Analyse harmonique et dernier théorème de Fermat

TOUILEB Bashir

2023-2024

Introduction

Théorème (Fermat-Wiles)

Il n'existe pas d'entiers strictement positifs x,y et z tels que $x^k + y^k = z^k$ dés que $k \geq 3$

Quand est-il des corps finis ?

Introduction

Théorème (Fermat-Wiles)

Il n'existe pas d'entiers strictement positifs x,y et z tels que $x^k + y^k = z^k$ dés que $k \geq 3$

Quand est-il des corps finis ?

Théorème 0 (Babai)

Il existe $x, y, z \in \mathbb{F}_q^\times$ tel que $x^k + y^k = z^k$ dés que $q \geq k^4 + 4$

Plan

1. Analyse harmonique
2. Nombre de solutions
3. Intermède
4. Corps finis

Analyse harmonique

On note G un groupe abélien fini de cardinal n.

Définition

$\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ est appelé le groupe dual de G.

Remarques

- $\widehat{G} = \mathrm{Hom}(G, \mathbb{U})$
- $\widehat{\prod_{i=1}^{r} G_i} \simeq \prod_{i=1}^{r} \widehat{G_i}$ où $G_1, ..., G_n$ abéliens finis
- $r \geq 1$, $\overline{a} \longmapsto (\chi_a : \overline{b} \longmapsto e^{\frac{2i\pi}{r}ab})$ induit $\mathbb{Z}_r \simeq \widehat{\mathbb{Z}_r}$

Donc par théorème de structure des groupes abéliens finis (admis),

Théorème 1

G est isomorphe à $\widehat{G}$

Analyse harmonique

Définition (algèbre de groupe)

- $L(G) = \mathbb{C}^G$.
- $(L(G), +, \times, \cdot)$ est une $\mathbb{C}$-algèbre de dimension n.
- $\langle f, g \rangle = \frac{1}{n} \sum_{a \in G} f(a)\overline{g(a)}$ est un produit scalaire sur $L(G)$.

Théorème 2

Les éléments de $\widehat{G}$ forment une base orthonormée de $L(G)$.

Démonstration 2

Soit $\chi \in \widehat{G}$ tq $\chi \neq 1$. Donc $\exists b \in G$ tq $\chi(b) \neq 1$.
Or $S(\chi) = \sum_{a \in G} \chi(a) = \sum_{\theta \in G} \chi(b\theta) = \chi(b)S(\chi)$ donc $S = 0$.
Pour $\chi, \psi \in \widehat{G}$,

$$\langle \chi, \psi \rangle = \frac{1}{n} S(\chi\overline{\psi}) = \frac{1}{n} S(\chi\psi^{-1}) = \delta_{\chi,\psi}$$

Et $|\widehat{G}| = |G| = n = \dim L(G)$ donc c'est une BON.

Analyse harmonique

Définition (transformée de Fourier)

À $f \in L(G)$ on associe $\widehat{f} \in L(\widehat{G})$ tel que $\widehat{f}(\chi) = n\langle f, \overline{\chi}\rangle = \sum_{a\in G} f(a)\chi(a)$.

Théorèmes (formule de Plancherel et inversion de Fourier)

Soit $f, g \in L(G)$

- $\langle \widehat{f}, \widehat{g}\rangle = n\langle f, g\rangle$
- $f = \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\overline{\chi}$

Remarque

En notant δ l'indicatrice de $\{0\}$ il suit que

$$\widehat{\delta} = 1$$

$$\delta = \frac{1}{n}\sum_{\chi\in\widehat{G}} \chi$$

Nombre de solutions

Théorème 3

Soit $A_1, ..., A_m \subset G$ d'indicatrices $(1_{A_i})_{1 \leq i \leq m}$.
Le nombre $\mathfrak{N}$ de solutions de l'équation $x_1 + ... + x_m = 0$ $(x_i \in A_i,\ 1 \leq i \leq m)$ est

$$\mathfrak{N} = \frac{|A_1|...|A_m|}{n} + \frac{1}{n} \sum_{\chi \in \widehat{G} \setminus \{1\}} \prod_{i=1}^{m} \widehat{1}_{A_i}(\chi)$$

