples de ce théorème coexistent dans la littérature, mais toutes reposent sur une théorie préalable des polynômes, en l'occurrence sur le fait que sur un corps le polynôme X^n-1 possède au plus n racines pour tout $n\in\mathbb{N}^*$. Je me propose de contourner ce résultat à moindre frais et c'est en ce sens que la preuve proposée ici est plus élémentaire que les preuves usuelles.

L'essentiel sera tiré de l'identité remarquable que voici.

Théorème **(Le fond de l'affaire)** Pour tous $n\in\mathbb{N}^*$ et $r\in[\![1,n]\!]$:
$$\sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k}\left(k^r-1\right)=\begin{cases}n!+(-1)^n & \text{si } r=n\\ (-1)^n & \text{si } r<n.\end{cases}$$

Nous proposerons cinq preuves de cette identité en fin de texte, désormais notée ★, mais nous allons d'abord tâcher d'en déduire le résultat annoncé. Nous en tirerons d'ailleurs deux théorèmes pour le prix d'un :

— le *théorème de Wilson* rappelé ci-dessous à partir du cas $r=n$,

— la structure cyclique du groupe multiplicatif $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ à partir des autres cas.

Le théorème de Lagrange sur l'ordre d'un élément dans un groupe est supposé connu — donc le petit théorème de Fermat aussi.

Théorème **(Théorème de Wilson)** Pour tout nombre premier p : $\quad(p-1)!\equiv-1\ [p]$.

On démontre d'ordinaire le théorème de Wilson en calculant le produit de tous les éléments du groupe multiplicatif abélien $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, lequel vaut -1 car tous les termes y meurent de leur inverse, 1 et -1 exceptés. Il est bien sûr difficile d'imaginer preuve plus courte et plus éclairante. La présente note n'y prétend pas et la preuve qui suit du théorème de Wilson n'est d'ailleurs pas originale, on la rencontre ici ou là.

Démonstration D'après ★ : $\quad(p-1)!+(-1)^{p-1}=\sum_{k=1}^{p-1}(-1)^{p-k-1}\binom{p-1}{k}\left(k^{p-1}-1\right)\overset{\text{Fermat}}{\equiv}0\ [p]$, donc $(p-1)!\equiv(-1)^p\ [p]$. Que p soit impair ou non : $\quad(p-1)!\equiv-1\ [p]$. ∎

À présent, pour montrer que le groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est cyclique, i.e. pour justifier l'existence d'un élément primitif modulo p, nous aurons besoin du lemme suivant. On y note $|g|$ l'ordre de g pour tout élément g d'un groupe quelconque.

Théorème **(Ordre d'un produit ou d'une puissance dans un groupe)** Soient G un groupe et $x,y\in G$ deux éléments d'ordre fini.

(i) Si x et y commutent et si $|x|$ et $|y|$ sont premiers entre eux : $\quad|xy|=|x|\times|y|$.

(ii) Pour tout diviseur d de $|x|$: $\quad\left|x^d\right|=\frac{|x|}{d}$.

Démonstration

(i) Comme x et y commutent : $(xy)^{|x|\times|y|} = \big(x^{|x|}\big)^{|y|}\big(y^{|y|}\big)^{|x|} = 1$, donc $|x|\times|y|$ est divisible par $|xy|$. Inversement $(xy)^{|xy|} = 1$ et x et y commutent, donc $x^{|xy|} = y^{-|xy|}$, puis $x^{|y|\times|xy|} = \big(y^{|y|}\big)^{-|xy|} = 1$, de sorte que $|y|\times|xy|$ est divisible par $|x|$. Comme $|x|$ et $|y|$ sont premiers entre eux, il en découle que $|xy|$ est divisible par $|x|$, mais donc aussi par $|y|$ par symétrie des rôles de x et y, et d'ailleurs même par leur produit $|x|\times|y|$.

(ii) L'entier $\dfrac{|x|}{d}$ est divisible par $\left|x^d\right|$ car $\left(x^d\right)^{\frac{|x|}{d}} = x^{|x|} = 1$.
Inversement $x^{d\times|x^d|} = \big(x^d\big)^{|x^d|} = 1$, donc $d\times\left|x^d\right|$ est divisible par $|x|$, donc $\left|x^d\right|$ l'est par $\dfrac{|x|}{d}$. ∎

Armés de ce lemme, nous sommes en mesure de « construire » un élément primitif modulo p.

