Équation de Fermat dans un corps fini

Notations : G un groupe commutatif fini, ϕ une fonction de G dans $\mathbb{C}$, χ un caractère de $|G|$, sa transformée de Fourier est

$$\hat{\phi}(\chi) = \sum_{x \in G} \phi(x)\chi(x)$$

Si H est un sous-groupe de G, on note $H^\perp$ les caractères dont la restriction à H est triviale. C'est un sous-groupe d'indice $|H|$.
Si χ est un caractère de $\mathbb{F}_q^\times$, ψ de $\mathbb{F}_q$, on prend la convention $\chi(0) = 0$ et on note

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x) = \mathcal{F}_{add}(\chi)(\psi) = \mathcal{F}_{mul}(\psi)(\chi)$$

Où $\mathcal{F}_{add}$ est la transformée de Fourier dans $\mathbb{F}_q$ et $\mathcal{F}_{mul}$ celle dans $\mathbb{F}_q^\times$.

Lemme. *$A_1, A_2..A_r$ des parties de G, $S = \{(a_1, .., a_r) \in A_1 \times .. \times A_r$ t.q. $a_1 + .. + a_r = 0\}$. On a :*

$$|S| = \frac{|A_1 \times .. \times A_r|}{|G|} + R$$
$$où\ R = \frac{1}{|G|} \sum_{\chi \in \hat{G},\ \chi \neq \chi_0} \prod_{i=1}^{r} \widehat{1_{A_i}}(\chi)$$

Démonstration. On a

$$\begin{aligned} |S| &= \sum_{a_1 + .. + a_r = 0} \prod_{i=1}^{r} 1_{A_i}(a_i) \\ &= 1_{A_1}(a_1) * .. 1_{A_r}(a_r)(0) \\ &= \frac{1}{|G|} \sum_{\chi \in \hat{G}} \prod_{i=1}^{r} \widehat{1_{A_i}}(\chi) \end{aligned}$$

On a utilisé la transformée de Fourier inverse, et le fait que la transformée de Fourier transforme convolution en produits. Il suffit d'isoler le terme $\chi = \chi_0$. □

Corollaire. *Dans le cas $r = 3$, S est non vide dès que*

$$\frac{\Lambda(A_3)}{A_3} < \frac{\sqrt{|A_1 \times A_2|}}{|G|} \tag{1}$$

Où $\Lambda(A) := \max_{\chi \in \hat{G},\ \chi \neq \chi_0} |\widehat{1_A}(\chi)|$.

Démonstration. Il suffit de montrer que sous cette condition, on a $R < \frac{|A_1 \times A_2 \times A_3|}{|G|}$. Avec une inégalité de Cauchy-Schwarz, on a :

$$\begin{aligned} R &\leq \frac{\Lambda(A_3)}{|G|} \left(\sum_{\chi \in \hat{G}} |\widehat{1_{A_1}}(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \in \widehat{G}} |\widehat{1_{A_2}}(\chi)|^2 \right)^{1/2} \\ &= \Lambda(A_3) \left(\sum_{x \in G} |1_{A_1}(x)|^2 \right)^{1/2} \left(\sum_{x \in G} |1_{A_2}(x)|^2|^2 \right)^{1/2} \\ &= \Lambda(A_3) \sqrt{|A_1 \times A_2|} \end{aligned}$$

Ce qui conclut. □

Théorème. *Soit q un nombre premier, k un entier et $d = k \wedge (q-1)$ tel que $q > d^4 + 4$. Alors $x^k + y^k = z^k$ admet des solutions non triviales dans $\mathbb{F}_q$.*

Démonstration. Notons $H = \{x^k,\ x \in \mathbb{F}_q^\times\} = \{x^d,\ x \in \mathbb{F}_q^\times\}$ (on a égalité par une relation de Bézout entre $k, q-1, d$). C'est un sous-groupe multiplicatif d'indice d.
On va appliquer le corollaire avec $A_1, A_2, A_3 = -H, H, H$ dans G le groupe (additif !) $\mathbb{F}_q$. Le terme de droite dans (1) vaut $\frac{q-1}{qd}$, il suffit donc de montrer :

$$\Lambda(H) < \frac{(q-1)^2}{qd^2}$$

Soit ψ un caractère non trivial de $\mathbb{F}_q$, on a :

$$\begin{aligned} \widehat{1_H}(\psi) &= \sum_{x \in H} \psi(x) \\ &= \frac{1}{q-1} \sum_{x \in H} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} G(\chi, \psi) \bar{\chi}(x) \\ &= \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} G(\chi, \psi) \sum_{x \in H} \bar{\chi}(x) \\ &= \frac{1}{d} \sum_{\chi \in H^\perp} G(\chi, \psi) \end{aligned}$$

Pour tout caractère non trivial χ, $|G(\chi, \psi)| = \sqrt{q}$ et $G(1, \psi) = -1$, d'où $\widehat{1_H}(\psi) \leq \frac{1 + (d-1)\sqrt{q}}{d} < \sqrt{q}$.
Il suffit alors de vérifier $\sqrt{q} \leq \frac{(q-1)^2}{qd^2}$, c'est-à-dire $d^4 < \frac{(q-1)^4}{q^3}$; $q > d^4 + 4$ convient. En effet, $(q-1)^4 = (q^2 - 2q + 1)^2 > (q^2 - 2q)^2 = q^4 - 4q^3 + 4q^2 > (q-4)q^3$. □

Référence : Peyré