Démonstration 3

$\mathfrak{N} = \sum_{x_1 \in A_1, \ldots, x_m \in A_m} \delta(x_1 + ... + x_m) = \sum_{x_1 \in A_1, \ldots, x_m \in A_m} \frac{1}{n} \sum_{\chi \in \widehat{G}} \chi(x_1 + ... + x_m) =$
$\frac{1}{n} \sum_{\chi \in \widehat{G}} \left(\sum_{x_1 \in A_1} \chi(x_1) \right) ... \left(\sum_{x_m \in A_m} \chi(x_m) \right) =$
$\frac{1}{n} \sum_{\chi \in \widehat{G}} \left(\sum_{x_1 \in G} 1_{A_1}(x_1)\chi(x_1) \right) ... \left(\sum_{x_m \in G} 1_{A_m}(x_m)\chi(x_m) \right) =$
$\frac{1}{n} \sum_{\chi \in \widehat{G}} \prod_{i=1}^{m} \widehat{1}_{A_i}(\chi)$

Nombre de solutions

Soit $A \subset G$

Définition

On définit $\phi(A) = \max_{\chi \in \widehat{G} \setminus 1} \left\{ |\widehat{1}_A(\chi)| \right\}$

Nombre de solutions

Théorème 4

Lorsque $m = 3$ on a,

$$\Delta = \left| \mathfrak{N} - \frac{|A_1||A_2||A_3|}{n} \right| < \phi(A_3)\sqrt{|A_1||A_2|}$$

Démonstration 4

Par le théorème 3 et l'inégalité triangulaire,

$$\Delta \leq \frac{1}{n} \sum_{\chi \in \widehat{G} \setminus \{1\}} |\widehat{1}_{A_1}(\chi)||\widehat{1}_{A_2}(\chi)||\widehat{1}_{A_3}(\chi)| \leq \frac{\phi(A_3)}{n} \sum_{\chi \in \widehat{G}} |\widehat{1}_{A_1}(\chi)||\widehat{1}_{A_2}(\chi)|$$

Par inégalité de Cauchy-Schwartz,

$$\Delta \leq \frac{\phi(A_3)}{n} \sqrt{\sum_{\chi \in \widehat{G}} |\widehat{1}_{A_1}(\chi)|^2} \sqrt{\sum_{\chi \in \widehat{G}} |\widehat{1}_{A_2}(\chi)|^2} = \frac{\phi(A_3)}{n} \parallel \widehat{1}_{A_1} \parallel \cdot \parallel \widehat{1}_{A_2} \parallel$$

Par la formule de Parseval, $\Delta \leq \phi(A_3) \parallel 1_{A_1} \parallel \cdot \parallel 1_{A_2} \parallel = \phi(A_3)\sqrt{|A_1||A_2|}$

Nombre de solutions

Bilan !

On souhaite majorer $\phi(A_3)$ dans $G = \mathbb{F}_q$ lorsque $A_1 = A_2 = A_3 = H(q,k)$ où

$$H(q,k) = \left\{ a^k, a \in \mathbb{F}_q^\times \right\}$$

afin d'obtenir $\mathfrak{N} > 0$

Intermède

Définitions

- $\mathfrak{N}(q,k) = \mathfrak{N}$ dans $\mathbb{F}_q$ pour $k \geq 3$ donné
- $\mathfrak{S}(q,k) = \left|\left\{(x,y,z) \in \mathbb{F}_q^{\times}, x^k + y^k = z^k\right\}/\sim\right|$
- $\mathfrak{D}(q,k) = \frac{2\mathfrak{S}(q,k)}{q(q-1)^2}$

Remarque

- $\mathfrak{N}(q,k) = \left|\left\{(x,y,z) \in H(q,k), x+y=z\right\}\right|$
- En général $\mathfrak{N}(q,k) \neq \mathfrak{S}(q,k)$
- Mais $\mathfrak{N}(q,k) > 0$ si et seulement si $\mathfrak{S}(q,k) > 0$

Intermède

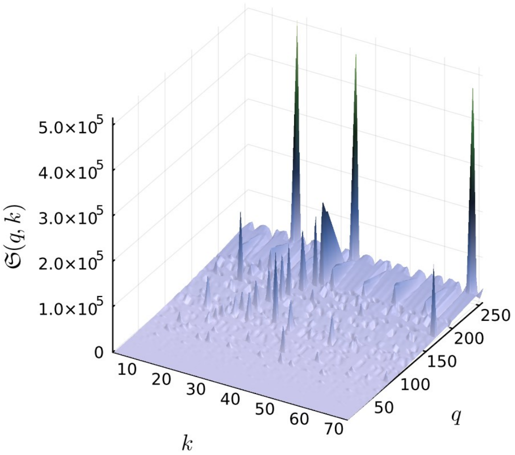


Figure: Nombre $\mathfrak{S}(q,k)$ de solutions non triviales de $x^k + y^k = z^k$ dans $\mathbb{F}_q$.

