Théorème de Chevalley-Warning et EGZ (120, 123, 144, 190)

Zavidovique p. 32-36

Lem 1 : Soit $u \in \mathbb{N}$ et $\mathbb{K} = \mathbb{F}_q$

$$S(X^u) = \sum_{x \in \mathbb{K}} x^u = \begin{cases} 0 & \text{si } u = 0 \\ -1 & \text{si } u \text{ est divisible par } q-1 \text{ et } u \neq 0 \\ 0 & \text{si } u \text{ n'est pas divisible par } q-1 \end{cases}$$

démo : * Si $u = 0$ alors $S(X^u) = q = 0$

* Si u est divisible par $q-1$, alors $0^u = 0$ et si $x \neq 0$ alors $x^u = 1$. $u = (q-1)m$ + petit thm de Fermat

Ainsi $S(X^u) = q - 1 = -1$

* Si u n'est pas divisible par $q-1$, comme $\mathbb{K}^*$ est cyclique de cardinal $q-1$, il existe $y \in \mathbb{K}^*$ tel que $y^u \neq 1$. On a alors les égalités suivantes :

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

Ainsi $(1 - y^u) S(X^u) = 0$ or $y^u \neq 1$. D'où $S(X^u) = 0$.

Thm 2 : (Chevalley-Warning) Soit $(f_a)_{a \in A}$ une famille de polynôme de $\mathbb{K}[X_1, \dots, X_m]$ où $\mathbb{K} = \mathbb{F}_q$. On suppose que $\sum_{a \in A} \deg(f_a) < m$ et on pose $V \subset \mathbb{K}^m$ l'ensemble des zéros communs aux f_a.

Alors on a $\mathrm{Card}(V) \equiv 0 \ [\mathrm{mod}\ p]$.

démo : On pose $P = \prod_{a \in A} (1 - f_a^{q-1})$. Soit $x \in \mathbb{K}^m$

- Si $x \in V$ alors $P(x) = 1$.
- Si $x \notin V$ alors il existe $a \in A$ tel que $f_a(x) \neq 0$ donc $f_a^{q-1}(x) = 1$ (car $\mathbb{K}^*$ cyclique d'ordre $q-1$) et donc $P(x) = 0$.

Ainsi $P = \mathbb{1}_V$.

Pour $f \in \mathbb{K}[X_1, \dots, X_m]$, on définit $S(f) = \sum_{x \in \mathbb{K}^m} f(x)$. Alors on a $S(P) = \sum_{x \in \mathbb{K}^m} P(x) = \sum_{x \in V} 1 = \mathrm{card}(V) \ [\mathrm{mod}\ p]$.

Comme $\sum_{a \in A} \deg f_a < m$, on a $\deg(P) < m(q-1)$. On écrit P comme combinaison linéaire de monômes $X^U = X^{u_1} \dots X^{u_m}$ avec $\sum u_i < m(q-1)$. Ainsi il suffit de montrer que $S(X^u) = 0$.

Par le principe des tiroirs, il existe un indice i tel que $u_i < q-1$. Donc par le lemme 1, on a bien

$S(X^u) = 0$.

thm 3 : (EGZ) Soit $n \in \mathbb{N}^*$, $a_1, \dots, a_{2n-1}$ des entiers. On peut toujours en choisir n dont la somme est divisible par n.

démo : * Pour $n = p$ premier. On se place dans $\mathbb{F}_q = \mathbb{K}$.

Soit $a_1, \dots, a_{2p-1}$ les $2p-1$ entiers. On considère :

$$P_1(x_1, \dots, x_{2p-1}) = \sum_{k=1}^{2p-1} x_i^{p-1} \quad \text{et} \quad P_2(x_1, \dots, x_{2p-1}) = \sum_{k=1}^{2p-1} \overline{a_i} \; x_i^{p-1}$$

On a $(0, \dots, 0)$ qui est racine communes de P_1 et P_2, par le thm de Chevalley-Warning, ils possèdent au moins p racines communes. Soit $(x_1, \dots, x_{2p-1})$ une racine commune non triviale.

- $P_1(x_1, \dots, x_{2p-1}) = 0$, on déduit qu'exactement p entiers sont non nuls.
- $P_2(x_1, \dots, x_{2p-1}) = 0$, on déduit que $\sum_{i=0}^{p} \overline{a_{n_i}} \equiv 0 \, [\text{mod } p]$.

D'où le résultat.

* Pour n quelconque. Par récurrence forte sur n.

