Nombre de solutions d'équations sur des corps finis

Baptiste Arnaudo

2022-2023

Table des matières

1 Introduction **1**

2 Généralités sur les caractères **1**

3 Quelques propriétés des sommes de Gauss **3**

4 Nombre de solutions d'équations polynomiales dans $\mathbb{F}_p$ **4**

5 Méthodes plus générales, application au théorème de Fermat-Wiles sur $\mathbb{F}_{p^n}$ **6**
5.1 Cadre et résultats généraux 7
5.2 Application à l'équation de Fermat sur $\mathbb{F}_q$ 7

6 Commentaires **9**

7 Annexe **9**

8 Références **9**

1 Introduction

Dans ce travail, nous utilisons la dualité des groupes abéliens finis pour donner une estimation (et parfois calculer) le nombre d'éléments de ce groupe solutions d'une équation algébrique.
Nous commençons par introduire les concepts centraux d'orthogonalité des caractères et de transformée de Fourier sur un groupe. Nous nous intéressons ensuite à certaines équations algébriques sur $\mathbb{F}_p$, avant de présenter une autre méthode, plus générale, permettant de montrer que si $k \in \mathbb{N}^*$, l'équation $x^k + y^k = z^k$ admet au moins une solution non triviale dans $\mathbb{F}_q$ pour $q = p^n$ assez grand.

2 Généralités sur les caractères

Définition 1. ***Caractères et dual d'un groupe***
Soit G un groupe. On appelle ***caractère*** *de G tout morphisme de groupes $\chi : G \longrightarrow (\mathbb{C}^*, \times)$. On appelle* ***dual*** *de G, noté $\widehat{G}$, l'ensemble des caractères de G. Muni du produit de deux fonctions, c'est un groupe abélien.*

Définition 2. *Si G est un groupe, on note $\mathbb{C}[G]$ l'ensemble des applications de G dans $\mathbb{C}$. C'est un $\mathbb{C}$-espace vectoriel, de dimension $|G|$ quand G est fini.*

On se donne désormais G un groupe abélien fini de cardinal n.

Proposition 1.

$$\forall \chi \in \hat{G}, \quad \chi(G) \subset \mathbb{U}_n$$

Si de plus G est cyclique de générateur x_0, alors en notant pour $0 \leq j \leq n-1$,

$$\begin{aligned} \chi_j \ &: G \to \mathbb{C}^* \\ x = x_0^k &\mapsto e^{\frac{2ijk\pi}{n}} \qquad 0 \leq k \leq n-1 \end{aligned}$$

on a $\widehat{G} = \{\chi_j, \quad 0 \leq j \leq n-1\}$.

Démonstration. On sait que $\forall x \in G, x^n = e_G$, d'où $\forall x \in G$, $\forall \chi \in \widehat{G}$, $\chi(x)^n = \chi(x^n) = \chi(e_G) = 1$.
Si G est cyclique, on peut s'en donner un générateur x_0. Alors, tout $\chi \in \widehat{G}$ est entièrement déterminé par l'image de x_0, qui vaut $e^{\frac{2ij\pi}{n}}$ pour un certain $j \in [\![0; n-1]\!]$, d'où l'autre résultat. □

Remarques. On obtient alors que $\widehat{G} \simeq \mathbb{Z}/n\mathbb{Z} \simeq G$. L'isomorphie entre G et son dual est encore vérifiée si G est seulement abélien et fini, **nous l'admettrons**. On a ainsi $\widehat{G} \simeq G$ et donc $|\widehat{G}| = |G|$.

Proposition 2. *Si $(\chi, \psi) \in \widehat{G}^2$, on définit $(\chi, \psi) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}$. On munit ainsi $\mathbb{C}[G]$ d'une structure d'espace hermitien.*

Théorème 1. ***Orthogonalité des caractères***
$\widehat{G}$ est une base orthonormée de $\mathbb{C}[G]$ pour le produit scalaire introduit.