Intermède

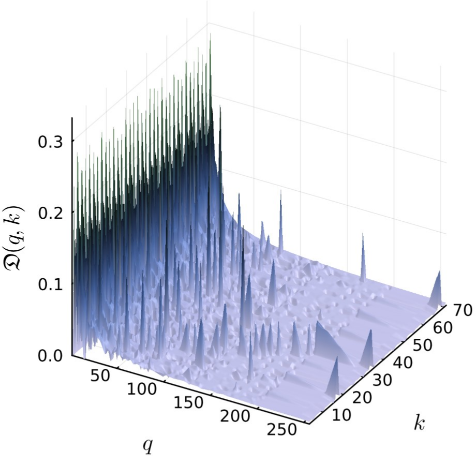


Figure: Densité $\mathfrak{D}(q,k)$ en solutions non triviales de $x^k + y^k = z^k$ dans $\mathbb{F}_q$.

Intermède

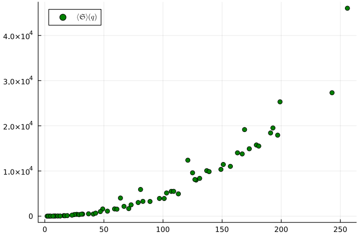


Figure: Nombre moyen $\langle\mathfrak{S}\rangle(q)$ de solutions

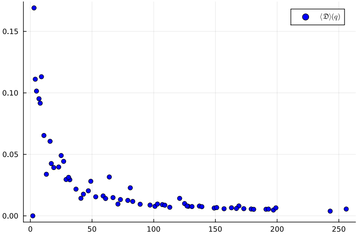


Figure: Densité moyenne $\langle\mathfrak{D}\rangle(q)$ en solutions

Corps finis

Définition (somme de Gauss)

Soit $\chi \in \widehat{\mathbb{F}_q}$, $\psi \in \widehat{\mathbb{F}_q^\times}$, on définit

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

en posant $\psi(0) = 0$

Remarques

- $G(\chi_0, \psi_0) = q - 1$, où χ_0, ψ_0 sont triviaux
- $G(\chi_0, \psi) = 0$ si $\psi \neq \psi_0$
- $G(\chi, \psi_0) = -1$ si $\chi \neq \chi_0$

Corps finis

Théorème 5

Si $\chi \neq \chi_0$ et $\psi \neq \psi_0$ alors,

$$|G(\chi, \psi)| = \sqrt{q}$$

Corps finis

Démonstrations 5

On calcul,
$|G(\chi,\psi)|^2 = G(\chi,\psi)\overline{G(\chi,\psi)} = \sum_{a\in\mathbb{F}_q^\times}\chi(a)\psi(a)\sum_{b\in\mathbb{F}_q^\times}\overline{\chi(b)\psi(b)} =$
$\sum_{a,b\in\mathbb{F}_q^\times}\chi(a-b)\psi(ab^{-1}) = \sum_{a,c\in\mathbb{F}_q^\times}\chi(a(1-c))\psi(c)$
donc,

$$|G(\chi,\psi)|^2 = \sum_{c\in\mathbb{F}_q^\times}\psi(c)\Bigg(\sum_{a\in\mathbb{F}_q}\chi(a(1-c)) - \chi(0)\Bigg)$$

or $\sum_{a\in\mathbb{F}_q}\chi(a) = 0$ et $\sum_{a\in\mathbb{F}_q^\times}\psi(a) = 0$,
donc,

$$|G(\chi,\psi)|^2 = \psi(1)(q-1) - \sum_{c\in\mathbb{F}_q^\times\setminus\{1\}}\psi(c) = (q-1) - 0 + 1 = q$$

d'où $|G(\chi,\psi)| = \sqrt{q}$

Corps finis

On suppose dorénavant que $k|q-1$

Remarque (exercice 6.4)

$$|H(q,k)| = \frac{q-1}{k}$$

Résolution

$\Lambda : a \in \mathbb{F}_q^\times \longmapsto a^k \in \mathbb{F}_q^\times$ est un morphisme donc $|\Lambda(\mathbb{F}_q^\times)| = |H(q,k)| = \frac{|\mathbb{F}_q^\times|}{|\ker\Lambda|}$.
soit $P = X^k - 1 \in \mathbb{F}_q[X]$, $P' = kX^{k-1} \neq 0$ donc P est à racines simples.
soit $\alpha \in \overline{\mathbb{F}_q}$ tel que $P(\alpha) = 0$.
or $\alpha^k = 1$ et $\exists n \in \mathbb{N} : q = nk + 1$ donc $\alpha^q = \alpha$ donc $\alpha \in \mathbb{F}_q$.
donc $|\ker\Lambda| = \deg P = k$ donc $|H(q,k)| = \frac{q-1}{k}$.

