Théorèmes de Chevalley-Warning et Erdös-Ginzburg-Ziv

Références : Zavidovique, *Un max de maths*, p 32
Serre, *Cours d'arithmétique*, p 12
Bourgade, *Olympiades internationales de mathématiques - 1976-2005*, p 87

Théorème.

Soient k un corps fini à $q = p^n$ éléments et m un entier naturel non nul. On considère A un ensemble fini et $(f_a)_{a\in A}$ une famille de polynômes de $k[X_1, \dots, X_m]$ telle que

$$\sum_{a\in A} \deg f_a < m.$$

Soit V l'ensemble des racines communes aux polynômes f_a, alors $\#V \equiv 0 \mod (p)$.

Pour commencer, on a besoin de démontrer le lemme suivant sur les sommes de puissances dans les corps finis.

Lemme.

Soit u un entier naturel. Alors :

$$\sum_{x\in k} x^u = \begin{cases} -1 & \text{si } u \geqslant 1 \text{ et } q-1 \text{ divise } u \\ 0 & \text{sinon} \end{cases}.$$

Démonstration. Notons $S(X^u)$ la somme mise en jeu. Si u est nul, le résultat est immédiat tandis que si u est divisible par $q-1$, alors

$$S(X^u) = 0^u + \sum_{x\in k^*} 1 = q - 1 = -1.$$

Enfin, si $u \geqslant 1$ et n'est pas divisible par $q-1$, sachant que k^* est cyclique, il existe $y \in k^*$ tel que y^u soit différent de 1. On a alors :

$$S(X^u) = \sum_{x\in k^*} x^u = \sum_{x\in k^*} (yx)^u = y^u S(X^u).$$

Comme y^u est distinct de 1, il s'ensuit que $S(X^u) = 0$. □

Démonstration. Considérons le polynôme

$$P(X_1, \dots, X_m) = \prod_{a\in A} (1 - f_a^{q-1}(X_1, \dots, X_m)).$$

Remarquons dans un premier temps que P est la fonction caractéristique de V :

- Si $x \in k^m$ vérifient $f_a(x) = 0$ pour tout $a \in A$, alors $P(x) = 1$.
- Si $x \in k^m$ n'est pas un élément de V, il existe $a \in A$ tel que $f_a(x)$ ne vaille pas 0, alors par théorème de Lagrange, $f_a(x)^{q-1} = 1$ et donc $P(x) = 0$.

On en déduit alors que $P \equiv \mathbb{1}_V$, donc

$$S(P) := \sum_{x\in k^m} P(x) \equiv \#V \mod (p).$$

Par hypothèse sur les degrés des polynômes f_a, il vient que $\deg P < m(q-1)$. On peut donc écrire

$$P = \sum_{|u|<m(q-1)} \alpha_u X^u,$$

où les α_u sont des éléments de k. A partir de là :

$$S(P) = \sum_{x\in\mathbb{F}_q^m} \sum_{|u|<m(q-1)} \alpha_u x^u = \sum_{|u|<m(q-1)} \alpha_u S(X^u),$$

avec

$$\forall u \in \mathbb{F}_q^m : S(X^u) = \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} x_1^{u_1}\ldots x_m^{u_m} = \left(\sum_{x_1\in\mathbb{F}_q} x_1^{u_1}\right)\ldots\left(\sum_{x_m\in\mathbb{F}_q} x_m^{u_m}\right) = \prod_{i=1}^{m} S(X^{u_i}).$$

Or, si $|u| < m(q-1)$, il existe $i \in [\![1, m]\!]$ tel que $u_i < q-1$ donc d'après le lemme précédent, $S(X^{u_i}) = 0$ ce qui entraîne que $S(P) = 0$ et le résultat s'ensuit. □

A présent, on utilise le théorème de Chevalley-Warning pour démontrer le théorème d'arithmétique d'Erdös-Gizburg-Ziv.

Théorème (Théorème d'Erdös-Gizburg-Ziv)**.**

Soit n un entier naturel non nul. Alors parmi $2n-1$ entiers $a_1, \ldots, a_{2n-1}$, on peut en trouver n dont la somme est divisible par n.

Démonstration. Notons EGZ l'ensemble des entiers naturels vérifiant la propriété énoncée dans le théorème précédent. L'objectif est de montrer que EGZ = $\mathbb{N}$.