Démonstration. On commence par montrer le lemme suivant :

Lemme 1. Si $\chi \in \widehat{G}$ alors

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{si } \chi = \chi_0 \text{ (le caractère trivial valant 1 partout)} \\ 0 & \text{sinon} \end{cases} \tag{1}$$

En effet, si $\chi = \chi_0$ le résultat est clair, et si $\chi \neq \chi_0$, $\exists g_0 \in G$, $\chi(g_0) \neq 1$. Alors puis que $x \mapsto g_0 x$ est bijective, on a $\sum_{g \in G} \chi(x) = \sum_{g \in G} \chi(g_0 x) = \chi(g_0) \sum_{g \in G} \chi(x)$ et puisque $\chi(g_0 x) \neq 1$, $\sum_{g \in G} \chi(x) = 0$.
Dès lors, si $(\chi, \psi) \in \widehat{G}^2$, $\chi\overline{\psi} \in \widehat{G}$ et le caractère orthogonal de $\widehat{G}$ suit immédiatement en appliquant le lemme à $\chi\overline{\psi}$. Puisque $\dim(\mathbb{C}[G]) = |G| = |\widehat{G}|$, $\widehat{G}$ est bien une base orthonormée de $\mathbb{C}[G]$. □

Corollaire .1. En appliquant le lemme à $\hat{x} : \chi \mapsto \chi(x)$, qui est donc un élément de $\widehat{\widehat{G}}$, on obtient que, si $x \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |G| & \text{si } x = e_G \\ 0 & \text{sinon} \end{cases} \tag{2}$$

Cette remarque sera importante pour la suite.

Corollaire .2. $\forall f \in \mathbb{C}[G], f = \sum_{\chi \in \widehat{G}} (f, \chi)\chi$

Cela nous amène à la définition de la transformée de Fourier d'un élément f de $\mathbb{C}[G]$.

Définition 3. ***Transformée de Fourier***
*On appelle **transformée de Fourier** l'application linéaire*

$$\begin{aligned} \mathcal{F} \ &: \mathbb{C}[G] \to \mathbb{C}[\widehat{G}] \\ &f \mapsto \hat{f} \end{aligned}$$

où $\hat{f} : \chi \mapsto |G|(f, \overline{\chi}) = \sum_{g \in G} f(g)\chi(g)$.

Proposition 3. ***Transformation inverse***
On a la formule :

$$\forall f \in \mathbb{C}[G], \quad f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi^{-1}$$

3 Quelques propriétés des sommes de Gauss

Nous nous intéressons maintenant au cas d'un corps fini $\mathbb{F}_q$ où q est une puissance d'un nombre premier. Il y existe deux structures de groupes, $(\mathbb{F}_q, +)$ et $(\mathbb{F}_q^*, \times)$, et donc deux types de caractères : les caractères additifs, éléments de $\widehat{(\mathbb{F}_q, +)}$ et les caractères multiplicatifs, éléments de $\widehat{(\mathbb{F}_q^*, \times)}$. On notera χ les caractères multiplicatifs et ψ les caractères additifs.

Définition 4. ***Sommes de Gauss***

Si $\chi \in \widehat{(\mathbb{F}_q^*, \times)}$, $\psi \in \widehat{(\mathbb{F}_q, +)}$, on appelle ***somme de Gauss*** *associée à χ et ψ la quantité*

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x)$$

Dorénavant, nous prolongeons tout caractère multiplicatif χ **non trivial** en un caractère $\tilde{\chi}$ défini sur $\mathbb{F}_q$ (que nous noterons encore χ) en posant $\tilde{\chi}(0) = 0$. Cela nous permet de voir $G(\chi, \psi)$ comme $\mathcal{F}(\tilde{\chi})(\psi)$ (où $\mathcal{F}$ est donc la transformée de Fourier définie sur $\mathbb{C}[\mathbb{F}_q]$) et d'énoncer la proposition suivante :

Proposition 4. $\forall \chi \in \widehat{\mathbb{F}_q}$,

$$\chi = \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} G(\chi, \overline{\psi})\psi$$

Démonstration. On applique la proposition 3 à χ, il vient $\chi = \frac{1}{q}\sum_{\psi \in \widehat{\mathbb{F}_q}} \hat{\chi}(\psi)\psi^{-1}$ avec $\hat{\chi}(\psi) = \sum_{g \in G} \chi(g)\psi(g) = G(\chi, \psi)$. Le résultat vient alors directement après avoir effectué le changement de variable $\psi \mapsto \psi^{-1} = \overline{\psi}$ dans la somme. □

Théorème 2. ***Module des sommes de Gauss***

Si $\chi \in \widehat{\mathbb{F}_q^*}$ et $\psi \in \widehat{\mathbb{F}_q}$ sont deux caractères ***non triviaux****, alors $|G(\chi, \psi)| = \sqrt{q}$.*

Démonstration.

