Existência de elementos primitivos 2-normais em Corpos Finitos

Josimar R. Aguirre, Victor Newmann

Universidade Federal de Uberlândia

21 de Agosto de 2020

$\mathbb{F}_{q^n}$

$\langle \mathbb{F}_{q^n}^*, \cdot \rangle$ grupo multiplicativo.

|

$\mathbb{F}_{q^n}$ espaço vetorial de dimensão n sobre $\mathbb{F}_q$.

$\mathbb{F}_q$

$\mathbb{F}_{q^n}$

$\langle \mathbb{F}_{q^n}^*, \cdot \rangle$ grupo multiplicativo.

$\mathbb{F}_{q^n}$ espaço vetorial de dimensão n sobre $\mathbb{F}_q$.

$\mathbb{F}_q$

Definição 1.1

Um elemento $\alpha \in \mathbb{F}_{q^n}$ é chamado **primitivo** *se $\langle \alpha \rangle = \mathbb{F}_{q^n}^*$.*

$\mathbb{F}_{q^n}$ — $\langle \mathbb{F}_{q^n}^*, \cdot \rangle$ grupo multiplicativo.

$|$ — $\mathbb{F}_{q^n}$ espaço vetorial de dimensão n sobre $\mathbb{F}_q$.

$\mathbb{F}_q$

Definição 1.1

Um elemento $\alpha \in \mathbb{F}_{q^n}$ é chamado **primitivo** *se $\langle \alpha \rangle = \mathbb{F}_{q^n}^*$.*

Definição 1.2

Um elemento $\alpha \in \mathbb{F}_{q^n}$ é chamado **normal** *se $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ como espaço vetorial sobre $\mathbb{F}_q$.*

Teorema 1.3 (Teorema da Base normal primitiva-1987)

Para todo entero positivo n e qualquer corpo finito $\mathbb{F}_q$, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ que é primitivo e normal sobre $\mathbb{F}_q$.

Teorema 1.3 (Teorema da Base normal primitiva-1987)

Para todo entero positivo n e qualquer corpo finito $\mathbb{F}_q$, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ que é primitivo e normal sobre $\mathbb{F}_q$.

1. Lenstra e Schoof (1987).
2. Cohen e **Huczynska** (2003).

Teorema 1.3 (Teorema da Base normal primitiva-1987)

Para todo entero positivo n e qualquer corpo finito $\mathbb{F}_q$, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ que é primitivo e normal sobre $\mathbb{F}_q$.

1. Lenstra e Schoof (1987).
2. Cohen e **Huczynska** (2003).

Como generalizar?

Seja $d(\alpha) = \dim \mathcal{B}$, onde $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$

$$\alpha \text{ é normal } \Leftrightarrow \ d(\alpha) = n$$

Seja $d(\alpha) = \dim \mathcal{B}$, onde $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$

$$\alpha \text{ é normal } \Leftrightarrow \ d(\alpha) = n$$

Definição 1.4 (Huczynska, Mullen, Panario, Thompson (2013))

Seja $\alpha \in \mathbb{F}_{q^n}$. Dizemos que α é um elemento k-normal *de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se $d(\alpha) = n - k$*

Seja $d(\alpha) = \dim \mathcal{B}$, onde $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$

$$\alpha \text{ é normal } \Leftrightarrow \ d(\alpha) = n$$

Definição 1.4 (Huczynska, Mullen, Panario, Thompson (2013))

Seja $\alpha \in \mathbb{F}_{q^n}$. Dizemos que α é um elemento k-normal *de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se $d(\alpha) = n - k$*

$$\text{normal} \Leftrightarrow 0\text{-normal}$$

Observação 1.5

0 é o único elemento n-normal.

Observação 1.5

0 é o único elemento n-normal.

Existem elementos k-normais primitivos?

$$k = 0 \quad \surd \text{ (TBNP)}$$

Observação 1.5

0 é o único elemento n-normal.

Existem elementos k-normais primitivos?

$$k = 0 \quad \surd \text{ (TBNP)}$$

$$k = 1 \quad \surd \text{ Lucas Reis - David Thomson (2018)}$$

Observação 1.5

0 é o único elemento n-normal.

