Number of Solutions of Equations over Finite Fields

Baptiste Arnaudo

2022–2023

Contents

1 Introduction

In this work, we use the duality of finite abelian groups to give an estimate (and sometimes compute) the number of elements of such a group that solve a given algebraic equation.
We begin by introducing the central concepts of orthogonality of characters and the Fourier transform on a group. We then study certain algebraic equations over $\mathbb{F}_p$, before presenting another, more general method showing that if $k \in \mathbb{N}^*$, the equation $x^k + y^k = z^k$ admits at least one nontrivial solution in $\mathbb{F}_q$ for $q = p^n$ large enough.

2 Generalities on characters

Definition 1. ***Characters and the dual of a group***
Let G be a group. A ***character*** *of G is any group homomorphism $\chi : G \to (\mathbb{C}^*, \times)$. The* ***dual*** *of G, denoted $\widehat{G}$, is the set of characters of G. Equipped with pointwise multiplication, it is an abelian group.*

Definition 2. *If G is a group, we write $\mathbb{C}[G]$ for the set of functions from G to $\mathbb{C}$. It is a $\mathbb{C}$-vector space of dimension $|G|$ when G is finite.*

From now on, let G be a finite abelian group of cardinality n.

Proposition 1.

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

If moreover G is cyclic with generator x_0, then for $0 \leq j \leq n-1$,

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

and $\widehat{G} = \{\chi_j \mid 0 \leq j \leq n-1\}$.

Proof. We know that $\forall x \in G, x^n = e_G$, hence $\forall x \in G$, $\forall \chi \in \widehat{G}$, $\chi(x)^n = \chi(x^n) = \chi(e_G) = 1$.
If G is cyclic, fix a generator x_0. Then any $\chi \in \widehat{G}$ is completely determined by the image of x_0, which equals $e^{\frac{2ij\pi}{n}}$ for some $j \in [\![0; n-1]\!]$, giving the claim. $\square$

Remarks. We obtain $\widehat{G} \simeq \mathbb{Z}/n\mathbb{Z} \simeq G$. The isomorphism between G and its dual still holds when G is merely finite abelian; **we will take this for granted**. Thus $\widehat{G} \simeq G$ and $|\widehat{G}| = |G|$.

Proposition 2. *If $(\chi, \psi) \in \widehat{G}^2$, define $(\chi, \psi) = \frac{1}{|G|}\sum_{g \in G} \chi(g)\overline{\psi(g)}$. This endows $\mathbb{C}[G]$ with the structure of a Hermitian inner-product space.*

Theorem 1. *Orthogonality of characters*
$\widehat{G}$ is an orthonormal basis of $\mathbb{C}[G]$ for the inner product above.

Proof. We first show the following lemma:

Lemma 1. If $\chi \in \widehat{G}$ then

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{if } \chi = \chi_0 \text{ (the trivial character equal to 1 everywhere)} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Indeed, if $\chi = \chi_0$ the result is clear, and if $\chi \neq \chi_0$, there exists $g_0 \in G$ with $\chi(g_0) \neq 1$. Since $x \mapsto g_0 x$ is bijective, $\sum_{g \in G} \chi(x) = \sum_{g \in G} \chi(g_0 x) = \chi(g_0) \sum_{g \in G} \chi(x)$ and because $\chi(g_0) \neq 1$, we get $\sum_{g \in G} \chi(x) = 0$.
Therefore, if $(\chi, \psi) \in \widehat{G}^2$, then $\chi\overline{\psi} \in \widehat{G}$ and orthogonality follows immediately by applying the lemma to $\chi\overline{\psi}$.
Since $\dim(\mathbb{C}[G]) = |G| = |\widehat{G}|$, $\widehat{G}$ is indeed an orthonormal basis of $\mathbb{C}[G]$. $\square$

Corollary .1. Applying the lemma to $\hat{x} : \chi \mapsto \chi(x)$, an element of $\widehat{\widehat{G}}$, we obtain for $x \in G$:

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

This observation will be important later on.

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

This leads to the definition of the Fourier transform of an element f of $\mathbb{C}[G]$.