$$|G(\chi,\psi)|^2 = \Big(\sum_{x\in\mathbb{F}_q^*}\chi(x)\psi(x)\Big)\overline{\Big(\sum_{y\in\mathbb{F}_q^*}\chi(y)\psi(y)\Big)} = \sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q^*}\chi(xy^{-1})\psi(x-y) = \sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q^*}\chi(x)\psi(y(x-1))$$

où l'on a effectué le changement de variable $u = xy^{-1}$. Ensuite,

$$|G(\chi,\psi)|^2 = \sum_{x\in\mathbb{F}_q^*}\chi(x)\sum_{y\in\mathbb{F}_q^*}\psi(y(x-1)) = q-1+\sum_{x\in\mathbb{F}_q^*,x\neq 1}\chi(x)\sum_{y\in\mathbb{F}_q^*}\psi(y(x-1)) = q-1-\sum_{x\in\mathbb{F}_q^*,x\neq 1}\chi(x) = q-1-(-1) = q$$

où on a encore effectué un changement de variables $u = y(x-1)$ lors du passage à la dernière égalité. On s'est ensuite servi du fait que $\sum_{x\in\mathbb{F}_q}\psi(x) = 0$ en vertu du lemme 1. □

On se place désormais sur $\mathbb{F}_p$ avec p un nombre premier impair. $\mathbb{F}_p$ étant cyclique, on sait que les éléments de $\widehat{\mathbb{F}_p}$ sont, d'après la proposition 1, les

$$\begin{aligned}\psi_j \ : \mathbb{F}_p &\to \mathbb{C}^* \\ x &\mapsto e^{\frac{2ijx\pi}{p}} \qquad 0 \leq j \leq p-1\end{aligned}$$

(Par abus, nous confondons classe dans $\mathbb{F}_p$ et représentant). Nous montrons un dernier lemme :

Lemme 2. $\forall x \in \mathbb{F}_p^*, \forall j \in [\![0; p-1]\!], \forall \chi \in \mathbb{F}_p^*, G(\chi, \psi_j) = \chi(x)G(\chi, \psi_{jx})$

Démonstration. $G(\chi, \psi_j) = \sum_{y\in\mathbb{F}_p} \chi(y)e^{\frac{2ijy\pi}{p}} = \sum_{y\in\mathbb{F}_p} \chi(xy)e^{\frac{2ijxy\pi}{p}} = \chi(x)G(\chi, \psi_{jx})$ grâce au changement de variable $u = xy$ (x est bien non nul). □

4 Nombre de solutions d'équations polynomiales dans $\mathbb{F}_p$

On se donne $n \in \mathbb{N}^*$ ainsi que $F \in \mathbb{F}_p[X_1, ..., X_n]$. On cherche à étudier la quantité

$$N(F, p) = |\{(x_1, ..., x_n) \in \mathbb{F}_p^n, \quad F(x_1, ..., x_n) = 0\}|$$

On sait déjà, en vertu du corollaire 1.1, que $x \mapsto \frac{1}{p}\sum_{\psi\in\widehat{\mathbb{F}_p}} \psi(x)$ est la fonction indicatrice de $\{0\}$, la quantité recherchée vaut donc

$$N(F, p) = \frac{1}{p} \sum_{(x_1,...,x_n)\in\mathbb{F}_p^n} \sum_{\psi\in\widehat{\mathbb{F}_p}} \psi(F(x_1, ..., x_n)) = \frac{1}{p} \sum_{(x_1,...,x_n)\in\mathbb{F}_p^n} \sum_{j=0}^{p-1} \psi_j(F(x_1, ..., x_n))$$

On fixe θ un générateur de $\mathbb{F}_p^*$. Pour $x \in \mathbb{F}_p^*$ et $r \in \mathbb{N}^*$, on note $\nu(x) = |\{y \in \mathbb{F}_p^*, y^r = x\}|$. On a alors le résultat suivant :

Théorème 3. *Soit $x = \theta^k$, $0 \leq k \leq p-2$. On note $\delta = r \wedge (p-1)$. Alors,*

$$\nu(x) = \begin{cases} \delta & \text{si } \delta | k \\ 0 & \text{sinon} \end{cases} \tag{3}$$

Démonstration. Soit $y = \theta^{k'} \in \mathbb{F}_p^*$. Si $y^r = x$ alors $k \equiv rk' \pmod{p-1}$ et donc $\delta | k$. Par suite, si $\delta \nmid k$, $\nu(x) = 0$. Dès lors,

$$y^r = x \Leftrightarrow rk' \equiv k \pmod{p-1} \Leftrightarrow \frac{r}{\delta}k' \equiv \frac{k}{\delta} \pmod{\frac{p-1}{\delta}} \Leftrightarrow k' \equiv \left(\frac{r}{\delta}\right)^{-1} \frac{k}{\delta} \pmod{\frac{p-1}{\delta}}$$

car $\frac{r}{\delta} \wedge \frac{p-1}{\delta} = 1$ donc $\frac{r}{\delta}$ est inversible modulo $\frac{p-1}{\delta}$. Ainsi, k' est entièrement déterminé modulo $\frac{p-1}{\delta}$. Si $\theta^{k'_0}$ est solution particulière, les autres sont les $\theta^{k'}$ où $k' = k'_0 + s\frac{p-1}{\delta}$: il y a exactement δ k' distincts modulo $p-1$ d'où le résultat. □

