Chevalley-Warning et Erdös-Ginsburg-Ziv

Leçons : 120, *121*, 123, 142, 144

Théorème 1

Soit $q = p^s$ où p est premier et $(f_a)_{a\in A}$ une famille finie de polynômes de $\mathbb{F}_q[X_1,\dots,X_m]$ tels que $\sum\limits_{a\in A} \deg f_a < m$. Alors si $V = \{x = (x_1,\dots,x_m) \in K^m : \forall a \in A, f_a(x_1,\dots,x_m) = 0\}$, on a $\mathrm{Card}(V) \equiv 0[p]$.

Démonstration. On note $K = \mathbb{F}_q$.

Étape 1 : Soit $u \in \mathbb{N}$ et $S(u) = \sum\limits_{x\in K} x^u$. Montrons que $S(u) = 0$ si $u = 0$ ou $q-1 \nmid u$ et -1 sinon.

D'abord, si $u = 0$, avec la convention $0^0 = 1$, on a $S(0) = 1 + \sum\limits_{x\in K^\times} 1 = q = 0$ dans $\mathbb{F}_q$. Si $u \neq 0$, rappelons que $K^\times$ est cyclique. Prenons en un générateur z, qui est donc d'ordre q de sorte que $z^u = 1 \Leftrightarrow q-1|u$.

Ainsi, si $q-1 \not| u$, $S(u) = \sum\limits_{j=0}^{q-1} z^{ju} = \dfrac{z^{qu}-1}{z^u-1} = 0$ car $z^q = z$.

Et sinon, $S(u) = \sum\limits_{j=1}^{q-1} 1 = q-1 = -1$ dans $\mathbb{F}_q$.

Étape 2 : soit $P = \prod\limits_{a\in A}\left(1 - f_a^{q-1}\right)$. Si $x \in V, P(x) = 1$ et si $x \notin V$, il existe $a \in A$ tel que $f_a(x) \neq 0$ donc $f_a(x)^{q-1} = 1$, si bien que $P(x) = 0$. Donc la fonction $x \mapsto P(x)$ est l'indicatrice $\mathbb{1}_V$.

Par ailleurs, le degré de V est inférieur à $\sum\limits_{a\in A}(\deg f_a)(q-1) < m(q-1)$ par hypothèse. Donc P est une combinaison linéaire de monômes $X^u = X_1^{u_1}\dots X_m^{u_m}$ où $u_1+\dots+u_m < m(q-1)$. Pour un tel monôme :

$$\sum_{x\in K^m} x^u = \sum_{x\in K^m} x_1^{u_1}\dots x_m^{u_m} = \prod_{j=1}^{m}\sum_{x_i\in K} x_i^{u_i} = \prod_{j=1}^{m} S(u_i)$$

Or, il existe i_0 tel que $u_{i_0} < q-1$ donc $\sum_{x\in K^m} x^u = 0$

Par linéarité, $\forall x \in \mathbb{F}_q, 0 = \sum\limits_{x\in K^m} P(x) = \sum\limits_{x\in K^m} \mathbb{1}_V(x) = \mathrm{Card} V$. Comme $\mathbb{F}_q$ est de caractéristique p, le résultat désiré s'ensuit. □

Proposition 2 (*Erdös-Ginsburg-Ziv*)

Soit $n \in \mathbb{N}^*$. Parmi $2n-1$ entiers $a_1,\dots,a_{2n-1}$, on peut en trouver n dont la somme est divisible par n.

Démonstration. Étape 1 : pour $n = p$ premier. Introduisons les polynômes de $\mathbb{F}_p[X_1,\dots,X_{2p-1}]$, $P_1(X_1,\dots,X_{2p-1}) = \sum\limits_{k=1}^{2p-1} X_k^{2p-1}$ et $P_2(X_1,\dots,X_{2p-1}) = \sum\limits_{k=1}^{2p-1} \overline{a_k} X_k^{2p-1}$. On a $\deg P_1 + \deg P_2 = 2(p-1) < 2p-1$

De plus, $P_1(0) = 0 = P_2(0)$ donc en reprenant les notations du théorème précédent, V est non vide donc par Chevalley-Warning, V est de cardinal au moins p. Il existe donc $x \neq 0$ tel que $P_1(x) = P_2(x) = 0$. Or, si $x = (x_1,\dots,x_{2p-1})$, $P_1(x) = \mathrm{Card}\left\{i \in [\![1, 2p-1]\!], x_i \neq 0\right\}$ donc il y a exactement p composantes de x non nulles.

Donc comme $P_2(x) = \sum_{k\in[\![1,2p-1]\!], x_k\neq 0} \overline{a_k} = 0$, il existe $a_{i_1}, \ldots, a_{i_p}$ tels que $\sum_{k=1}^{p} \overline{a_{i_k}}$ soit divisible par p.

Étape 2 : pour le cas général, on procède par récurrence forte sur n.

Si n est premier, il n'y a rien à démontrer ; sinon, on écrit $n = pn'$ avec p premier et $n' > 1$. Soit $E = \{a_1, \ldots, a_{2n-1}\}$ un ensemble de $2n-1$ entiers.

On a $2n-1 = 2pn'-1 = (2n'-1)p+p-1$. Selon l'étape 1, on peut trouver un ensemble E_1 de p entiers pris parmi $a_1, \ldots, a_{2p-1}$ dont la somme est divisible par p ; puis E_2 ensemble de p entiers pris dans $\left\{a_1, \ldots, a_{3p-1}\right\} \setminus E_1$ de somme divisible par p, etc...

On construit ainsi des ensembles deux à deux disjoints $E_1, \ldots, E_{2n'-1}$. On note $S_i = \sum_{x\in E_i} x$, et on peut donc écrire $S_i = pS'_i$.

Par hypothèse de récurrence, il existe $\{i_1, \ldots, i_{n'}\} \subset [\![1, 2n'-1]\!]$ tel que $\sum_{k=1}^{n'} S'_{i_k}$ est divisible par n' de sorte que $\sum_{k=1}^{n'} S_{i_k}$ est divisible par n. Or, par construction, cette dernière somme est une somme de $n' \times p = n$ éléments de E ce qui termine la démonstration. $\square$

Références :

- Jean-Pierre SERRE (1994). *Cours d'arithmétique*. Presses universitaires de France
- Maxime ZAVIDOVIQUE (2013). *Un max de maths*. Calvage et Mounet