Existem elementos k-normais primitivos?

$k = 0 \quad \surd$ (TBNP)

$k = 1 \quad \surd$ Lucas Reis - David Thomson (2018)

$k = 2 \quad \surd$ Victor Newmann - J.R. (2020)

Observação 1.5

0 é o único elemento n-normal.

Existem elementos k-normais primitivos?

$$k = 0 \quad \surd \text{ (TBNP)}$$

$$k = 1 \quad \surd \text{ Lucas Reis - David Thomson (2018)}$$

$$k = 2 \quad \surd \text{ Victor Newmann - J.R. (2020)}$$

$$k > 2 \quad ?$$

Como estudar os k-normais?

Linearized Polynomials

$$f(x) = \sum_{i=0}^{r} a_i x^i \;\Leftrightarrow\; q\text{-associado sobre } \mathbb{F}_{q^n} \;\Leftrightarrow\; L_f(x) = \sum_{i=0}^{r} a_i x^{q^i}$$

Linearized Polynomials

$$f(x) = \sum_{i=0}^{r} a_i x^i \;\Leftrightarrow\; q\text{-associado sobre } \mathbb{F}_{q^n} \;\Leftrightarrow\; L_f(x) = \sum_{i=0}^{r} a_i x^{q^i}$$

$$\mathcal{I}_\alpha = \{f \in \mathbb{F}_q[x] \mid L_f(\alpha) = 0\} = \langle m_{\alpha,q}(x) \rangle.$$

Linearized Polynomials

$$f(x) = \sum_{i=0}^{r} a_i x^i \;\Leftrightarrow\; q\text{-associado sobre } \mathbb{F}_{q^n} \;\Leftrightarrow\; L_f(x) = \sum_{i=0}^{r} a_i x^{q^i}$$

$$\mathcal{I}_\alpha = \{f \in \mathbb{F}_q[x] \mid L_f(\alpha) = 0\} = \langle m_{\alpha,q}(x)\rangle.$$

Definição 2.1

O polinômio mônico $m_{\alpha,q}(x) \in \mathbb{F}_q[x]$ é conhecido como o $\mathbb{F}_q$-ordem de α.

Teorema 2.2

α *é k-normal* $\Leftrightarrow$ $m_{\alpha,q}(x)$ *tem grau* $n-k$.

Teorema 2.2

α é k-normal $\Leftrightarrow$ $m_{\alpha,q}(x)$ tem grau $n-k$.

α é normal $\Leftrightarrow$ O $\mathbb{F}_q$-ordem de α é $x^n - 1$.

Teorema 2.2

α é k-normal $\Leftrightarrow$ $m_{\alpha,q}(x)$ tem grau $n-k$.

α é normal $\Leftrightarrow$ O $\mathbb{F}_q$-ordem de α é $x^n - 1$.

primitivo?

Teorema 2.3

O número dos elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é dado por

$$\sum_{\substack{h|x^n-1 \\ \deg(h)=n-k}} \Phi_q(h),$$

onde os divisores são mônicos e a divisão é sobre $\mathbb{F}_q$.

Teorema 2.3

O número dos elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é dado por

$$\sum_{\substack{h|x^n-1 \\ \deg(h)=n-k}} \Phi_q(h),$$

onde os divisores são mônicos e a divisão é sobre $\mathbb{F}_q$.

Corolário 2.4

Elementos k-normais existem (não necessariamente primitivo) se, e somente se $x^n - 1$ admite um divisor de grau k sobre $\mathbb{F}_q$.

Freeness

Definição 2.5

(a) *Seja* $m|(q^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}^*$ *é m-livre se* $\alpha = \beta^d$, *para algum divisor* d *de* m *implica* $d = 1$.

Freeness

Definição 2.5

(a) *Seja* $m|(q^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}^*$ *é m-livre se* $\alpha = \beta^d$, *para algum divisor* d *de* m *implica* $d = 1$.

(b) *Seja* $M|(x^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}$ *é M-livre se* $\alpha = L_h(\beta)$ *para algum divisor* h *de* M *implica* $h = 1$.

