Chevalley-Warning + EGZ

[Serre = cours d'arithmétique p 12] + [Zavidovique = 1 max de maths p 32]

(TA) Soit $K = \mathbb{F}_q$ ($q = p^s$ avec $p \in \mathbb{P}$). Soit $f_1, \dots, f_n \in K[X_1, \dots, X_m]$ tq $\sum_{i=1}^{n} \deg(f_i) < m$.
On note $Z = \{x \in \mathbb{F}_q^m \mid \forall i \in [\![1,n]\!], f_i(x) = 0\}$. Alors $\mathrm{card}(Z) \equiv 0 \bmod p$

démo lemme Soit $u \in \mathbb{N}$; on note $S(X^u) = \sum_{x \in K} x^u$. Alors $S(X^u) = \begin{cases} -1 \text{ si } u \geq 1 \text{ et } q-1 \mid u \\ 0 \text{ sinon} \end{cases}$ $(0^0 = 1)$ $(\bmod p)$

démo lemme
- Si $u = 0$, $S(X^u) = \sum_{x \in K} 1 = q \equiv 0 \bmod p$
- Si $u \geq 1$ et $q-1 \mid u$: $K^\times$ est cyclique d'ordre $q-1$ donc $\forall x \in K^\times$, $x^{q-1} = 1$ donc $x^u = 1$
  Donc $S(X^u) = \sum_{x \in K^\times} 1 = q-1 \equiv -1 \bmod p$
- Si $u \geq 1$ et $q-1 \nmid u$: $K^\times$ est cyclique d'ordre $q-1$ donc $\exists\, y \in K^\times$ tq $\mathrm{ord}(y) = q-1$
  Donc $y^u \neq 1$ (sinon $\mathrm{ord}(y) = q-1 \mid u$)
  Donc $S(X^u) = \sum_{x \in K} x^u = \sum_{x \in K} (yx)^u$ car $y \in K^\times$
  $= y^u S(X^u) \Rightarrow S(X^u)\underbrace{(1-y^u)}_{\neq 0} = 0 \Rightarrow S(X^u) = 0$

Notons $P = \prod_{i=1}^{n} (1 - f_i^{q-1}) \in K[X_1, \dots, X_m]$ et montrons que P vaut 1 ou 2 et 0 ailleurs
Si $x \in Z$, $P(z) = \prod_{i=1}^{n} (1 - \underbrace{f_i^{q-1}(x)}_{=0}) = 1$
Si $x \notin Z$, $\exists\, i \in [\![1,n]\!]$ tq $f_i(x) \neq 0$. Comme $K^\times$ est cyclique d'ordre $q-1$, on a alors $f_i(x)^{q-1} = 1$ donc un facteur nul de $P(x)$ donc $P(x) = 0$

Étendons S des monômes aux $f \in K[X_1, \dots, X_m]$ ainsi : $S(f) = \sum_{x \in K^m} f(x)$
On a alors $S(P) = \mathrm{card}(Z)$ (et ceci est vrai mod P)
On veut donc montrer $S(P) \equiv 0 \bmod p$

Or $P = \sum_u a_u X^u$. Il suffit donc de montrer $\forall X^u$ monôme de P, $S(X^u) \equiv 0\ (p)$
Soit $X^u = \prod_{i=1}^{m} X_i^{u_i}$ un monôme de P

$$S(X^u) = \sum_{x \in K^m} \prod_{i=1}^{m} x_i^{u_i} = \prod_{i=1}^{m} \left(\sum_{x_i \in K} x_i^{u_i} \right) = \prod_{i=1}^{m} S(X_i^{u_i})$$

Or, $\deg(P) \leq \sum_{i=1}^{n} (q-1) \deg(f_i) < m(q-1)$ par hp donc pour tout monôme X^u de P,

il existe $i \in [\![2,m]\!]$ tq $\alpha_i < (q-1)$ / forme $S(x_i^{\alpha_i}) \equiv 0 \bmod p$