Pour $a \in \mathbb{F}_p^*$, on note $S(a, r) = \sum_{y\in\mathbb{F}_p} \psi_a(y^r)$.

Proposition 5. *Avec les notations précédentes pour δ, en notant $\Gamma_\delta = \{\chi \in \widehat{\mathbb{F}_p^*}, \chi \neq \chi_0, \chi^\delta = \chi_0\}$, on a*

$$S(a, r) = \sum_{\chi\in\Gamma_\delta} G(\chi, \psi_a)$$

Démonstration. Essentiellement du calcul. □

On énonce maintenant un des théorèmes principaux :

Théorème 4. *Soient $n \geq 3$, $(a_1, ..., a_n) \in (\mathbb{F}_p^{*n})$, $(r_1, ..., r_n) \in (\mathbb{N}^*)^n$, on pose $F(X_1, ..., X_n) = \sum_{k=1}^n a_k X_k^{r_k}$ ainsi que $\delta_k = r_k \wedge (p-1)$. Alors,*

$$N(F,p) = p^{n-1} + \frac{1}{p} \sum_{x \in \mathbb{F}_p^*} \prod_{i=1}^n \sum_{\chi \in \Gamma_{\delta_i}} G(\chi, \psi_{a_i x})$$

Démonstration. D'après la remarque du début de la section,

$$N(F,p) = \frac{1}{p} \sum_{(x_1,...,x_n) \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \psi_j(F(x_1, ..., x_n)) = p^{n-1} + \frac{1}{p} \sum_{j=1}^{p-1} \sum_{(x_1,...,x_n) \in \mathbb{F}_p^n} \psi_j(F(x_1, ..., x_n))$$

On note $\zeta = e^{\frac{2i\pi}{p}}$, alors,

$$N(F,p) = p^{n-1} + \frac{1}{p} \sum_{j=1}^{p-1} \sum_{(x_1,...,x_n) \in \mathbb{F}_p^n} \prod_{i=1}^n \zeta^{j a_i x_i^{r_i}} = p^{n-1} + \frac{1}{p} \sum_{j=1}^{p-1} \prod_{i=1}^n \sum_{y \in \mathbb{F}_p} \zeta^{j a_i y^{r_i}} = p^{n-1} + \frac{1}{p} \sum_{j=1}^{p-1} \prod_{i=1}^n S(a_i j, r_i)$$

$$= p^{n-1} + \frac{1}{p} \sum_{j=1}^{p-1} \prod_{i=1}^n \sum_{\chi \in \Gamma_{\delta_i}} G(\chi, \psi_{a_i j})$$

d'après la proposition 5. □

Regardons le cas $r_1 = ... = r_n = 2$. On montrera en annexe qu'il n'existe qu'un seul caractère multiplicatif d'ordre 2 sur $\mathbb{F}_p$, appelé **symbole de Legendre**, que l'on notera $\left(\frac{\div}{p}\right)$, défini pour $a \in \mathbb{F}_p$ par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a \text{ est un carré non nul dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases} \tag{4}$$

Puisque $r_1 = ... = r_n = 2$, $\forall i \in [\![1; n]\!]$, $\delta_i = 2$ donc $\Gamma_{\delta_i} = \{\left(\frac{\div}{p}\right)\}$. On peut alors calculer explicitement $N(F,p)$!

Lemme 3. Si a et b sont deux éléments de $\mathbb{F}_p^*$, $G\left(\left(\frac{\div}{p}\right), \psi_a\right) G\left(\left(\frac{\div}{p}\right), \psi_b\right) = p\left(\frac{-ab}{p}\right)$.