Démonstration **(de l'existence d'un élément primitif modulo p)** Soit p un nombre premier supérieur ou égal à 3.

- Pour tout diviseur STRICT d de $p-1$, d'après ★ : $\displaystyle\sum_{k=1}^{p-1}(-1)^{p-k-1}\binom{p-1}{k}\big(k^d-1\big) = (-1)^{p-1} \not\equiv 0\ [p]$.
  Cette non-congruence à 0 modulo p oblige l'un des termes de la somme à être lui-même non congru à 0 modulo p. Ainsi $k^d \not\equiv 1\ [p]$ pour un certain $k\in[\![1,p-1]\!]$, donc le groupe $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ contient un élément d'ordre ne divisant pas d. L'essentiel est maintenant fait et l'hypothèse $d\neq p-1$ a été décisive.

- Écrivons à présent la factorisation première de $p-1$: $p-1 = q_1^{\alpha_1}\dots q_r^{\alpha_r}$ où $q_1,\dots,q_r$ sont des nombres premiers distincts et $\alpha_1,\dots,\alpha_r\in\mathbb{N}^*$. Fixons $i\in[\![1,r]\!]$. D'après le point précédent, $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ contient un élément x_i dont l'ordre ne divise pas $\dfrac{p-1}{q_i}$, mais divise $p-1$ d'après le théorème de Lagrange. Nécessairement, $|x_i|$ est divisible par $q_i^{\alpha_i}$, donc si on pose $y_i = x_i^{q_i^{-\alpha_i}|x_i|}$, y_i est d'ordre $q_i^{\alpha_i}$. Finalement, le groupe $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ étant abélien, le produit $y_1\dots y_r$ est d'ordre $q_1^{\alpha_1}\dots q_r^{\alpha_r} = p-1$. Il n'en fallait pas plus. ∎

En résumé, l'existence d'un élément primitif modulo p a découlé d'une simple non-congruence à 0 modulo p, un peu comme l'existence d'éléments centraux non triviaux dans un p-groupe fini découle d'une congruence à 0 modulo p dans l'équation aux classes.

Il ne nous reste finalement plus qu'à démontrer l'identité remarquable ★. Nous en donnerons plusieurs preuves dont certaines à base de polynômes, même si de telles preuves contrarient notre souhait initial d'une démonstration sans polynômes de la structure cyclique de $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.

Comme pour tout $n\in\mathbb{N}^*$: $\displaystyle\sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k} = (1-1)^n - \overbrace{(-1)^n}^{k=0} = -(-1)^n$, il nous suffit de montrer que pour tout $r\in[\![1,n]\!]$: $\displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r = \begin{cases} n! & \text{si } r=n \\ 0 & \text{si } r<n \end{cases}$ — et ceci est d'ailleurs est vrai pour $n=0$ et $r=0$.

Démonstration **(n°1, analytique, à partir de la formule du binôme et de la fonction exponentielle)** Soient $n\in\mathbb{N}$ et $r\in[\![0,n]\!]$. Tout simplement : $\displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\mathrm{e}^{kx} = (\mathrm{e}^x-1)^n \underset{x\to 0}{=} x^n + \mathrm{o}\big(x^n\big)$, donc par unicité des coefficients d'un développement limité en 0, à l'ordre r : $\dfrac{1}{r!}\displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r = \begin{cases} 1 & \text{si } r=n \\ 0 & \text{si } r<n. \end{cases}$ ∎

Démonstration **(n°2, combinatoire, à partir de la formule du crible)** Soient $n\in\mathbb{N}^*$ et $r\in[\![1,n]\!]$. Pour tout $i\in[\![1,n]\!]$, notons A_i l'ensemble des applications de $[\![1,r]\!]$ dans $[\![1,n]\!]$ dont l'image ne contient pas i. Dans $[\![1,n]\!]^{[\![1,r]\!]}$, $\overline{A_1\cup\dots\cup A_n}$ est exactement l'ensemble des surjections de $[\![1,r]\!]$ dans $[\![1,n]\!]$. Par conséquent :

$$\left|\overline{A_1\cup\dots\cup A_n}\right| = \begin{cases} 0 & \text{si } r\in[\![1,n-1]\!] \\ n! & \text{si } r=n. \end{cases}$$