- init $n = 1$: ok.
- héré : Supposons $HR(k)$ vraie pour tout $2 \leq k < n$ et montrons le au rang n. Si n est premier alors on retourne au cas 1, sinon $n = pn'$ avec $p \in \mathcal{P}$ et $n' \in \mathbb{N}$. On remarque $2n - 1 = (2n' - 1)p + p - 1$

On applique $HR(p)$ aux $a_1, \dots, a_{2p-1}$ entiers, donc on peut trouver E_1 tel que $|E_1| = p$ et leur somme est divisible par p.

On peut appliquer ce processus aux $2n-1-p$ entiers qui restent. On itère ce processus tant qu'il reste plus de $2p-1$ entiers, c'est-à-dire exactement $2n'-1$ fois.

Soit S_i, $\forall i \in [\![1, 2n'-1]\!]$, la somme des éléments de E_i, ainsi construit. On peut alors écrire $S_i = p \cdot S_i'$

On applique HR à S_i'. On trouve $k_1, \dots, k_{n'}$ tels que

$$n' \text{ divise } \sum_{i=1}^{n'} S'_{k_i}$$

On considère $\bigcup_{i=1}^{n'} E_{n_i}$ qui est de cardinal $p \cdot n' = n$. On note $a_{i_1}, \dots, a_{i_n}$ ses éléments et on a

$$\sum_{k=1}^{n} a_{i_k} = \sum_{j=1}^{n'} S_{n_j} = p \sum_{j=1}^{n'} S'_{n_j} \quad . \text{ D'où } pn' = n \text{ divise } \sum_{k=1}^{n} a_{i_k}$$

Questions : Théorème de Chevalley-Warning et EGZ.

- $\mathbb{K}^*$ est cyclique ?

Comme $\mathbb{K}$ est un corps commutatif, $\forall d \in \mathbb{N}$, le polynôme $X^d - 1$ admet au plus d racines.

Si $d | q-1$, on en déduit qu'il y a au plus un sous-groupe de $\mathbb{K}^*$ d'ordre d (celui dont tous les éléments vérifient la relation $x^d = 1$.

Notons A_d le nb d'éléments d'ordre d.

Si A_d est non nul, il existe alors un élément d'ordre d qui engendre l'unique sous groupe de $\mathbb{K}^*$ d'ordre d, on a alors $A_d = \varphi(d)$.

$\sum_{d|q-1} A_d = q-1$, comme tout élément engendre un sous-groupe.

Or $q-1 = \sum_{d|q-1} A_d \leq \sum_{d|q-1} \varphi(d) = q-1$. Donc $A(d) = \varphi(d)$ $\forall d | q-1$.

En particulier pour $d = q-1$, on a $A(d) = \varphi(d)$ donc il existe une élément de $\mathbb{K}^*$ d'ordre $q-1$.

- $S(x^u) = y^u S(x^u)$?

L'application $\varphi : \mathbb{K}^* \longrightarrow \mathbb{K}^*$, $x \longmapsto xy$ est une bijection car $\varphi^{-1} : \mathbb{K}^* \longrightarrow \mathbb{K}^*$, $x \longmapsto xy^{-1}$ est sa réciproque

- il suffit de mq $S(x^u) = 0$?

Comme $S(x^u) = \sum_{x \in \mathbb{K}^m} x_i^{u_i} = \sum_{x_i \in \mathbb{K}} x_i^{u_i} \sum_{\mathbb{K}^{m-1}} x_1^{u_1} \dots \widehat{x_i^{u_i}} \dots x_m^{u_m} = S(X_i^{u_i}) S(X_1^{u_1} \dots \widehat{X_i^{u_i}} \dots X_m^{u_m})$

$u_i < q-1 \Rightarrow S(X_i^{u_i}) = 0$.

- $P_1(x) = 0$ alors on a exactement p entiers non nuls ?

$\sum_{k=1}^{2p-1} x_k^{p-1} = 0$ or $x_k^{p-1} = 1$ pour $x_k \neq 0$.

donc $\exists i_1, \dots, i_p$ tel que $\sum_{k=1}^{p} x_{i_k}^{p-1} = 0$. ou $\underline{x = 0}$
impossible car x racine non triviale.

- HR appliquée aux S_i' :

On a $S_1', \dots, S_{2n'-1}'$ qui sont des entiers. Comme $n' < n$, on a l'existence $k_1, \dots, k_{n'} \in [\![1, 2n'-1]\!]$

tels que n' divise $\sum_{j=1}^{n'} S_{k_j}'$.

- EGZ est optimal car :

Si on prend la suite formée de $n-1$ fois le terme 0 et de $n-1$ fois le terme 1.
On a alors $2n-2$ entiers dont on ne peut pas extraire de n-uplet tel que leur somme soit divisible par n.