Donc $\mathrm{card}(Z) \equiv 0 \bmod p$

(iv) Si les $(f_i)_i$ ont zéro facteurs cstes, 0 est racine commune de $\mathrm{card}(Z) \geq p$

En particulier 1 forme quad en 3 var admet 1 zéro non trivial

(IH) Erdos - Ginzburg - Ziv $\forall m \geq 2$, $\forall a_1, \dots, a_{2m-1} \in \mathbb{Z}^{2m-1}$, $\exists i_1, \dots i_m \in [\![1, 2m-1]\!]$ tq

$$\sum_{j=1}^{m} a_{i_j} \equiv 0 \bmod m$$

démo On note EGZ l'ensemble des n qui vérifient le IH

- Soit $p \in \mathbb{P}$ et $a_1, \dots, a_{2p-1} \in \mathbb{Z}^{2p-1}$. On def $P_1 = \sum_{k=1}^{2p-1} X_k^{p-1}$ et $P_2 = \sum_{k=1}^{2p-1} \overline{a_k} X_k^{p-1} \in \mathbb{F}_p[X_1, \dots, X_{2p-1}]$

On note $Z = \{x \in \mathbb{F}_p^{2p-1} \mid P_1(x) = P_2(x) = 0\}$

Comme $0 \in Z$, $|Z| \geq 1$. De plus, $\deg(P_1) + \deg(P_2) = 2p-2 < 2p-1$

donc par Chevalley-Warning, $|Z| \equiv 0 \bmod p$. Donc y a au moins p éléments de Z

En particulier, $\exists (x_1, \dots, x_{2p-1}) \in Z \setminus \{0\}$ tq $P_1(x_1, \dots, x_{2p-1}) = 0$ et $P_2(x_1, \dots, x_{2p-1}) = 0$

$= (\mathrm{card}\{i \mid x_i \neq 0\})$ car si $x \in \mathbb{F}_p$, $x^{p-1} = \begin{cases} 1 \text{ si } x \neq 0 \\ 0 \text{ sinon.} \end{cases}$

Dc $\mathrm{card}\{i \mid x_i \neq 0\} \in p\mathbb{N} \cap [\![1, 2p-1]\!] = \{p\}$ donc exactement p composantes

de $(x_1, \dots, x_{2p-1})$ sont $\neq 0$. Notons les $x_{i_1}, \dots x_{i_p}$

Alors $0 = P_2(x_1, \dots, x_{2p-1}) = \sum_{j=1}^{p} \overline{a_{i_j}} \underbrace{x_{i_j}^{p-1}}_{=1}$ donc $\sum_{j=1}^{p} a_{i_j} \equiv 0 \bmod p$. Dc $p \in EGZ$

- Soit $m, n \in EGZ$ et $a_1, \dots, a_{mn-1} \in \mathbb{Z}$

De $a_1, \dots, a_{mn-1}$ on extrait $i_{1,1}, \dots i_{m,1}$ tq $m \mid \sum_{j=1}^{m} a_{i_{j,1}} = S_1$

Des $2mn-1-m$ entiers restants on en extrait m d'indices $i_{1,2}, \dots i_{m,2}$ tq $m \mid \sum_{j=1}^{m} a_{i_{j,2}} = S_2$

On répète le procédé jusqu'à ce qu'il reste moins de $2n-1$ entiers

Comme $2mn-1 = (2n-1)m + m-1$, on le réitère $2n-1$ fois

Alors $\frac{S_1}{m}, \dots \frac{S_{2n-1}}{m}$ sont $2n-1$ entiers : comme $n \in EGZ$, $\exists k_1, \dots, k_n$ tq

$\sum_{j=1}^{n} \frac{S_{k_j}}{m} \equiv 0 \bmod n$. D'où $\sum_{j=1}^{n} \sum_{k=1}^{m} a_{i_k, k_j} \equiv 0 \bmod mn$

contient mn entiers parmi ceux du début

Dc $mn \in EGZ$

Comme EGZ contient les nb 1^{ers} et est stable par multiplication, $EGZ = \mathbb{N} \setminus \{0, 1\}$ ce qui conclut