Démonstration. D'après le lemme 2, $G\left(\left(\frac{\div}{p}\right), \psi_a\right) = \left(\frac{a}{p}\right) G\left(\left(\frac{\div}{p}\right), \psi_1\right)$ et $G\left(\left(\frac{\div}{p}\right), \psi_b\right) = \left(\frac{-b}{p}\right) G\left(\left(\frac{\div}{p}\right), \psi_{-1}\right)$. Or $\left(\frac{\div}{p}\right)$ est à valeurs réelles donc $G\left(\left(\frac{\div}{p}\right), \psi_{-1}\right) = G\left(\overline{\left(\frac{\div}{p}\right)}, \psi_{-1}\right) = \overline{G\left(\left(\frac{\div}{p}\right), \psi_1\right)}$ d'où $G\left(\left(\frac{\div}{p}\right), \psi_a\right) G\left(\left(\frac{\div}{p}\right), \psi_b\right) = \left(\frac{-ab}{p}\right) \left|G\left(\left(\frac{\div}{p}\right), \psi_1\right)\right|^2 = p\left(\frac{-ab}{p}\right)$ d'après le théorème 2. □

On en déduit la proposition suivante :

Proposition 6. *Si $F(X_1, ..., X_n) = \sum_{k=1}^n a_k X_k^2 \in \mathbb{F}_p[X_1, ..., X_n]$ alors :*

$$N(F,p) = \begin{cases} p^{n-1} & \text{si } n \text{ est impair} \\ p^{n-1} + \left(\frac{(-1)^{\frac{n}{2}} a_1 ... a_n}{p}\right) (p-1) p^{\frac{n}{2}-1} & \text{si } n \text{ est pair} \end{cases} \tag{5}$$

Démonstration. Si n est impair, on déduit du lemme 3 que $\forall j \in [\![1; p-1]\!]$,

$$\prod_{i=1}^{n} G\left(\left(\frac{\cdot}{p}\right), \psi_{a_i j}\right) = p^{\frac{n-1}{2}} \left(\frac{(-1)^{\frac{n-1}{2}} a_1 ... a_{n-1} j^{n-1}}{p}\right) G\left(\left(\frac{\cdot}{p}\right), \psi_{a_n j}\right) = p^{\frac{n-1}{2}} \left(\frac{(-1)^{\frac{n-1}{2}} a_1 ... a_{n-1}}{p}\right) G\left(\left(\frac{\cdot}{p}\right), \psi_{a_n j}\right)$$

car $n-1$ est pair donc $\left(\frac{j^{n-1}}{p}\right) = 1$. Alors,

$$N(F,p) = p^{n-1} + p^{\frac{n-3}{2}} \left(\frac{(-1)^{\frac{n-1}{2}} a_1 ... a_{n-1}}{p}\right) \sum_{j=1}^{p-1} G\left(\left(\frac{\cdot}{p}\right), \psi_{a_n j}\right)$$

En calculant la somme de droite, on montre qu'elle est nulle, d'où $N(F,p) = p^{n-1}$.
Si n est pair, on a cette fois :

$$\prod_{i=1}^{n} G\left(\left(\frac{\cdot}{p}\right), \psi_{a_i j}\right) = p^{\frac{n}{2}} \left(\frac{(-1)^{\frac{n}{2}} a_1 ... a_n}{p}\right)$$

d'où $N(F,p) = p^{n-1} + \left(\frac{(-1)^{\frac{n}{2}} a_1 ... a_n}{p}\right)(p-1)p^{\frac{n}{2}-1}$ □

Dans le cas plus général où $r_1, ..., r_n$ sont quelconques, on ne sait pas s'il existe une expression plus explicite de $N(F,p)$. Néanmoins, les résultats établis jusqu'ici permettent d'en établir une estimation, ainsi qu'une estimation de l'erreur. Précisément, on a le théorème :

Théorème 5. *Il existe une constante $C(F)$ ne dépendant que de F telle que*

$$|N(F,p) - p^{n-1}| \leq C(F)\frac{p-1}{p} p^{\frac{n}{2}}$$

En conséquence, $N(F,p) = p^{n-1} + O(p^{\frac{n}{2}})$.

Démonstration. D'après le théorème 4,

$$|N(F,p) - p^{n-1}| = \left|\frac{1}{p} \sum_{x \in \mathbb{F}_{|}^{*}} \prod_{i=1}^{n} \sum_{\chi \in \Gamma_{\delta_i}} G(\chi, \psi_{a_i x})\right| \leq \frac{1}{p} \sum_{x \in \mathbb{F}_{|}^{*}} \prod_{i=1}^{n} \sum_{\chi \in \Gamma_{\delta_i}} |G(\chi, \psi_{a_i x})| \leq \frac{1}{p} \sum_{x \in \mathbb{F}_{|}^{*}} \prod_{i=1}^{n} \delta_i \sqrt{p}$$

