H. Hindry, Arithmétique, p. 90-92

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

L'objectif est ici de montrer le théorème suivant :

Théorème : Soient d divisant $q-1$ et S_d l'ensemble des m-uplets de caractères $(\chi_1, \dots, \chi_m)$ tels que $\chi_j \neq \chi_0$, $\chi_j^d = \chi_0$ et $\chi_1 \cdots \chi_m = \chi_0$, où χ_0 est le caractère trivial. Le nombre N de solutions de l'équation $a_1 x_1^d + \dots + a_m x_m^d = 0$ dans $\mathbb{F}_q^m$ est égal à :

$$N = q^{m-1} + \frac{q-1}{q} \sum_{(\chi_1,\dots,\chi_m) \in S_d} \overline{\chi_1}(a_1) \cdots \overline{\chi_m}(a_m)\, G(\chi_1, \psi) \cdots G(\chi_m, \psi).$$

On commence par fixer les notations. Soient p un nombre premier, $m \in \mathbb{N}^*$. On pose $q = p^m$. On définit la trace de $\mathbb{F}_q$ sur $\mathbb{F}_p$ comme étant l'application $\mathbb{F}_p$-linéaire $\mathrm{Tr}_{\mathbb{F}_p}^{\mathbb{F}_q} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$, $x \longmapsto x + x^p + \dots + x^{p^{m-1}}$. On construit alors un caractère additif $\psi : \mathbb{F}_q \longrightarrow \mathbb{C}^*$, $a \longmapsto \exp\left(\frac{2i\pi}{p} \mathrm{Tr}_{\mathbb{F}_p}^{\mathbb{F}_q} a\right)$.

Lemme 1 : Soit $b \in \mathbb{F}_q$. On a $\sum_{a \in \mathbb{F}_q} \psi(ab) = \begin{cases} q & \text{si } b = 0 \\ 0 & \text{si } b \neq 0 \end{cases}$.

Démonstration : Le résultat est clair si $b = 0$. Si $b \neq 0$, l'application $\mathbb{F}_q \longrightarrow \mathbb{F}_p$, $a \longmapsto \mathrm{Tr}_{\mathbb{F}_p}^{\mathbb{F}_q}(ab)$ est $\mathbb{F}_p$-linéaire et surjective, donc $\sum_{a \in \mathbb{F}_q} \psi(ab) = p^{m-1} \sum_{x \in \mathbb{F}_p} \exp\left(\frac{2i\pi x}{p}\right) = 0$.

On définit le caractère trivial χ_0 comme valant 1 sur tout $\mathbb{F}_q$.

Si $\chi : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ est un caractère non trivial, on le prolonge à $\mathbb{F}_q$ en posant $\chi(0) = 0$.

On pose alors, pour tout caractère χ, $G(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\, \psi(x)$.

Pour tous $d \in \mathbb{N}^*$ et $a \in \mathbb{F}_q$, on pose $T(d,a) = \sum_{y \in \mathbb{F}_q} \psi(a y^d)$, on

note G_d l'ensemble des caractères χ tels que $\chi^d = \chi_0$, et $G'_d = G_d \setminus \{\chi_0\}$.

Lemme 2: Soit d divisant $q-1$. Pour tout $a \in \mathbb{F}_q$, on a $T(d,a) = \sum_{\chi \in G'_d} \overline{\chi}(a)\, G(\chi)$.

Démonstration: Soit $x \in \mathbb{F}_q$. On a $\sum_{\chi \in G_d} \chi(x) = \begin{cases} d & \text{si } x \in \mathbb{F}_q^{*d} \\ 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases}$.

En effet, si $x = y^d \in \mathbb{F}_q^{*d}$, $\sum_{\chi \in G_d} \chi(x) = \sum_{\chi \in G_d} \chi(y)^d = \sum_{\chi \in G_d} \chi_0(y) = |G_d| = d$.

Si $x = 0$, on a $\sum_{\chi \in G_d} \chi(0) = \chi_0(0) = 1$. Enfin, si $x \notin \mathbb{F}_q^{*d}$ et $x \neq 0$,

on fixe $\tilde{\chi}$ un générateur de G_d. On a alors $\sum_{\chi \in G_d} \chi(x) = \sum_{j=0}^{d-1} \tilde{\chi}(x)^j = \frac{\tilde{\chi}^d(x) - 1}{\tilde{\chi}(x) - 1}$

car $\tilde{\chi}(x) \neq 1$, donc $\sum_{\chi \in G_d} \chi(x) = 0$.