Definition 3. *Fourier transform*
*The **Fourier transform** is the linear map*

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

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

Proposition 3. ***Inverse transform***
We have:

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

3 Some properties of Gauss sums

We now focus on a finite field $\mathbb{F}_q$ where q is a prime power. There are two group structures, $(\mathbb{F}_q, +)$ and $(\mathbb{F}_q^*, \times)$, hence two kinds of characters: additive characters, elements of $\widehat{(\mathbb{F}_q, +)}$, and multiplicative characters, elements of $\widehat{(\mathbb{F}_q^*, \times)}$. We will denote multiplicative characters by χ and additive characters by ψ.

Definition 4. ***Gauss sums***

If $\chi \in \widehat{(\mathbb{F}_q^*, \times)}$ and $\psi \in \widehat{(\mathbb{F}_q, +)}$, the ***Gauss sum*** *associated with χ and ψ is*

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

From now on, we extend every **nontrivial** multiplicative character χ to a character $\tilde{\chi}$ defined on $\mathbb{F}_q$ (and still write it χ) by setting $\tilde{\chi}(0) = 0$. This allows us to view $G(\chi, \psi)$ as $\mathcal{F}(\tilde{\chi})(\psi)$ (where $\mathcal{F}$ is the Fourier transform on $\mathbb{C}[\mathbb{F}_q]$) and to state:

Proposition 4. *For all $\chi \in \widehat{\mathbb{F}_q}$,*

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

Proof. Apply Proposition 3 to χ to get $\chi = \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} \hat{\chi}(\psi)\psi^{-1}$ with
$\hat{\chi}(\psi) = \sum_{g \in G} \chi(g)\psi(g) = G(\chi, \psi)$. The result follows directly after the change of variables $\psi \mapsto \psi^{-1} = \overline{\psi}$ in the sum. $\square$

Theorem 2. ***Magnitude of Gauss sums***

If $\chi \in \widehat{\mathbb{F}_q^*}$ and $\psi \in \widehat{\mathbb{F}_q}$ are both ***nontrivial****, then $|G(\chi, \psi)| = \sqrt{q}$.*

Proof.

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

where we changed variables via $u = xy^{-1}$. Next,

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

where we again changed variables $u = y(x-1)$ to reach the last equality. We then used $\sum_{x \in \mathbb{F}_q} \psi(x) = 0$ by Lemma 1. $\square$

We now work over $\mathbb{F}_p$ with p an odd prime. Since $\mathbb{F}_p$ is cyclic, by Proposition 1 the elements of $\widehat{\mathbb{F}_p}$ are

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

(By a slight abuse, we identify a class in $\mathbb{F}_p$ with a representative.) We prove one last lemma:

Lemma 2. For all $x \in \mathbb{F}_p^*$, $j \in [\![0; p-1]\!]$, and $\chi \in \mathbb{F}_p^*$, we have $G(\chi, \psi_j) = \chi(x)G(\chi, \psi_{jx})$.

Proof. $G(\chi, \psi_j) = \sum_{y \in \mathbb{F}_p} \chi(y) e^{\frac{2ijy\pi}{p}} = \sum_{y \in \mathbb{F}_p} \chi(xy) e^{\frac{2ijxy\pi}{p}} = \chi(x)G(\chi, \psi_{jx})$ by the change of variables $u = xy$ (note $x \neq 0$). □

4 Number of solutions of polynomial equations in $\mathbb{F}_p$

Fix $n \in \mathbb{N}^*$ and $F \in \mathbb{F}_p[X_1, ..., X_n]$. We wish to study

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

By Corollary 1.1, $x \mapsto \frac{1}{p} \sum_{\psi \in \widehat{\mathbb{F}_p}} \psi(x)$ is the indicator of $\{0\}$, hence

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

Fix θ a generator of $\mathbb{F}_p^*$. For $x \in \mathbb{F}_p^*$ and $r \in \mathbb{N}^*$, write $\nu(x) = |\{y \in \mathbb{F}_p^* \mid y^r = x\}|$. Then:

Theorem 3. *Let $x = \theta^k$, $0 \leq k \leq p-2$. Write $\delta = r \wedge (p-1)$. Then*

$$\nu(x) = \begin{cases} \delta & \text{if } \delta \mid k \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

Proof. Let $y = \theta^{k'} \in \mathbb{F}_p^*$. If $y^r = x$ then $k \equiv rk' \pmod{p-1}$ so $\delta \mid k$. Thus if $\delta \nmid k$, $\nu(x) = 0$. Moreover,