Corps finis

Soit $H = H(q,k)$

Théorème 6

Soit $\psi \in \widehat{\mathbb{F}_q^\times/H}$, on définit

$$\widetilde{\psi} : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times/H \longrightarrow \mathbb{C}^*$$

$$a \longmapsto \psi(\bar{a})$$

Alors pour $\chi \in \widehat{\mathbb{F}_q}$,

$$\widehat{1_H}(\chi) = \frac{1}{k} \sum_{\psi \in \widehat{\mathbb{F}_q^\times/H}} G(\chi, \widetilde{\psi})$$

Démonstration 6

On observe $\frac{1}{k} \sum_{\psi \in \widehat{\mathbb{F}_q^\times/H}} G(\chi, \widetilde{\psi}) = \frac{1}{k} \sum_{a \in \mathbb{F}_q^\times} \chi(a) \sum_{\psi \in \widehat{\mathbb{F}_q^\times/H}} \widetilde{\psi}(a) = \frac{1}{k} =$
$\frac{1}{k} \sum_{a \in \mathbb{F}_q^\times} \chi(a) \sum_{\psi \in \widehat{\mathbb{F}_q^\times/H}} \psi(\bar{a}) = \sum_{a \in \mathbb{F}_q^\times} \chi(a) \delta_{\bar{1},\bar{a}} k = \sum_{a \in H} \chi(a) = \widehat{1_H}(\chi)$

Corps finis

Conséquence + bilan

Or $\phi(H) = \max_{\chi \in \widehat{\mathbb{F}}_q \setminus \{1\}} |\widehat{1}_H(\chi)|$

Donc par inégalité triangulaire on en déduit $\phi(H) \leq \sqrt{q}$.

On a réussi à majorer ϕ !

Corps finis

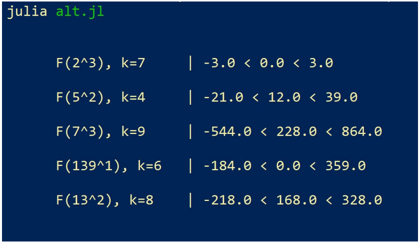
Théorème 7

Supposons que $k|q-1$, alors

$$\left|\mathfrak{N}(q,k)-\frac{(q-1)^3}{qk^3}\right|<\sqrt{q}\frac{q-1}{k}$$

Démonstration 7

Suit du théorème 4 avec $A_1=A_2=A_3=H(q,k)$ et $\phi(H(q,k))\leq\sqrt{q}$



```
julia alt.jl


      F(2^3), k=7     | -3.0 < 0.0 < 3.0

      F(5^2), k=4     | -21.0 < 12.0 < 39.0

      F(7^3), k=9     | -544.0 < 228.0 < 864.0

      F(139^1), k=6   | -184.0 < 0.0 < 359.0

      F(13^2), k=8    | -218.0 < 168.0 < 328.0
```

Figure: Exemple d'encadrements dans $\mathbb{F}_8$, $\mathbb{F}_{25}$, $\mathbb{F}_{343}$, $\mathbb{F}_{139}$ et $\mathbb{F}_{169}$

Corps finis

Démonstration 0 quand $k|q-1$

Supposons que $q \geq k^4+4$,

$$\frac{1}{q}(\frac{q-1}{k})^3 \geq \sqrt{q}\frac{q-1}{k} \longleftrightarrow \frac{(q-1)^4}{q^3} \geq k^4 \longleftrightarrow q(1-\frac{1}{q})^4 \geq k^4$$

Or $(1-\frac{1}{q})^4 \geq 1-\frac{4}{q}$ donc $q(1-\frac{1}{q})^4 \geq q-4 \geq k^4$ donc $\mathfrak{N}(q,k) > 0$

Soit $k \geq 3$

Remarque

Il suit du théorème de Bezout que

$$H(q,k) = H(q, \text{pgcd}(q-1,k))$$

ce qui permet de se ramener au cas précedent.

