

Équation de Fermat sur un corps fini

Lemme (admis). Soient G un groupe abélien fini, $A_1, \dots, A_r$ des parties non vides de G et $a \in G$. Le nombre de solutions de l'équation $x_1 + \dots + x_r = a$, d'inconnue $(x_1, \dots, x_r) \in A_1 \times \dots \times A_r$ est

$$\frac{|A_1| \dots |A_r|}{|G|} + R,$$

où

$$R = \sum_{\substack{\chi \in \widehat{G} \\ \chi \neq \chi_0}} \prod_{i=1}^r \widehat{\mathbf{1}_{A_i}}(\chi).$$

Proposition. Soient $k \geq 1$ un entier et $d = \text{pgcd}(d, q-1)$. Si $q \geq d^4 + 4$, l'équation $x^k + y^k = z^k$ possède des solutions dans $(\mathbb{F}_q^\times)^3$.

Démonstration : avant de nous intéresser au cas particulier d'une équation sur $\mathbb{F}_q$, commençons par majorer $|R|$ lorsque $r = 3$. Pour $A \subset G$, notons

$$\Phi(A) = \max \left\{ |\widehat{\mathbf{1}_A}(\chi)|, \chi \neq \chi_0 \right\}.$$

On a alors

$$\begin{aligned} |R| &\leq \frac{1}{|G|} \sum_{\chi \neq \chi_0} |\widehat{\mathbf{1}_{A_1}}(\chi)| |\widehat{\mathbf{1}_{A_2}}(\chi)| |\widehat{\mathbf{1}_{A_3}}(\chi)| \\ &\leq \frac{1}{|G|} \Phi(A_3) \left(\sum_{\chi \in \widehat{G}} |\widehat{\mathbf{1}_{A_1}}(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \in \widehat{G}} |\widehat{\mathbf{1}_{A_2}}(\chi)|^2 \right)^{1/2} && \text{par inégalité de Cauchy-Schwarz} \\ &= \frac{1}{|G|} \Phi(A_3) \sqrt{|G|} \|\widehat{\mathbf{1}_{A_1}}\|_2 \sqrt{|G|} \|\widehat{\mathbf{1}_{A_2}}\|_2 \\ &= \sqrt{|G|} \|\mathbf{1}_{A_1}\|_2 \sqrt{|G|} \|\mathbf{1}_{A_2}\|_2 && \text{par formule de Plancherel} \end{aligned}$$

Or, pour toute partie $A \subset G$, on a

$$\|\mathbf{1}_A\|_2^2 = \frac{1}{|G|} \sum_{s \in G} |\mathbf{1}_A|^2 = \frac{|A|}{|G|};$$

par suite, on a $|R| \leq \Phi(A_3) \sqrt{|A_1| |A_2|}$.

Intéressons-nous à présent au cas particulier où G est le groupe additif $\mathbb{F}_q$. On a

$$\{x^k, x \in \mathbb{F}_q^\times\} = \{x^d, x \in \mathbb{F}_q^\times\};$$

en effet, si l'on écrit $k = dk'$, on a $x^k = (x^{k'})^d$ pour tout $x \in \mathbb{F}_q^\times$, et si l'on écrit $d = ku + (q-1)v$ grâce au théorème de Bézout, il vient $x^d = (x^u)^k$ pour tout $x \in \mathbb{F}_q^\times$, puisque $x^{q-1} = 1$ en vertu du théorème de Lagrange appliqué dans $\mathbb{F}_q^\times$. Il suffit donc de prouver que l'équation $x^d + y^d = z^d$ possède des solutions.

Notons $H_d = \{x^d, x \in \mathbb{F}_q^\times\}$ l'unique sous-groupe d'indice d de $\mathbb{F}_q^\times$ et $G_d = \{\chi \in \widehat{\mathbb{F}_q^\times}, \chi^d = \chi_0\}$ l'unique sous-groupe d'ordre d de $\widehat{\mathbb{F}_q^\times}$. On a alors $G_d = H_d^\perp \cong \mathbb{F}_q^\times / H_d$.

Soit $\psi \in \widehat{\mathbb{F}_q}$. Considérons la somme

$$\frac{1}{d} \sum_{\chi \in G_d} G(\chi, \psi) = \frac{1}{d} \sum_{x \in \mathbb{F}_q^\times} \psi(x) \sum_{\chi \in G_d} \chi(x).$$

Par orthogonalité des caractères de $\widehat{G_d} \cong F_q^\times / H_d$, la somme

$$\sum_{\chi \in G_d} \chi(x)$$

vaut $|G_d| = d$ si $x \in H_d$ et vaut 0 sinon. Ainsi,

$$\frac{1}{d} \sum_{\chi \in G_d} G(\chi, \psi) = \sum_{x \in H_d} \psi(x) = \widehat{\mathbf{1}_{H_d}}(\psi).$$

Comme $|G(\chi, \psi)| = \sqrt{q}$ dès que $(\chi, \psi) \neq (\chi_0, \psi_0)$, il vient

$$\Phi(H_d) \leq \frac{1}{d} \sum_{\chi \in G_d} \sqrt{q} = \sqrt{q}.$$

Considérons les ensembles

$$\mathcal{E} = \{(x, y, z) \in A_1 \times A_2 \times \mathbb{F}_q^\times, x + y = z^d\}$$

et

$$\mathcal{E}' = \{(x, y, u) \in A_1 \times A_2 \times H_d, x + y = u\}.$$

L'application

$$\begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E}' \\ (x, y, z) & \longmapsto & (x, y, z^d) \end{array}$$

est surjective et ses fibres sont toutes de cardinal d , donc $|\mathcal{E}| = d|\mathcal{E}'|$. D'après le lemme admis, et les majorations de $|R|$ et de $\Phi(H_d)$, on a

$$\left| |\mathcal{E}'| - \frac{1}{q} |A_1| |A_2| \frac{q-1}{d} \right| \leq \sqrt{q |A_1| |A_2|},$$

d'où, multipliant cette inégalité par d ,

$$\left| |\mathcal{E}| - \frac{1}{q} |A_1| |A_2| (q-1) \right| \leq d \sqrt{q |A_1| |A_2|}.$$

Si

$$q \geq \frac{(q-1)^2 d^2}{|A_1| |A_2|} + 4,$$

alors

$$d \sqrt{q |A_1| |A_2|} = |A_1| |A_2| \sqrt{\frac{q(q-1)^2 d^2}{(q-1)^2 |A_1| |A_2|}} \leq |A_1| |A_2| \sqrt{\frac{q(q-4)}{(q-1)^2}} < |A_1| |A_2| \frac{q-1}{q},$$

la dernière inégalité étant vraie car équivalente à $6q^2 - 4q + 1 > 0$, qui est vraie pour tout réel q . On a alors $|\mathcal{E}| > 0$.

Prenons $A_1 = A_2 = H_d$, de sorte que $\mathcal{E}$ est non vide si et seulement si l'équation $x^k + y^k = z^k$ possède des solutions. La condition $q \geq d^4 + 4$ entraîne

$$q \geq \frac{(q-1)^2 d^2}{|A_1| |A_2|} + 4,$$

donc $\mathcal{E}$ est non vide, d'après ce qui précède. ■