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

since $\frac{r}{\delta}$ is invertible modulo $\frac{p-1}{\delta}$ (as $\frac{r}{\delta} \wedge \frac{p-1}{\delta} = 1$). Thus k' is fully determined modulo $\frac{p-1}{\delta}$. If $\theta^{k'_0}$ is one particular solution, the others are $\theta^{k'}$ with $k' = k'_0 + s\frac{p-1}{\delta}$: there are exactly δ distinct k' modulo $p-1$, as claimed. □

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

Proposition 5. *With δ as above and $\Gamma_\delta = \{\chi \in \widehat{\mathbb{F}_p^*} \mid \chi \neq \chi_0,\ \chi^\delta = \chi_0\}$, we have*

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

Proof. Essentially a computation. □

We now state one of the main theorems:

Theorem 4. *Let $n \geq 3$, $(a_1, ..., a_n) \in (\mathbb{F}_p^{*n})$, $(r_1, ..., r_n) \in (\mathbb{N}^*)^n$, and set $F(X_1, ..., X_n) = \sum_{k=1}^n a_k X_k^{r_k}$ and $\delta_k = r_k \wedge (p-1)$. Then*

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

Proof. By the remark at the start of the section,

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

Let $\zeta = e^{\frac{2i\pi}{p}}$. Then

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

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

by Proposition 5. □

Consider the case $r_1 = \cdots = r_n = 2$. We will show in the appendix that there is a unique multiplicative character of order 2 over $\mathbb{F}_p$, called the **Legendre symbol**, denoted $\left(\frac{\cdot}{p}\right)$, defined for $a \in \mathbb{F}_p$ by:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a nonzero square in } \mathbb{F}_p \\ -1 & \text{otherwise} \end{cases} \tag{4}$$

Since $r_1 = \cdots = r_n = 2$, for all $i \in [\![1;n]\!]$, $\delta_i = 2$ so $\Gamma_{\delta_i} = \{\left(\frac{\cdot}{p}\right)\}$. We can then compute $N(F,p)$ explicitly!

Lemma 3. *If $a, b \in \mathbb{F}_p^*$, then $G\left(\left(\frac{\cdot}{p}\right), \psi_a\right) G\left(\left(\frac{\cdot}{p}\right), \psi_b\right) = p\left(\frac{-ab}{p}\right)$.*

Proof. By Lemma 2, $G\left(\left(\frac{\cdot}{p}\right),\psi_a\right) = \left(\frac{a}{p}\right)G\left(\left(\frac{\cdot}{p}\right),\psi_1\right)$ and $G\left(\left(\frac{\cdot}{p}\right),\psi_b\right) = \left(\frac{-b}{p}\right)G\left(\left(\frac{\cdot}{p}\right),\psi_{-1}\right)$. Since $\left(\frac{\cdot}{p}\right)$ is real-valued, $G\left(\left(\frac{\cdot}{p}\right),\psi_{-1}\right) = G\left(\overline{\left(\frac{\cdot}{p}\right)},\psi_{-1}\right) = \overline{G\left(\left(\frac{\cdot}{p}\right),\psi_1\right)}$, hence

$$G\left(\left(\frac{\cdot}{p}\right),\psi_a\right)G\left(\left(\frac{\cdot}{p}\right),\psi_b\right) = \left(\frac{-ab}{p}\right)\left|G\left(\left(\frac{\cdot}{p}\right),\psi_1\right)\right|^2 = p\left(\frac{-ab}{p}\right)$$

by Theorem 2. □

We deduce:

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

$$N(F,p) = \begin{cases} p^{n-1} & \text{if } n \text{ is odd} \\ p^{n-1} + \left(\frac{(-1)^{\frac{n}{2}}a_1\cdots a_n}{p}\right)(p-1)p^{\frac{n}{2}-1} & \text{if } n \text{ is even} \end{cases} \tag{5}$$

Proof. If n is odd, Lemma 3 gives for all $j \in [\![1;p-1]\!]$,

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

since $n-1$ is even and $\left(\frac{j^{n-1}}{p}\right) = 1$. Hence

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

Computing the right-hand sum shows it is zero, so $N(F,p) = p^{n-1}$.
If n is even, then

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

so $N(F,p) = p^{n-1} + \left(\frac{(-1)^{\frac{n}{2}} a_1 \cdots a_n}{p}\right)(p-1)p^{\frac{n}{2}-1}$. $\square$