Soit p un nombre premier. Montrons que p est élément de EGZ. Soient pour cela $a_1, \ldots, a_{2p-1}$ des entiers. Considérons les deux polynômes de $\mathbb{F}_p[X]$ suivants :

$$P_1(X_1, \ldots, X_{2p-1}) = \sum_{k=1}^{2p-1} X_k^{p-1},$$

$$P_2(X_1, \ldots, X_{2p-1}) = \sum_{k=1}^{2p-1} a_i X_k^{p-1}.$$

Ces deux polynômes vérifient $\deg P_1 + \deg P_2 = 2p-2 < 2p-1$ ont $(0, \ldots, 0)$ pour racine commune donc d'après le théorème de Chevalley-Warning, ils possèdent une racine commune non nulle $(x_1, \ldots, x_{2p-1})$. D'après le théorème de Lagrange, pour tout x de $\mathbb{F}_p$, $x^{p-1} = 1$ si est seulement si x est non nul donc en notant W l'ensemble des indices i pour lesquels x_i est non nul, il vient

$$P_1(x_1, \ldots, x_{2p-1}) = \sum_{i\in W} x_i^{p-1} = |W| = 0.$$

Ainsi, $|W|$ est un entier divisible par p vérifiant $1 \leqslant |W| \leqslant 2p-1$ donc $|W| = p$ et on note $W = \{i_1, \ldots, i_p\}$. Vient ensuite

$$P_2(x_1, \ldots, x_{2p-1}) = \sum_{j=1}^{p} a_{i_j} = 0$$

donc p divise $a_{i_1} + \ldots + a_{i_p}$ et le résultat est démontré.

Montrons à présent que EGZ est stable par multiplication. D'après le théorème fondamental de l'arithmétique, la démonstration sera achevée. Soient donc m et n deux éléments de EGZ. Considérons $a_1, \ldots, a_{2mn-1}$ entiers. Étant donné que $n \in$ EGZ, il existe $I_1 \subset \{1, \ldots, 2mn-1\}$ de cardinal n tel que

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

De même, il existe $I_2 \subset \{1, \ldots, 2mn-1\}\backslash I_1$ de cardinal n tel que

$$\sum_{i\in I_2} a_i \equiv 0 \mod (n).$$

On termine ce procédé après avoir construit l'ensemble d'indices I_{2m-1} car au bout de $2m-2$ étapes, il reste $2nm - 1 - (2m-2)n = 2n-1$ entiers. Pour tout $j \in \{1, \ldots, 2m-1\}$, on considère l'entier c_j défini par

$$\sum_{i\in I_j} a_i = c_j n.$$

Alors comme m est un élément de EGZ, on peut considérer $J \subset \{1, \dots 2m-1\}$ de cardinal m tel que

$$\sum_{j \in J} c_j \equiv 0 \mod (m).$$

À partir de là :

$$\sum_{j \in J} \sum_{i \in I_j} a_i = n \left(\sum_{j \in J} c_j \right) \equiv 0 \mod (mn)$$

ce qui termine la démonstration. □

Remarques : • Il faut savoir que la quantité $2n-1$ dans le théorème d'Erdös-Gizburg-Ziv est incompressible comme le montre l'exemple constitué de $n-1$ "0" et $n-1$ "1".
• Il existe une autre méthode plus combinatoire pour démontrer que les nombres premiers sont éléments de EGZ. Étant donnés p un nombre premier et $a_1, \dots a_{2p-1}$ des entiers, on considère pour tout $J \subset \{1, \dots, 2p-1\}$ la somme $S_J = \sum_{i \in J} x_i$. L'idée est alors de calculer de deux manières différentes la quantité

$$\Sigma = \sum_{J \subset \{1,\dots,2p-1\} \,:\, \#J = p} S_J^{p-1}.$$

Tout d'abord, S_J^{p-1} est la somme de divers monômes de degré $p-1$ faisant intervenir k facteurs ($1 \leqslant k \leqslant p-1$) que l'on peut écrire sous la forme $\lambda x_1^{a_{i_1}} \dots x_{i_k}^{a_{i_k}}$. Ce type de monôme se retrouve, avec le même coefficient, dans le développement de S_J pour $\binom{2p-1-k}{p-k}$ ensembles J distincts : il suffi d'avoir pour J un ensemble contenant $i_1, \dots, i_k$ puis de choisir les $p-k$ indices restants dans les $2p-1-k$ indices disponibles. Ainsi, après le développement complet de Σ, tout monôme est un multiple de $\binom{2p-1-k}{p-k}$ donc est divisible par p. L'entier Σ est donc nul dans $\mathbb{F}_p$.
D'autre part, si aucun des S_j n'était divisible par p, on aurait pour tout J, $S_j^{p-1} \equiv 1 \mod (p)$ et σ est non nul modulo p. Ceci continue une contradiction avec le paragraphe précédent donc il existe J de cardinal p tel que $S_J \equiv 0 \mod (p)$.

Adapté du travail de Paul Alphonse, Justine Velly et Joséphine Boulanger