Théorèmes de Chevalley-Warning et d'Erdös-Ginzburg-Ziv

Référence : Serre : Cours d'arithmétique, p. 12-13 ou Zavidovique : Un Max de Math, p. 32

Soit $\mathbb{K}$ un corps fini de cardinal $q = p^k$ avec p premier. Donc $\text{car}(\mathbb{K}) = p$.

Théorème (Théorème de Chevalley-Warning - 1936)

Soient $P_1, P_2, ..., P_r \in \mathbb{K}[X_1, .., X_n]$ et $V = \{x \in \mathbb{K}^n \ / \ \forall i,\ P_i(x) = 0\}$

Si $\sum_{i=1}^{r} \deg P_i < n$ alors $\text{Card}(V) \equiv 0\,[p]$

Lemme

Soit m un entier positif ou nul. Alors la somme $S(X^m) := \sum_{x\in\mathbb{K}} x^m = 0$ si $m \geqslant 1$ et non divisible par $q-1$

Convention : $x^m = 1$ si $m = 0$ pour tout x même $x = 0$.

Preuve du Lemme :

Comme $\text{Card}(\mathbb{K}) = q = p^k$; $\mathbb{K}^*$ est cyclique d'ordre $q-1$.
Donc il existe un élément $y \in \mathbb{K}^*$ d'ordre $q-1$ donc tel que $y^m \neq 1$.
Alors $S(X^m) = \sum_{x\in\mathbb{K}^*} x^m = \sum_{x\in\mathbb{K}^*} y^m x^m = y^m S(X^m)$.
Soit $(1-y^m)S(X^m) = 0$ donc $S(X^m) = 0$. ■

Preuve du Théorème :

• Soit

$$P = \prod_{i=1}^{r}(1 - P_i^{q-1})$$

Soit $x \in \mathbb{K}$, avec $x \in V$, alors $\forall i\ P_i(x) = 0$ donc $P(x) = 1$.
Si $x \notin V$, alors $\exists i \ / \ P_i(x) \neq 0$
Donc par le théorème de Lagrange : $P_i(x)^{q-1} = 1$ ie $P(x) = 0$.
Ainsi P est l'indicatrice de V.

• De plus pour $Q \in \mathbb{K}[X_1, .., X_n]$, on pose :

$$\tilde{S} = \sum_{(x_1,..,x_n)\in\mathbb{K}^n} Q(x_1, .., x_n)$$

Alors $\text{Card}(V) \equiv \tilde{S}(P)\,[p]$ ($\tilde{S}(P) = \sum_{x\in V} 1 + \sum_{x\notin V} 0$ et on utilise la caractéristique p).

Il ne reste donc plus qu'à montrer que $\tilde{S}(P) = 0$.

• Or comme $\sum_{i=1}^{r} \deg P_i < n$ alors $\deg P < n(q-1)$.
Ainsi P est combinaison linéaire de monôme $X^\alpha = X_1^{\alpha_1}...X_n^{\alpha_n}$ avec
$\sum_{i=1}^{n} \alpha_i < n(q-1)$. Il suffit alors de prouver que pour un tel monôme $\tilde{\mathrm{S}}(X^\alpha) = 0$.
Or $\tilde{S}(X^\alpha) = \prod_{i=1}^{n} S(X_i^{\alpha_i})$. Et comme $\sum_{i=1}^{n} \alpha_i < n(q-1)$ on a au moins un des $\alpha_i < q-1$. Donc d'après le lemme $S(X_i^{\alpha_i}) = 0$ donc $\tilde{\mathrm{S}}(X^\alpha) = 0$.
D'où le résultat : $\tilde{S}(P) = 0$ et donc $\mathrm{Card}(V) \equiv 0\,[p]$

Détails : $\tilde{S}(X_1^{\alpha_1}..X_n^{\alpha_n}) = S(X^{\alpha_1})...S(X^{\alpha_n})$

$$\begin{aligned}\tilde{\mathrm{S}}(X_1^{\alpha_1}..X_n^{\alpha_n}) \sum_{(x_1,..,x_n)\in\mathbb{K}^n} x_1^{\alpha_1}..x_n^{\alpha_n} &= \sum_{x_1\in\mathbb{K}} x_1^{\alpha_1} \sum_{(x_2,..,x_n)\in\mathbb{K}^{n-1}} x_2^{\alpha_2}..x_n^{\alpha_n} \\ &= .. \\ &= S(X^{\alpha_1})...S(X^{\alpha_n})\end{aligned}$$

■

Corollaire (Théorème d'EGZ - 1961)

Parmi $2n-1$ entiers $a_1, \ldots, a_{2n-1}$, on peut en trouver n dont la somme est divisible par n.

Preuve du Corollaire :

Etape 1 : On montre le résultat si $n = p$ premier.

Soit $a_1, \ldots, a_{2p-1}$ des entiers. On se place dans $\mathbb{F}_p$. Cela revient à prendre $k = 1$ dans le théorème précédent. On note $\bar{a}$ la classe d'un entier dans $\mathbb{F}_p$.
On considère les deux polynômes suivant de $\mathbb{K}[X_1, \ldots, X_{2p-1}]$:

$$P_1(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1} \text{ et } P_2(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} \bar{a}_i X_i^{p-1}$$