Indépendamment, pour tous $k\in[\![1,n]\!]$ et $i_1,\dots,i_k\in[\![1,n]\!]$ distincts, $A_{i_1}\cap\dots\cap A_{i_k}$ est l'ensemble des applications de $[\![1,r]\!]$ dans $[\![1,n]\!]\setminus\{i_1,\dots,i_k\}$, donc $\left|A_{i_1}\cap\dots\cap A_{i_k}\right| = (n-k)^r$. Enfin, l'ensemble des k-listes strictement croissantes de $[\![1,n]\!]$ est de cardinal $\binom{n}{k}$, donc d'après la formule du crible :

$$\left|A_1\cup\ldots\cup A_n\right| = \sum_{k=1}^{n}(-1)^{k+1}\sum_{1\leqslant i_1<\ldots<i_k\leqslant n}\left|A_{i_1}\cap\ldots\cap A_{i_k}\right| = \sum_{k=1}^{n}(-1)^{k+1}\sum_{1\leqslant i_1<\ldots<i_k\leqslant n}(n-k)^r = \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}(n-k)^r \overset{l=n-k}{=} -\sum_{l=0}^{n-1}(-1)^{n-l}\binom{n}{l}l^r.$$

Finalement : $\displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r = n^r + \sum_{k=0}^{n-1}(-1)^{n-k}\binom{n}{k}k^r = \left|[\![1,n]\!]^r\right| - \left|A_1\cup\ldots\cup A_n\right| = \left|\overline{A_1\cup\ldots\cup A_n}\right|$, ce qui est exactement le résultat attendu. ∎

Cette deuxième preuve a le mérite d'offrir une interprétation combinatoire simple à l'entier $\displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r$ pour tous $n,r\in\mathbb{N}^*$ — y compris pour $r>n$. Cet entier, en l'occurrence, est exactement le nombre de surjections de $[\![1,r]\!]$ dans $[\![1,n]\!]$.

Démonstration **(n°3, par récurrence, à partir des propriétés des coefficients binomiaux)** Pour tous $n,r\in\mathbb{N}$, posons : $S_{n,r} = \displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r$. Pour tous $n\in\mathbb{N}$ et $k\in\mathbb{Z}$: $\displaystyle\binom{n}{k}k = n\binom{n-1}{k-1} \overset{\text{Pascal}}{=} n\left(\binom{n}{k}-\binom{n-1}{k}\right)$,

donc pour tout $r\in\mathbb{N}$: $\displaystyle S_{n,r+1} = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^{r+1} = n\sum_{k=0}^{n}(-1)^{n-k}\left(\binom{n}{k}-\binom{n-1}{k}\right)k^r = n\left(S_{n,r}+S_{n-1,r}\right)$.

Nous allons maintenant démontrer par récurrence sur r que pour tout $n\geqslant r$: $S_{n,r} = \begin{cases} n! & \text{si } r=n \\ 0 & \text{si } r<n. \end{cases}$

Initialisation : Pour tout $n\geqslant 0$: $\displaystyle S_{n,0} = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k} = 0^n = \begin{cases} 1 & \text{si } n=0 \\ 0 & \text{si } n>0. \end{cases}$

Hérédité : Soit $r\in\mathbb{N}$. Si la proposition à démontrer est vraie au rang r, alors d'une part :

$$S_{r+1,r+1} = (r+1)\left(S_{r+1,r}+S_{r,r}\right) \overset{\text{HDR}}{=} (r+1)\left(0+r!\right) = (r+1)!,$$

et d'autre part, pour tout $n>r+1$: $S_{n,r+1} = n\left(S_{n,r}+S_{n-1,r}\right) = n(0+0) = 0$. ∎

Démonstration **(n°4, polynomiale, à partir d'une interpolation de Lagrange)** Soient $n\in\mathbb{N}^*$ et $r\in[\![0,n]\!]$. Notons $L_0,\ldots,L_n$ les polynômes de Lagrange des réels $0,1,\ldots,n$. De degré inférieur ou égal à n, le polynôme X^r est l'unique polynôme $P\in\mathbb{R}_n[X]$ pour lequel $P(k)=k^r$ pour tout $k\in[\![0,n]\!]$, donc sa décomposition dans la base $(L_1,\ldots,L_n)$ de $\mathbb{R}_n[X]$ s'écrit $X^r = \displaystyle\sum_{k=0}^{n}k^rL_k$.