In the more general case where $r_1, ..., r_n$ are arbitrary, we do not know whether there is a more explicit expression for $N(F,p)$. Nevertheless, the results established so far provide an estimate, along with an error bound. Precisely:

Theorem 5. *There exists a constant $C(F)$ depending only on F such that*

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

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

Proof. By Theorem 4,

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

by Theorem 2. But

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

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

5 More general methods; application to Fermat–Wiles over $\mathbb{F}_{p^n}$

Some methods used earlier only work over $\mathbb{F}_p$ (we will clarify this later): here we present general methods for studying equations over a finite abelian group G, which we then apply to the equation $x^k + y^k = z^k$ over $\mathbb{F}_{p^n}$.

5.1 Framework and general results

Let G be a finite abelian group **written additively**, $k \in \mathbb{N}^*$, $A_1, ..., A_k \subset G$, and $a \in G$. We study the equation $x_1 + \cdots + x_k = a$ with $\forall i \in [\![1;k]\!]$, $x_i \in A_i$. Let N be the number of solutions. Since $x \mapsto x - a$ is bijective, we do not change N by replacing one of the sets A_i with $A_i - a$; hence we may assume $a = 0$. By the remark at the start of Section 4, we have:

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

The rightmost sum rewrites as

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

where f_A denotes the characteristic function of $A \subset G$. Therefore

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

Let R (for "remainder") denote the right-hand term. Our goal is to control its size. To this end, for $A \subset G$ define $\Phi(A) = \max\{|\hat{f}_A(\chi)| : \chi \in \widehat{G},\ \chi \neq \chi_0\}$. To study the Fermat equation over $\mathbb{F}_{p^n}$, we now restrict to $k = 3$. First a lemma:

Lemma 4. If $f \in \mathbb{C}[G]$, then $\|\hat{f}\| = \sqrt{|G|}\,\|f\|$. Since it is clear that if $A \subset G$, $\|f_A\| = \sqrt{\frac{|A|}{|G|}}$, it follows that $\|\hat{f}_A\|^2 = |A|$.

Proof. Immediate from Definition 3. □

Now the theorem:

Theorem 6. *If $A_1, A_2, A_3 \subset G$ and $\dfrac{\Phi(A_3)}{|A_3|} < \dfrac{\sqrt{|A_1||A_2|}}{|G|}$, then the equation $x_1 + x_2 + x_3 = a$, $a \in G$, with $\forall i \in \{1,2,3\}$, $x_i \in A_i$, has at least one solution.*

Proof. We need to show $|R| < \dfrac{|A_1||A_2||A_3|}{|G|}$. We have

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

by Cauchy–Schwarz.
On the right we recognize $\sqrt{|G|^2\|\hat{f}_{A_1}\|^2\|\hat{f}_{A_2}\|^2} = |G|\sqrt{|A_1||A_2|}$ by Lemma 4, hence

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

□

5.2 Application to the Fermat equation over $\mathbb{F}_q$

For the moment, A_1 and A_2 are arbitrary. Fix $k \in \mathbb{N}^*$ and set $A_3 = H_k = \{x^k : x \in \mathbb{F}_q^*\}$. Noting $H_k = H_{k \wedge (q-1)}$, we may assume $k \mid q-1$. Let N be the number of solutions to $x + y = z^k$ with $x \in A_1$, $y \in A_2$, $z \in \mathbb{F}_q^*$, and let N' be the number of solutions to $x + y = u$ with $u \in H_k$.

Lemma 5. We have $N = kN'$.

Proof. Since $\mathbb{F}_q^*$ is cyclic, the proof of Theorem 3 applies and shows there are k k-th roots of unity in $\mathbb{F}_q^*$, whence the result. □

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

Proof. Extend canonically the elements of $\widehat{\mathbb{F}_q^*/H_k}$ to elements of $\widehat{\mathbb{F}_q^*}$ by composing with $x \mapsto xH_k$. Denote them $\chi_0, \ldots, \chi_{k-1}$ (since $\left|\widehat{\mathbb{F}_q^*/H_k}\right| = \left|\mathbb{F}_q^*/H_k\right| = k$). For any nontrivial additive character ψ,