On a donc $T(d,a) = \sum_{y \in \mathbb{F}_q} \psi(a y^d) = \sum_{t \in \mathbb{F}_q} \sum_{\chi \in G_d} \chi(t)\, \psi(at)$

$= \sum_{\chi \in G'_d} \overline{\chi}(a)\, G(\chi)$

Démonstration du théorème: Soit d un diviseur de $q-1$. On fixe $a_1, \dots, a_m \in \mathbb{F}_p$,

et on pose $F : (\mathbb{F}_q)^m \longrightarrow \mathbb{F}_q$ $\quad x = (x_1, \dots, x_m) \longmapsto a_1 x_1^d + \dots + a_m x_m^d$. On a :

$$qN = \sum_{a\in\mathbb{F}_q}\sum_{x\in(\mathbb{F}_q)^m}\psi(aF(x)) = q^m + \sum_{a\in\mathbb{F}_q^*}\sum_{x\in(\mathbb{F}_q)^m}\psi(aF(x))$$

$$= q^m + \sum_{a\in\mathbb{F}_q^*}\sum_{x\in(\mathbb{F}_q)^m}\exp\left(\frac{2i\pi}{p}\sum_{j=1}^{m} a_j \operatorname{Tr}_{\mathbb{F}_p}^{\mathbb{F}_q}(a x_j^d)\right)$$

$$= q^m + \sum_{a\in\mathbb{F}_q^*}\sum_{x_1,\dots,x_m\in\mathbb{F}_q}\prod_{j=1}^{m}\underbrace{\exp\left(\frac{2i\pi}{p}\,a a_j x_j^d\right)}_{=\psi(aa_j x_j^d)}$$

$$= q^m + \sum_{a\in\mathbb{F}_q^*}\prod_{j=1}^{m}\sum_{y\in\mathbb{F}_q}\psi(aa_j y^d)$$

$$= q^m + \sum_{a\in\mathbb{F}_q^*}\prod_{j=1}^{m} T(d, aa_j)$$

donc, par lemme 2 :

$$qN = q^m + \sum_{a\in\mathbb{F}_q^*}\prod_{j=1}^{m}\sum_{\chi\in G_d'}\overline{\chi}(aa_j)\,G(\chi)$$

$$= q^m + \sum_{a\in\mathbb{F}_q^*}\sum_{\chi_1,\dots,\chi_m\in G_d'}\prod_{j=1}^{m}\overline{\chi_j}(aa_j)\,G(\chi_j)$$

$$= q^m + (q-1)\sum_{(\chi_1,\dots,\chi_m)\in S_d}\prod_{j=1}^{m}\overline{\chi_j}(a_j)\,G(\chi_j)$$

car $\displaystyle\sum_{a\in\mathbb{F}_q^*}\overline{\chi_1}(a)\cdots\overline{\chi_m}(a) = \begin{cases} q-1 & \text{si } \overline{\chi_1}\cdots\overline{\chi_m} = \chi_0 \ (\text{i.e } \chi_1\cdots\chi_m = \chi_0) \\ 0 & \text{sinon} \end{cases}$

Ceci achève la preuve du théorème.

Cas $d = 2$: Ici, on prend $p \geq 3$. On a bien $d = 2 \mid q-1$.

On sait que $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$ d'indice 2. Soit $\varepsilon \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$.

On a $\mathbb{F}_q^* = \mathbb{F}_q^{*2} \cup \varepsilon \mathbb{F}_q^{*2}$. Soit $\chi : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ un caractère tel que $\chi^2 = \chi_0$.

Pour tout $x \in \mathbb{F}_q^{*2}$, on a $\chi(x) = 1$. Le caractère χ est donc entièrement déterminé par $\chi(\varepsilon)$, qui vérifie $\chi(\varepsilon)^2 = 1$, ce qui donne $\chi(\varepsilon) \in \{\pm 1\}$.

On a donc $G_2 = \{\chi_0, \chi\}$ (où χ désigne l'unique caractère non trivial),

d'où $S_d = \begin{cases} \emptyset & \text{si } n \text{ est impair} \\ \{(\chi, \dots, \chi)\} & \text{si } n \text{ est pair} \end{cases}$.

Le théorème donne $$N = q^{n-1} + \frac{q-1}{q} \prod_{j=1}^{n} \chi(a_j)\, G(\chi_j)$$

$$= q^{n-1} + \frac{q-1}{q}\, \chi\left(\prod_{j=1}^{n} a_j\right) G(\chi)^n$$

et $$\chi\left(\prod_{j=1}^{n} a_j\right) = \begin{cases} 1 & \text{si } \prod_{j=1}^{n} a_j \text{ est un carré non nul} \\ 0 & \text{si } \prod_{j=1}^{n} a_j = 0 \\ -1 & \text{sinon} \end{cases}.$$