On a $\deg P_1 + \deg P_2 \leqslant p-1+p-1 = 2p-2 < 2p-1$ on peut donc appliquer le théorème précédent et comme $\mathrm{Card}V \geqslant 1$ (ces deux polynômes ont une racine commune triviale : $(0, \ldots, 0)$) on a que $\mathrm{Card}V \neq 0$ donc est un multiple de p ie $\geqslant 2$. Ainsi, ces polynômes ont une autre racine commune non triviale : notons la $x := (x_1, \ldots, x_{2p-1})$.
On a $y^{p-1} = 1$ dans $\mathbb{F}_p$ ssi il est non nul dans $\mathbb{F}_p$. Soit W l'ensemble des x_i qui sont non nuls.
x annule P_1 donc $\sum_{i=1}^{2p-1} x_i^{p-1} = 0 = \overline{\mathrm{Card}W}$.
$\mathrm{Card}W \neq 0$ car $x \neq 0$. Donc $p|\mathrm{Card}W$ et comme $\mathrm{Card}W \leqslant 2p-1$ on a $\mathrm{Card}W = p$. Il y a donc précisément p x_i non nuls : $x_{n_1}, \ldots, x_{n_p}$.
Mais on a également x annule P_2 donc $\sum_{i=1}^{2p-1} \bar{a}_i x_i^{p-1} = 0 = \sum_{i=1}^{p} \overline{a_{n_i}}$.
Finalement, on a bien trouvé p éléments parmi $a_1, \ldots, a_{2p-1}$ tels que leur somme soit divisible par p.

Etape 2 : On montre le résultat par récurrence forte pour n quelconque.

Pour $n = 1$, il est clair que parmi un entier, l'un d'eux est divisible par 1.
Supposons donc le résultat montré jusqu'au rang $n-1$. Si n est premier, on l'a montré. Si n non premier, on écrit $n = pn'$ avec p premier et n' entier. Idée : faire des paquets de p entiers dont la somme va être divisible par p, on peut faire $2n'-1$ tels paquets car $2n-1 = p(2n'-1)+p-1$.

On applique l'hypothèse de récurrence aux entiers $a_1, \dots, a_{2p-1}$ et on trouve un ensemble E_1 de p entiers dont la somme est divisible par p.
Ensuite, on peut appliquer le même processus aux $2n-1-p = 2p(n'-1)-1$ entiers qui restent pour construire un ensemble E_2, disjoints de E_1 constitué lui aussi de p entiers dont la somme est divisible par p.
On itère ce procédé tant qu'il reste plus de $2p-1$ entiers c'est à dire $2n'-1$ fois (car $2n-1 = (2n'-1)p+p-1$).
On note S_i la somme des éléments de l'ensemble E_i, pour $i \in [\![1, 2n'-1]\!]$. Comme on a fait exprès qu'à chaque fois la somme soit divisible par p, on peut écrire $S_i = pS'_i$.
Maintenant, on applique à nouveau l'hypothèse de récurrence aux S'_i (il y en a $2n'-1$ et $n' \leqslant n-1$). On trouve n' indices $k_1, \dots, k_{n'}$ tels que $n' \Big| \sum_{i=1}^{n'} S'_{k_i}$.
Si l'on considère la réunion des éléments des E_{k_i}, on a p éléments dans chaque E_{k_i} donc $pn' = n$ élements au total. Notons les $a_{l_1}, \dots, a_{l_n}$. Ils vérifient :

$$\sum_{i=1}^{n} a_{l_i} = \underbrace{\sum_{j=1}^{n'} S_{k_j}}_{\text{la somme a été séparée sur chaque } E_{n_j}} = p \sum_{j=1}^{n'} S'_{k_j}$$

Finalement $n = pn' \Big| \sum_{i=1}^{n} a_{l_i}$

■

Notes :

✓ **A l'oral**, **en speedant** : CW (avec le cas du lemme qui nous intéresse dedans la démo) : 8'11 + EGZ p premier = 14'06, une seconde fois 12'. EGZ tout tout seul 12' + avec un peu de CW = 14'36.
✓ On peut montrer les autres cas du **Lemme :**

Lemme

Soit m un entier positif ou nul. Alors la somme $S(X^m) = \sum_{x \in \mathbb{K}} x^m$ est égale à -1 si $m \geqslant 1$ et divisible par $q-1$ et 0 si $m = 0$

Preuve du Lemme :

Si $m = 0$ **:**
Alors tous les termes de la somme sont égaux à 1. Donc $S(X^m) = q * 1 = 0$ car on est en caractéristique p.

Si $m \geqslant 1$ **et** $q-1 \mid m$ **:**
Alors $0^m = 0$ et $\underline{x^m = 1}$ si $x \neq 0$. Donc $S(X^m) = (q-1) * 1 = -1$.

■

✓ Le degré d'un polynôme non nul est celui de son monôme de plus haut degré.
✓ Le résultat d'EGZ est optimal : parmi $2n-2$ entiers, il peut ne pas en exister n dont la somme est divisible par n. En effet, on peut prendre par exemple la suite formée de $n-1$ fois 0 et de $n-1$ fois 1 : on ne peut pas extraire de n-uplets dont la somme soit divisible par n.
✓ Vers 1935, Emil Artin proposa ce problème à son étudiant Ewald Warning. Il l'exposa également à Chevalley qui lui rendait visite. Les 2 prouvèrent se théorème indépendamment en 1936.

♣ Claude Chevalley (1909-1984) est un mathématicien français spécialiste de l'algèbre et un des fondateurs du groupe Bourbaki.
♣ Paul Erdös(1913 - 1996) est un mathématicien hongrois d'origine juive, célèbre pour son excentricité, le nombre de ses publications scientifiques (environ 1 500) et de ses collaborateurs. Son oeuvre prolifique a donné naissance au concept de nombre d'Erdös représentant le degré de séparation entre le mathématicien hongrois, la centaine de collaborateurs directs, coauteurs d'articles, de nombre 1, indirects, de nombre 2, etc.
♣ Abraham Ziv (1940 - 2013) est un mathématicien israëlien surtout connu pour ce théorème.
♣ Abraham Ginzburg : il a écrit des livres...