d'après le théorème 2. Or,

$$\prod_{i=1}^{n} \delta_i \leq \prod_{i=1}^{n} r_i = C(F)$$

d'où $|N(F,p) - p^{n-1}| \leq C(F)\frac{p-1}{p} p^{\frac{n}{2}}$. □

5 Méthodes plus générales, application au théorème de Fermat-Wiles sur $\mathbb{F}_{p^n}$

Certaines des méthodes utilisées pour obtenir les résultats précédents ne sont valables que sur $\mathbb{F}_p$ (on précisera ce point plus loin) : on présente donc ici des méthodes générales d'étude d'équation sur un groupe abélien G, que nous appliquerons à l'équation $x^k + y^k = z^k$ sur $\mathbb{F}_{p^n}$.

5.1 Cadre et résultats généraux

On considère un groupe abélien G fini **noté additivement**, $k \in \mathbb{N}^*$, des ensembles $A_1, ..., A_k \subset G$ et $a \in G$. On s'intéresse à l'équation $x_1 + ... + x_k = a$ où $\forall i \in [\![1; k]\!]$, $x_k \in A_k$. On note N le nombre de solutions. On remarque que, puisque $x \mapsto x - a$ est bijective, on ne change pas N en changeant l'un des A_k en $A_k - a$: on peut donc supposer $a = 0$. En vertu de la remarque au début de la section 4, on a l'expression :

$$N = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \sum_{(x_1,...,x_n) \in A_1 \times ... \times A_n} \chi(x_1 + ... + x_n) = \frac{|A_1|...|A_n|}{|G|} + \frac{1}{|G|} \sum_{\chi \in \widehat{G}, \chi \neq \chi_0} \sum_{(x_1,...,x_n) \in A_1 \times ... \times A_n} \chi(x_1)...\chi(x_n)$$

Or la somme de droite se réécrit

$$\prod_{i=1}^{k} \sum_{x \in A_i} \chi(x) = \prod_{i=1}^{k} \hat{f}_{A_i}(\chi)$$

où on a noté f_A la fonction caractéristique de l'ensemble $A \subset G$, d'où :

$$N = \frac{|A_1|...|A_n|}{|G|} + \frac{1}{|G|} \sum_{\chi \in \widehat{G}, \chi \neq \chi_0} \prod_{i=1}^{k} \hat{f}_{A_i}(\chi)$$

Notons R (comme « reste ») le terme de droite. L'objectif est de contrôler sa taille, pour ce faire on introduit pour $A \subset G$ la quantité $\Phi(A) = \max\Big(\{|\hat{f}_A(\chi)|, \chi \in \widehat{G}, \chi \neq \chi_0\}\Big)$. En vue d'étudier l'équation de Fermat sur $\mathbb{F}_{p^n}$, on se restreint désormais à $k = 3$. On énonce d'abord le lemme :

Lemme 4. Si $f \in \mathbb{C}[G]$, $||\hat{f}|| = \sqrt{|G|}||f||$. Puisqu'il est clair que si $A \subset G$, $||f_A|| = \sqrt{\frac{|A|}{|G|}}$, il s'ensuit que $||\hat{f}_A||^2 = |A|$.

Démonstration. Immédiat avec la définition 3. □

On énonce maintenant le théorème :

Théorème 6. *Si $A_1, A_2, A_3 \subset G$, si $\frac{\Phi(A_3)}{|A_3|} < \frac{\sqrt{|A_1||A_2|}}{|G|}$ alors l'équation $x_1 + x_2 + x_3 = a$, $a \in G$, $\forall i \in \{1; 2; 3\}, x_i \in A_i$ a au moins une solution.*

Démonstration. Il s'agit de montrer qu'alors $|R| < \frac{|A_1||A_2||A_3|}{|G|}$. On a :

$$|R| = \left| \frac{1}{|G|} \sum_{\chi \in \widehat{G}, \chi \neq \chi_0} \hat{f}_{A_1}(\chi)\hat{f}_{A_2}(\chi)\hat{f}_{A_3}(\chi) \right| \leq \frac{\Phi(A_3)}{|G|} \sum_{\chi \in \widehat{G}} |\hat{f}_{A_1}(\chi)||\hat{f}_{A_2}(\chi)| \leq \frac{\Phi(A_3)}{|G|} \sqrt{\sum_{\chi \in \widehat{G}} |\hat{f}_{A_1}(\chi)|^2} \sqrt{\sum_{\chi \in \widehat{G}} |\hat{f}_{A_2}(\chi)|^2}$$