Le théorème 0 est donc démontré !

```julia
using Nemo
using Base
using Plots
using Statistics
using LaTeXStrings

# objet corps finis
struct Field
    p::Int64
    r::Int64
    q::Int64
    a::FqFieldElem
    F::Vector{FqFieldElem}
    F_z::Vector{FqFieldElem}
    Chr
    function Field(p,r,gen_chr)
        function to_int(x)
            return Int(lift(ZZ,x))
        end
        function primitive_e(p)
            GF, _ = finite_field(p,1,"a")
            a = GF(2)
            L = [GF(i) for i in 2:(p-1)]
            while L != []
                a = L[1]
                c = [a^i for i in 1:(p-1)]
                deleteat!(L,findall(x -> x in c, L))
            end
            return a
        end
        GF, a = finite_field(p,r,"a")
        q = p^r
        if r == 1
            a = primitive_e(p)
        end
        F = [a^k for k in 0:(q-2)]
        if gen_chr
            F_z = vcat([GF(0)],[a^k for k in 0:(q-2)])
            Chr = [x -> exp(2*pi*im*to_int(absolute_tr(b*x))/p) for b in F_z]
            return new(p,r,q,a,F,F_z,Chr)
        else
            return new(p,r,q,a,F)
        end
    end
end

# indicatrice
function ind(A)
    x -> Int64(x in A)
end

# transformée de Fourier
function FT(Fld,f)
    return c -> sum([c(b)*f(b) for b in Fld.F_z])
end

# calcul de H(q,k)
function H(Fld,k)
    H = []
    for i in 1:(Fld.q)
        h = Fld.F[mod(i*k,Fld.q-1) + 1]
        if !(h in H)
            push!(H, h)
        end
    end
    return H
end

# calcul de N(q,k) et de son encadrement (théorème 7.1)
function N_bounds(Fld,k)
    A = H(Fld,k)
    L = length(A)
    f = FT(Fld,ind(A))
    N = real(1/Fld.q * sum(map(x -> f(x)^3,Fld.Chr)))
    # e, m = k*L*sqrt(Fld.q), (Fld.q - 1)*L*L/Fld.q

    m,e = (Fld.q - 1)^3 / (Fld.q * k^3), sqrt(Fld.q)*(Fld.q-1)/k

    return m-e, N, m+e
end

# calcul de S(q,k) par bruteforce exploitant la cyclicité de F*
function S_btf_cyc(Fld,k)
    S = 0
    t = 0
    q = Fld.q
    for i in 0:q-2, j in i:q-2, l in 0:q-2
        x,y,z = Fld.F[mod(i*k,q-1)+1], Fld.F[mod(j*k,q-1)+1], Fld.F[mod(l*k,q-1)+1]
        if x+y==z
            S += 1
        end
    end
    return S
end

# calcul et enregistremenet de S(q,k) pour 1 < q < 257 et 2 < k < 72
function generate(file,prime)
    s = 0
    f = open(file,"w")
    for p in prime, r in 1:8
        q = p^r
        if q <= 256 && q > 0
            Fld = Field(p,r,false)
            for k in 3:71
                S = S_btf_cyc(Fld,k)
                r = "("*string(k)*","*string(q)*","*string(S)*");"
                write(f,r)
                print("[+] "*r*"\n")
            end
        end
    end
    close(f)
end

# extraction des données enregistrées
function extract(file)
    f = open(file)
    raw = readline(f)
    close(f)

    raw2 = split(raw,";")
    l = length(raw2) - 1

    data_s = [map(x -> parse(Float64,x),split(strip(raw2[i], ['(',')']),',')) for i in 1:l]
    data_d = map(l -> [l[1],l[2], 2*l[3]/(l[2]*(l[2]-1)^2)], data_s)

    return data_s, data_d
end

# graphique de <S>(q) et <D>(q)
function SD_mean(file)
    data_s,data_d = extract(file)

    qs = union([l[2] for l in data_s])

    data_sks = [filter(l -> l[2]==q, data_d) for q in qs]
    data_dks = [filter(l -> l[2]==q, data_d) for q in qs]

    mean_prop = [mean(map(l -> l[3], item)) for item in data_dks]
    mean_sol = [mean(map(l -> l[3], item)) for item in data_sks]

    p = plot(qs,mean_prop, seriestype=:scatter, label=L"\langle\mathfrak{D}\rangle(q)", mc=:blue)
    # p = plot(qs, mean_sol, seriestype=:scatter, label=L"\langle\mathfrak{S}\rangle(q)", mc=:red)
    display(p)
    readline()
end

# affichage 3D de S(q,k) et D(q,k)
```

```
function SD_3d(file)
    data_s, data_d = extract(file)

    k = map(l -> l[1], data)
    q = map(l -> l[2], data)
    S = map(l -> l[3], data_s)
    # D = map(l -> l[3], data_d)

    p = surface(k,q,S, xlabel=L"k", ylabel=L"q",zlabel=L"\mathfrak{S}(q,k)",c=cgrad(:tofino100))
    display(p)
    readline()
end
```