Développement: Théorème d'Erdös-Ginzburg-Ziv

Adrien Fontaine

1er juillet 2014

Ce développement consiste en la preuve du théorème d'Erdös-Ginzbur-Ziv. On commence par rappeler le théorème de Chevalley-Warning, qui est un outil essentiel de la démonstration. On peut en trouver une preuve au début du *Cours d'arithmétique* de Jean-Pierre Serre.

Théorème 1 (*Chevalley-Warning*)

Soit q une puissance d'un nombre premier p ($q = p^d$). Soient $f_1, ..., f_r \in \mathbb{F}_q[X_1, ..., X_n]$, vérifiant la condition

$$\sum_{i=1}^{r} deg(f_i) < n$$

Alors, en notant $V = \{x \in \mathbb{F}_q^n / f_1(x) = ... = f_q(x) = 0\}$, l'ensemble des zéros communs aux polynômes $f_1, ..., f_r$, on a :

$$|V| \equiv 0[p]$$

Venons en maintenant au théorème d'Erdös-Ginzburg-Ziv.

Théorème 2 (*Erdös-Ginzburg-Ziv*)

Soit $n \in \mathbb{N}^*$, et $a_1, ..., a_{2n-1}$ des entiers. Alors, il existe des indices $i_1, ..., i_n \in \{1, ..., 2n-1\}$ tels que

$$a_{i_1} + ...a_{i_n} \equiv 0[n]$$

Démonstration : Notons EGZ l'ensemble des entiers $n \in \mathbb{N}^*$ vérifiant le théorème d'Erdös-Ginzburg-Ziv. Plus précisément,

$$EGZ = \{n \in \mathbb{N}^*, \forall a_1, ..., a_{2n-1} \in \mathbb{N}, \text{ il exite des indices } i_1, ..., i_n \in \{1, ..., 2n-1\} / a_{i_1} + ... + a_{i_n} \equiv 0[n]\}$$

Bien évidemment, le but est de montrer que $EGZ = \mathbb{N}^*$.
Pour cela, on va procéder en deux étapes. On va d'abord montrer que EGZ contient tous les nombres premiers, puis que EGZ est stable par multiplication, ce qui permettra de conclure.

1. EGZ **contient tous les nombres premiers :**
   Soit p premier et $a_1, ..., a_{2p-1}$ des entiers. On travaille dans $\mathbb{F}_p$ et on considère les deux polynômes

   $$f_1 = \sum_{i=1}^{2p-1} \overline{a_i} X_i^{p-1} \text{ et } f_2 = \sum_{i=1}^{2p-1} X_i^{p-1}$$

   Alors, comme $deg(f_1) + deg(f_2) \leq 2p-2 < 2p-1$ (le nombre de variables), on peut appliquer le théorème de Chevalley-Warning. En conservant les notations du théorème, on a donc,

   $$p \mid |V|$$

Or, $(0, ..., 0) \in V$ donc $|V| \geq 2$.
Donc, il existe $(x_1, ...x_{2p-1}) \in V$ non nul, tel que

$$f_1(x_1, ..., x_{2p-1}) = f_2(x_1, ..., x_{2p-1}) = 0$$

Or, $x^{p-1} = 1$ dans $\mathbb{F}_p$, si et seulement si, x est non nul dans $\mathbb{F}_p$. Notons alors

$$W = \{i \in \{1, ..., 2p-1\} / x_i \neq 0\}$$

On a alors

$$f_2(x_1, ..., x_{2p-1}) = \sum_{i \in W} x_i^{p-1} = \overline{|V|} = 0$$

Or, $1 \leq |W| \leq 2p - 1$. Donc, $|W| = p$.
Donc, en notant $W = \{i_1, ..., i_p\}$, on a

$$f_1(x_1, ..., x_{2p-1}) = \sum_{k=1}^{n} \overline{a_{i_k}} x_{i_k}^{p-1} = \sum_{k=1}^{p} \overline{a_{i_k}} = 0$$

c'est à dire

$$a_{i_1} + ... + a_{i_p} \equiv 0[p]$$

2. EGZ **est stable par multiplication**
Soient $m, n \in EGZ$. On veut montrer que $nm \in EGZ$.
Soient donc $a_1, ..., a_{2nm-1}$ des entiers.
Prenons en $2n-1$. Comme $n \in EGZ$, il existe un ensemble I_1 d'indices, de cardinal n, tel que $I_1 \subset \{1, ..., 2_n - 1\}$ et

$$\sum_{i \in I_1} a_i \equiv 0[n]$$

Considérons ensuite les entiers (a_i) avec $i \in \{1, ..., 2nm-1\} \setminus I_1$. Prenons en $2n-1$. Il existe alors I_2 tel que $I_2 \subset \{1, ..., 2nm-1\} \setminus I_1$, $|I_2| = n$ et

$$\sum_{i \in I_2} a_i \equiv 0[n]$$

Terminons le procédé après avoir construit l'ensemble d'indices I_{2m-1}, ce qui est possible car au bout de $2m-2$ étapes, il reste

$$2nm - 1 - (2m-2).n = 2n - 1 \text{ entiers}$$

Pour $j \in \{1, ..., 2m-1\}$, soit c_j défini par

$$\sum_{i \in I_j} a_i = nc_j$$

Alors, comme $m \in EGZ$, on peut finalement extraire un sous-ensemble d'indices J tel que

$$\sum_{j \in J} c_j \equiv 0[m]$$

Alors,

$$\sum_{j \in J} \sum_{i \in I_j} a_i = n \underbrace{\sum_{j \in J} c_j}_{\text{divisible par } m} \equiv 0[nm]$$

Donc, ces nm derniers entiers répondent au problème posé. ■