Une application combinatoire du théorème de Chevalley-Warning

Richard Leroy

richard.leroy@univ-rennes1.fr
http ://perso.univ-rennes1.fr/richard.leroy/

Préparation à l'agrégation de Mathématiques 2008
Université de Rennes 1

On démontre dans cette note le résultat suivant :

Théorème 1 *Parmi $2n-1$ entiers ($n \geq 1$), il existe un sous-ensemble de cardinal n dont la somme des éléments est divisible par n.*

Preuve :
Notons $\mathfrak{P}_n$ la propriété à démontrer.

• Il s'agit d'une propriété multiplicative : si $n, m \geq 1$, alors $\mathfrak{P}_n$ et $\mathfrak{P}_m$ impliquent $\mathfrak{P}_{mn}$.

Soient en effet $a_1, \ldots, a_{2mn-1}$ des entiers relatifs. On choisit $2n-1$ éléments parmi ces entiers. Il existe un ensemble I_1 de cardinal n, tel que

$$\sum_{i \in I_1} a_i \equiv 0 \mod n.$$

On retire les n entiers et on recommence le procédé. On construit ainsi $2m-1$ ensembles $I_1, \ldots I_{2m-1}$ de cardinal n et disjoints, tels que

$$S_j = \sum_{i \in I_j} a_i \equiv 0 \mod n.$$

On pose $S'_j = S_j/n$. Parmi les $2m-1$ entiers $S'_1, \ldots, S'_{2m-1}$, il existe un ensemble J de cardinal m tel que

$$\sum_{j \in J} S'_j = 0 \mod m.$$

Finalement, $\displaystyle\sum_{j\in J}\sum_{i\in I_j} a_i$ est divisible par mn.

• La propriété étant multiplicative, il suffit de montrer $\mathfrak{P}_p$ pour tout nombre premier p.

Soit $(a_1,\ldots,a_{2p-1}) \in (\mathbb{F}_p)^{2p-1}$. On veut montrer que l'on peut trouver p éléments dont la somme est nulle.
On va montrer que le système

$$\left\{\begin{array}{ccccc} P & = & a_1X_1^{p-1}+\cdots+a_{2p-1}X_{2p-1}^{p-1} & = & 0 \\ Q & = & X_1^{p-1}+\cdots+X_{2p-1}^{p-1} & = & 0 \end{array}\right.$$

a des solutions non triviales.

Soit $V \subset (\mathbb{F}_p)^{2p-1}$ l'ensemble de ces solutions, et $\alpha = \mathrm{Card}(V) \mod p$.
On pose $R = (1-P^{p-1})(1-Q^{p-1})$.
On a alors l'équivalence $x \in V \Leftrightarrow R(x) = 1$, et sinon, $R(x) = 0$.
Par conséquent, $\alpha = \displaystyle\sum_{x\in\mathbb{F}_p^{2p-1}} R(x)$. On veut montrer que α est nul. En écrivant R sous la forme d'une somme de monômes, il suffit de montrer que la somme est déjà nulle si R est un monôme de la forme $X_1^{i_1}\ldots X_{2p-1}^{i_{2p-1}}$, avec $i_1+\cdots i_{2p-1} \leq (2p-2)(p-1)$:

$$\sum_{x\in(\mathbb{F}_p)^{2p-1}} x_1^{i_1}\ldots x_{2p-1}^{i_{2p-1}} = \prod_{k=1}^{2p-1}\sum_{x\in\mathbb{F}_p} x^{i_k} = \prod_{k=1}^{2p-1}\sum_{x\in\mathbb{F}_p^*} x^{i_k}.$$

Il existe un k tel que $i_k < p-1$: sinon,

$$\sum_{k=1}^{2p-1} i_k \geq (2p-1)(p-1) > (2p-2)(p-1).$$

$\mathbb{F}_p^*$ est cyclique, donc il existe $x_0 \in \mathbb{F}_p^*$ tel que

$$\sum_{x\in\mathbb{F}_p^*} x^{i_k} = \sum_{k=0}^{p-2}\left(x_0^k\right)^{i_k} = \frac{1-(x_0^{i_k})^{p-1}}{1-x_0^{i_k}} = 0,$$

puisque $x_0^{i_k} \neq 1$.

Finalement, $\alpha = 0$, c'est à dire $\mathrm{Card}(V)$ est divisible par p.

Or, V contient clairement le vecteur nul, donc contient aussi un élément non nul x. Soit $I = \{1 \leq i \leq 2p-1 | x_i \neq 0\}$.
On a alors l'équivalence $i \in I \Leftrightarrow x_i^{p-1} = 1$. Sinon, $x_i^{p-1} = 0$.

Par conséquent, $0 = Q(x) \equiv \text{Card}(I) \mod p$. Comme de plus $1 \leq \text{Card}(I) \leq 2p-1$, $\text{Card}(I) = p$.
Et $P(x) = 0$ fournit $\sum_{i \in I} a_i \equiv 0 \mod p$, d'où le résultat. ■

Remarque : Le lecteur avisé aura reconnu la démonstration d'un cas particulier du théorème de Chevalley-Warning, et l'utilisation répétée du petit théorème de Fermat.

Remarque : Il ne lui échappera pas non plus la similitude de ce théorème avec le résultat suivant, dû à Vazsonyi et Sved ([AZ] page 162) :

Théorème 2 *Soient n entiers $a_1, \ldots, a_n$. Il existe alors un ensemble de nombres consécutifs $a_{k+1}, a_{k+2}, \ldots, a_l$ dont la somme est divisible par n.*

La preuve de ce dernier réulstat est plus aisée, et utilise le principe des tiroirs.

Preuve :
Considérons l'ensemble $S = \{0, a_1, a_1 + a_2, \ldots, a_1 + \cdots + a_n\}$, ainsi que la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
Puisque $\text{Card}(S) = n + 1 > \text{Card}(\mathbb{Z}/n\mathbb{Z})$, il existe deux éléments s_1 et s_2 de S ayant la même image par π.
Notant $s_1 = a_1 + \cdots + a_k$ et $s_2 = a_1 + \cdots + a_l$ avec par exemple $k < l$, on obtient bien

$$\sum_{i=k+1}^{l} a_i = s_1 - s_2 \equiv 0 \mod n,$$

ce qui établit le résultat. ■

Références

[AZ] Aigner, Ziegler Raisonnements divins, Springer.