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

By Lemma 1, the inner sum equals k if $x \in H_k$ and 0 otherwise, so

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

Hence for all $\psi \in \widehat{\mathbb{F}_q}$, $\psi \neq \psi_0$,

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

□

Theorem 7. *Let* $l_1 = \dfrac{q-1}{|A_1|}$ *(and similarly for* l_2*). If* $q \geq k^2 l_1 l_2 + 4$*, then the equation* $x + y = z^k$ *with* $x \in A_1$*,* $y \in A_2$*,* $z \in \mathbb{F}_q^*$ *has at least one solution.*

Proof. We know that

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

by Proposition 7, hence

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

Now

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

One checks by a simple calculus argument that for $q > 1$, $\dfrac{(q-4)q}{(q-1)^2} \leq \dfrac{(q-1)^2}{q^2}$, hence

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

Therefore $N > 0$. □

Finally, take $A_1 = A_2 = H_k$, so $l_1 = l_2 = k$, and we deduce:

Theorem 8. *If* $k \in \mathbb{N}^*$ *and* $q \geq k^4 + 4$*, the equation* $x^k + y^k = z^k$ *has at least one nontrivial solution over* $\mathbb{F}_q$*.*

6 Comments

In my investigations, I tried to apply the methods of Section 4 to the Fermat equation, but encountered the following issue: I did not *a priori* know the additive characters of $\mathbb{F}_q$ when q is not prime, since $\mathbb{F}_q$ is not cyclic (so Proposition 1 does not apply). Looking deeper, I found that one can indeed describe the additive characters of $\mathbb{F}_{p^n}$ using the trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, the $\mathbb{F}_p$-linear map defined by

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

Define the canonical additive character ψ_1 by

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

and then for every $\psi \in \widehat{\mathbb{F}_{p^n}}$ there exists $a \in \mathbb{F}_{p^n}$ such that for all $x \in \mathbb{F}_{p^n}$, $\psi(x) = \psi_1(ax)$.
Knowing this, one can prove results entirely analogous to those at the end of Section 4 in the more general case of $\mathbb{F}_{p^n}$.

7 Appendix

Proof of existence and uniqueness of the multiplicative character of order 2 of $\mathbb{F}_p$: Since $\mathbb{F}_p^*$ is cyclic and $\mathbb{F}_p^* \simeq \widehat{\mathbb{F}_p^*}$, the latter is cyclic as well; let χ be a generator.
If $\lambda = \chi^k$ is of order 2, then $p-1 \mid 2k$ because χ has order $p-1$. Thus there exists $k' \in \mathbb{N}$ with $k = \frac{p-1}{2}k'$, and since $0 < k < p-1$, $k' = 1$ so $\lambda = \chi^{\frac{p-1}{2}}$, proving existence and uniqueness.

Showing that $\left(\frac{\cdot}{p}\right)$ is indeed the multiplicative character of order 2 of $\mathbb{F}_p$: we prove the formula, valid when p is odd (as assumed):

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

If $x = y^2 \in \mathbb{F}_p^*$, then $x^{\frac{p-1}{2}} = 1$. Since p is odd, $x \mapsto x^2$ is a homomorphism with kernel $\{-1, 1\}$ of cardinality 2, hence there are $\frac{p-1}{2}$ quadratic residues, which are precisely the roots of $X^{\frac{p-1}{2}} - 1$. This polynomial cannot have more than $\frac{p-1}{2}$ roots, so its roots are exactly the quadratic residues; we deduce $x^{\frac{p-1}{2}} = 1$ iff x is a quadratic residue.
Thus, if $x^{\frac{p-1}{2}} = -1$, then x is not a quadratic residue, and conversely if x is not a quadratic residue, then $\left(x^{\frac{p-1}{2}}\right)^2 = 1$ so $x^{\frac{p-1}{2}} \in \{-1, 1\}$, hence $x^{\frac{p-1}{2}} = -1$, which completes the proof.
It follows immediately that $\left(\frac{\cdot}{p}\right)$ is a homomorphism, and that it is the multiplicative character of order 2 of $\mathbb{F}_p$.

8 References

[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**. The discrete algebra of the Fourier transform

[4] **Jean-Marie Arnaudiès**. Problems for preparing the mathematics *agrégation*, 1. Algebra, groups, arithmetic

[5] **Théo Untrau**. Duality of finite abelian groups and counting points.
https://perso.eleves.ens-rennes.fr/people/theo.untrau/dualitecomptage.pdf