d'après l'inégalité de Cauchy-Schwarz.
On reconnaît à droite les quantités $\sqrt{|G|^2||\hat{f}_{A_1}||^2||\hat{f}_{A_2}||^2} = |G|\sqrt{|A_1||A_2|}$ d'après le lemme 4, et ainsi

$$|R| \leq \Phi(A_3)\sqrt{|A_1||A_2|} < \frac{|A_1||A_2||A_3|}{|G|}$$

□

5.2 Application à l'équation de Fermat sur $\mathbb{F}_q$

Pour le moment, A_1 et A_2 restent quelconques. On se donne $k \in \mathbb{N}^*$ et on pose $A_3 = H_k = \{x^k, x \in \mathbb{F}_q^*\}$. En remarquant que $H_k = H_{k \wedge (q-1)}$, on est libre de supposer que $k|q-1$. On note N le nombre de solutions de $x + y = z^k$, $x \in A_1$, $y \in A_2$, $z \in \mathbb{F}_q^*$ et N' celui de $x + y = u$, où $u \in H_k$.

Lemme 5. On a $N = kN'$

Démonstration. Puisque $\mathbb{F}_q^*$ est cyclique, la preuve du théorème 3 s'applique et nous permet de déduire qu'il y a k racines de l'unité dans $\mathbb{F}_q^*$, d'où le résultat. □

Proposition 7. $\Phi(H_k) < \sqrt{q}$

Démonstration. On étend canoniquement les éléments de $\widehat{\mathbb{F}_q^*/H_k}$ en des éléments de $\widehat{\mathbb{F}_q^*}$ en les composant par $x \mapsto xH_k$. On les note $\chi_0, ..., \chi_{k-1}$ (car $\left|\widehat{\mathbb{F}_q^*/H_k}\right| = \left|\mathbb{F}_q^*/H_k\right| = k$). On remarque alors que si ψ est un caractère additif non trivial :

$$\sum_{i=0}^{k-1} G(\chi_i, \psi) = \sum_{x \in \mathbb{F}_q^*} \psi(x) \sum_{i=0}^{k-1} \chi_i(x)$$

D'après le lemme 1, la somme de droite vaut k si $x \in H_k$ et 0 sinon, d'où :

$$\sum_{i=0}^{k-1} G(\chi_i, \psi) = k \sum_{x \in H_k} \psi(x) = k\hat{f}_{H_k}(\psi)$$

Alors, $\forall \psi \in \widehat{\mathbb{F}_q}$, $\psi \neq \psi_0$,

$$|\hat{f}_{H_k}(\psi)| \leq \frac{1}{k} \sum_{i=0}^{k-1} |G(\chi_i, \psi)| = \frac{1 + (k-1)\sqrt{q}}{k} < \sqrt{q}$$

□

Théorème 7. *On pose $l_1 = \frac{q-1}{|A_1|}$ (et idem pour l_2). Alors, si $q \geq k^2 l_1 l_2 + 4$, l'équation $x + y = z^k$, $x \in A_1$, $y \in A_2$, $z \in \mathbb{F}_q^*$ admet au moins une solution.*

Démonstration. On sait que

$$\left| N' - \frac{|A_1||A_2||H_k|}{q} \right| = \left| \frac{N}{k} - \frac{|A_1||A_2|(q-1)}{kq} \right| \leq \Phi(H_k)\sqrt{|A_1||A_2|} < \sqrt{q|A_1||A_2|}$$

d'après la proposition 7, dès lors :

$$\left| N - \frac{|A_1||A_2|(q-1)}{q} \right| < k\sqrt{q|A_1||A_2|}$$

Or,

$$k\sqrt{q|A_1||A_2|} = k|A_1||A_2|\sqrt{\frac{l_1 l_2 q}{(q-1)^2}} \leq |A_1||A_2|\sqrt{\frac{(q-4)q}{(q-1)^2}}$$

On montre enfin par une étude de fonction que si $q > 1$, $\frac{(q-4)q}{(q-1)^2} \leq \frac{(q-1)^2}{q^2}$ et donc :

$$\left| N - \frac{|A_1||A_2|(q-1)}{q} \right| < \frac{|A_1||A_2|(q-1)}{q}$$

Alors, $N > 0$. □

Reste à prendre $A_1 = A_2 = H_k$, on a $l_1 = l_2 = k$ et on en déduit le théorème :

Théorème 8. *Si $k \in \mathbb{N}^*$, si $q \geq k^4 + 4$, l'équation $x^k + y^k = z^k$ a au moins une solution non triviale sur $\mathbb{F}_q$.*

