Références : *Un max de math*, Maxime Zavidovique

Théo (Chevalley-Warning)**.** *Soit $(f_i)_{i\in[\![1,r]\!]}$ une famille de polynômes non nuls de $\mathbb{F}_q[X_1,...,X_n]$ (q une puissance d'un nombre premier p). On suppose que les degrés des $(f_i)_{i\in[\![1,r]\!]}$ vérifient l'inégalité $\sum_{i=1}^r \deg(f_i) < n$. Posons $V = \{x \in \mathbb{F}_q^n : \forall i \in [\![1,r]\!], f_i(x) = 0\} \subset \mathbb{F}_q^n$. Alors, on a $Card(V) \equiv 0[p]$.*

Démonstration. Posons

$$S = \prod_{i\in[\![1,r]\!]} (1 - f_i^{q-1}) \in \mathbb{F}_q[X_1,...,X_n].$$

Montrons que $S = \mathbb{1}_V$. Soit $x \in \mathbb{F}_q^n$.

- Si $x \in V$, alors pour tout $i \in [\![1,r]\!]$, $f_i(x) = 0$ et $S(x) = 1$.
- Sinon, il existe $i \in [\![1,r]\!]$ tel que $f_i(x) \neq 0$.
  Alors, comme $f_i(x) \in \mathbb{F}_q^*$ alors $f_i(x)^{q-1} = 1$ et donc $S(x) = 0$.

D'où $S = \mathbb{1}_V$. On a ainsi

$$\sum_{x\in\mathbb{F}_q^n} S(x) = Card(V)1_{\mathbb{F}_q} = Card(V)[p].$$

Calculons maintenant $\sum_{x\in\mathbb{F}_q^n} S(x)$.
Tout d'abord, nous avons

$$\deg(S) = (\sum_{i\in[\![1,r]\!]} \deg(f_i))(q-1) < n(q-1).$$

On a donc

$$S(X) = \sum_{|k|<n(q-1)} a_k X^k.$$

Ainsi,

$$\sum_{x\in\mathbb{F}_q^n} S(x) = \sum_{|k|<n(q-1)} a_k \sum_{x\in\mathbb{F}_q^n} x^k$$

Calculons maintenant

$$\begin{aligned}\sum_{x\in\mathbb{F}_q^n} x^k &= \sum_{x_1\in\mathbb{F}_q} ... \sum_{x_n\in\mathbb{F}_q} x_1^{k_1}...x_n^{k_n} \\ &= (\sum_{x_1\in\mathbb{F}_q} x_1^{k_1})...(\sum_{x_n\in\mathbb{F}_q} x_n^{k_n}).\end{aligned}$$

Cela revient à calculer

$$\sum_{x\in\mathbb{F}_q} x^k, k \in \mathbb{N}.$$

- Si $k = 0$ alors $\sum_{x\in\mathbb{F}_q} x^k = q = 0$.
- Si $q-1|k$, avec $k \neq 0$, alors $\sum_{x\in\mathbb{F}_q} x^k = q-1 = -1$.
- Si $q-1 \nmid k$ alors il existe $x_0 \in \mathbb{F}_q^*$ tel que $x_0^k \neq 1$. Alors

$$x_0^k \sum_{x\in\mathbb{F}_q} x^k = \sum_{x\in\mathbb{F}_q} (x_0 x)^k = \sum_{x\in\mathbb{F}_q} x^k.$$

  On a donc

$$(1 - x_0^k) \sum_{x\in\mathbb{F}_q} x^k = 0.$$

  Comme $x_0^k \neq 1$, on a $\sum_{x\in\mathbb{F}_q} x^k = 0$

Or, on sait que $x = (x_1,...,x_n)$ et $k = (k_1,...,k_n)$ avec

$$|k| = \sum_{i=1}^n k_i < n(q-1) = \sum_{i=1}^n (q-1).$$

Si $q-1|k_i$ avec $k_i \neq 0$ pour tout $i \in [\![1,n]\!]$, alors $n(q-1) \leq \sum_{i=1}^n k_i$ ce qui est impossible. On se retrouve donc dans les cas où il existe $i \in [\![1,n]\!]$ tel que

$$\sum_{x_i\in\mathbb{F}_q} x_i^{k_i} = 0.$$

Donc on a

$$\sum_{x\in\mathbb{F}_p^n} x^k = 0.$$

On a donc

$$\sum_{x\in\mathbb{F}_q^n} S(x) = Card(V) = 0[p].$$

□

Leçons possibles : 123 - 142