Intéressons-nous alors simplement au coefficient de degré n des deux côtés de cette identité. À gauche, il vaut $\begin{cases} 1 & \text{si } r=n \\ 0 & \text{si } r<n, \end{cases}$ et sachant que $\displaystyle L_k = \prod_{\substack{0\leqslant i\leqslant n\\ i\neq k}}\frac{X-i}{k-i}$ pour tout $k\in[\![0,n]\!]$, il vaut à droite :

$$\sum_{k=0}^{n}k^r\prod_{\substack{0\leqslant i\leqslant n\\ i\neq k}}\frac{1}{k-i} = \sum_{k=0}^{n}\frac{k^r}{k(k-1)\ldots1\times(-1)(-2)\ldots(k-n)} = \sum_{k=0}^{n}\frac{(-1)^{n-k}k^r}{l!(n-k)!} = \frac{1}{n!}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r.$$

De nouveau, c'est le résultat attendu. ∎

Notre dernière preuve nous oblige à changer légèrement de perspective. Pour tout $n\in\mathbb{N}$, si on admet les $n+1$ identités ★ obtenues quand on fait varier r de 0 à n :

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}(X+k)^n = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\sum_{r=0}^{n}\binom{n}{r}k^rX^{n-r} = \sum_{r=0}^{n}\binom{n}{r}\underbrace{\left(\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^r\right)}_{0 \text{ ou } n!}X^{n-r} = n!.$$

De fait, l'identité polynomiale : $\displaystyle\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}(X+k)^n = n!$ est même équivalente aux identités ★ et c'est elle que nous allons établir directement.

Démonstration (n°5, polynomiale, à partir d'une identité synthétique)

Posons pour tout $n \in \mathbb{N}$: $P_n(X) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} (X+k)^n$. Le polynôme P_n est de degré au plus $n-1$ pour tout $n \in \mathbb{N}^*$ car son coefficient de degré n vaut $\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} = (1-1)^n = 0$.

À présent, pour tout $n \in \mathbb{N}$:
$$\begin{aligned} P_{n+1}(X) &= \sum_{k=0}^{n+1} (-1)^{n-k+1} \binom{n+1}{k} (X+k)^n \times (X+k) \\ &= X \sum_{k=0}^{n+1} (-1)^{n-k+1} \binom{n+1}{k} (X+k)^n + \sum_{k=0}^{n+1} (-1)^{n-k+1} \binom{n+1}{k} k (X+k)^n \\ &= \frac{X}{n+1} P'_{n+1}(X) + (n+1) \sum_{k=0}^{n+1} (-1)^{n-k+1} \binom{n}{k-1} (X+k)^n \\ &\overset{l=k+1}{=} \frac{X}{n+1} P'_{n+1}(X) + (n+1) \sum_{l=0}^{n} (-1)^{n-l} \binom{n}{l} (X+l+1)^n \\ &= \frac{X}{n+1} P'_{n+1}(X) + (n+1) P_n(X+1), \end{aligned}$$
puis après réorganisation :
$$\left(\frac{P_{n+1}(X)}{X^{n+1}} \right)' = \frac{X^{n+1} P'_{n+1}(X) - (n+1) X^n P_{n+1}(X)}{X^{2n+2}} = \frac{X P'_{n+1}(X) - (n+1) P_{n+1}(X)}{X^{n+2}} = -\frac{(n+1)^2 P_n(X+1)}{X^{n+2}}.$$
Nous pouvons maintenant enfin montrer par récurrence que $P_n(X) = n!$ pour tout $n \in \mathbb{N}$.

Initialisation : Triviale !

Hérédité : Soit $n \in \mathbb{N}$. Faisons l'hypothèse que $P_n(X) = n!$. Dans ce cas : $\left(\frac{P_{n+1}(X)}{X^{n+1}} \right)' = (n+1)! \left(\frac{1}{X^{n+1}} \right)'$, donc $\frac{P_{n+1}(X)}{X^{n+1}} = \frac{(n+1)!}{X^{n+1}} + \lambda$ pour un certain $\lambda \in \mathbb{R}$. Comme P_{n+1} est de degré au plus n, il en découle que $P_{n+1}(X) = (n+1)!$. ■