6 Commentaires

Lors de mes recherches, j'ai essayé d'appliquer les méthodes de la section 4 à l'étude de l'équation de Fermat, mais j'ai rencontré le problème suivant : je ne connaissais pas a priori les caractères additifs de $\mathbb{F}_q$ quand q n'est pas premier, puisque $\mathbb{F}_q$ n'est pas cyclique (la proposition 1 ne s'applique pas). En creusant le sujet, j'ai découvert que l'on pouvait effectivement décrire les caractères additifs de $\mathbb{F}_{p^n}$ à l'aide de la trace de $\mathbb{F}_{p^n}$ sur $\mathbb{F}_p$, application $\mathbb{F}_p$-linéaire définie par :

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} \ : \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ x &\mapsto x + x^p + ... + x^{p^{m-1}} \end{aligned}$$

On définit alors le caractère additif canonique ψ_1 :

$$\begin{aligned} \psi_1 \ : \mathbb{F}_{p^n} &\to \mathbb{C}^* \\ x &\mapsto e^{\frac{2i\pi \mathrm{Tr}(x)}{p}} \end{aligned}$$

et alors $\forall \psi \in \widehat{\mathbb{F}_{p^n}}$, $\exists a \in \mathbb{F}_{p^n}$, $\forall x \in \mathbb{F}_{p^n}$, $\psi(x) = \psi_1(ax)$.
Sachant cela, il est possible de prouver des résultats tout à fait analogues à ceux de la fin de la section 4 pour le cas, plus général, de $\mathbb{F}_{p^n}$.

7 Annexe

Preuve de l'existence et l'unicité du caractère multiplicatif d'ordre 2 de $\mathbb{F}_p$: Puisque $\mathbb{F}_p^*$ est cyclique, et que $\mathbb{F}_p^* \simeq \widehat{\mathbb{F}_p^*}$, $\widehat{\mathbb{F}_p^*}$ l'est aussi, soit donc χ un générateur.
Si $\lambda = \chi^k$ est d'ordre 2, alors $p-1|2k$ car χ est d'ordre $p-1$, donc $\exists k' \in \mathbb{N}$, $k = \frac{p-1}{2}k'$, et puisque $0 < k < p-1$, $k' = 1$ donc $\lambda = \chi^{\frac{p-1}{2}}$, ce qui prouve l'existence et l'unicité.

Montrons que $\left(\frac{\cdot}{p}\right)$ est bien le caractère multiplicatif d'ordre 2 de $\mathbb{F}_p$: on montre la formule, valable quand p est impair (ce que l'on a supposé) :

$$\forall x \in \mathbb{F}_p^*, \quad \left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$$

Si $x = y^2 \in \mathbb{F}_p^*$, $x^{\frac{p-1}{2}} = 1$. p étant impair, $x \mapsto x^2$ est un morphisme dont le noyau, $\{-1;1\}$ est de cardinal 2, il y a donc $\frac{p-1}{2}$ résidus quadratiques, qui sont racines de $X^{\frac{p-1}{2}} - 1$. Ce polynôme ne pouvant avoir plus de $\frac{p-1}{2}$ racines, ses racines sont exactement les résidus quadratiques, on en déduit que $x^{\frac{p-1}{2}} = 1$ si et seulement si x est un résidu quadratique.
Dès lors, si $x^{\frac{p-1}{2}} = -1$, x n'est pas un résidu quadratique, et si x n'est pas un résidu quadratique, alors puisque $\left(x^{\frac{p-1}{2}}\right)^2 = 1$, $x^{\frac{p-1}{2}} \in \{-1;1\}$, donc $x^{\frac{p-1}{2}} = -1$ (car x n'est pas un résidu quadratique), ce qui achève la preuve.
On en déduit immédiatement que $\left(\frac{\cdot}{p}\right)$ est bien un morphisme, et que c'est le caractère multiplicatif d'ordre 2 de $\mathbb{F}_p$.

8 Références

[1] **André Weil**. Number of solutions of equations over finite fields, Bull. Amer. Math. Soc. 55 (1949)

[2] **László Babai**. The Fourier Transform and Equations over Finite Abelian Groups, Department of Computer Science, University of Chicago (1989)

[3] **Gabriel Peyré**. L'algèbre discrète de la transformée de Fourier

[4] **Jean-Marie Arnaudiès**. Problème de préparation à l'agrégation de mathématiques, 1. Algèbre, groupes, arithmétique

[5] **Théo Untrau**. Dualité des groupes abéliens finis et comptage de points.
https ://perso.eleves.ens-rennes.fr/people/theo.untrau/dualitecomptage.pdf