Freeness

Definição 2.5

(a) *Seja* $m|(q^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}^*$ *é m-livre se* $\alpha = \beta^d$, *para algum divisor* d *de* m *implica* $d = 1$.

(b) *Seja* $M|(x^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}$ *é M-livre se* $\alpha = L_h(\beta)$ *para algum divisor* h *de* M *implica* $h = 1$.

α é primitivo $\Leftrightarrow$ α é (q^n-1)-livre.

Freeness

Definição 2.5

(a) *Seja* $m|(q^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}^*$ *é m-livre se* $\alpha = \beta^d$, *para algum divisor* d *de* m *implica* $d = 1$.

(b) *Seja* $M|(x^n-1)$, *dizemos que* $\alpha \in \mathbb{F}_{q^n}$ *é M-livre se* $\alpha = L_h(\beta)$ *para algum divisor* h *de* M *implica* $h = 1$.

α é primitivo $\Leftrightarrow$ α é (q^n-1)-livre.

α é normal $\Leftrightarrow$ α é (x^n-1)-livre.

Proposição 2.6 ($k = 1$)

Suponha que $x^n - 1$ *não possui factor repetido* $x - \varsigma$, $\varsigma \in \mathbb{F}_q$. *Logo*

$$\mathbb{F}_q\text{-}ord(\alpha) = \frac{x^n - 1}{x - \varsigma} \Leftrightarrow \alpha \text{ é } \left(\frac{x^n - 1}{x - \varsigma}\right) - free.$$

Proposição 2.6 ($k = 1$)

Suponha que $x^n - 1$ *não possui factor repetido* $x - \varsigma$, $\varsigma \in \mathbb{F}_q$. *Logo*

$$\mathbb{F}_q\text{-}ord(\alpha) = \frac{x^n - 1}{x - \varsigma} \Leftrightarrow \alpha \text{ é } \left(\frac{x^n - 1}{x - \varsigma}\right) - free.$$

Seja

$$W(t) = \begin{cases} \#\text{ divisores livres de quadrados de t, se } t \in \mathbb{Z}. \\ \#\text{ divisores mônicos livres de quadrados de t, se } t \in \mathbb{F}_q[x]. \end{cases}$$

Considere $p \dagger n$. Seja N o número de elementos primitivos, $\frac{x^n-1}{x-1}$-livre.

Considere $p \dagger n$. Seja N o número de elementos primitivos, $\frac{x^n-1}{x-1}$-livre.

$$N = \sum_{w \in \mathbb{F}_{q^n}} \omega_t(w) \cdot \Omega_T(w),$$

onde, $t = q^n - 1$, $T = \frac{x^n-1}{x-1}$ e

$$\begin{cases} \omega_t(w) \text{ função caraterística t-livre, } t \mid q^n - 1. \\ \Omega_T(w) \text{ função caraterística T-livre, } T \mid x^n - 1. \end{cases}$$

Considere $p \dagger n$. Seja N o número de elementos primitivos, $\frac{x^n-1}{x-1}$-livre.

$$N = \sum_{w \in \mathbb{F}_{q^n}} \omega_t(w) \cdot \Omega_T(w),$$

onde, $t = q^n - 1$, $T = \frac{x^n-1}{x-1}$ e

$$\begin{cases} \omega_t(w) \text{ função caraterística t-livre, } t \mid q^n - 1. \\ \Omega_T(w) \text{ função caraterística T-livre, } T \mid x^n - 1. \end{cases}$$

Precisamos $N > 0$

Considere $p \dagger n$. Seja N o número de elementos primitivos, $\frac{x^n-1}{x-1}$-livre.

$$N = \sum_{w \in \mathbb{F}_{q^n}} \omega_t(w) \cdot \Omega_T(w),$$

onde, $t = q^n - 1$, $T = \frac{x^n-1}{x-1}$ e

$$\begin{cases} \omega_t(w) \text{ função caraterística t-livre, } t \mid q^n - 1. \\ \Omega_T(w) \text{ função caraterística T-livre, } T \mid x^n - 1. \end{cases}$$

Precisamos $N > 0 \leftarrow$ Somas de Gauss

Teorema 2.7

Suponha que $\gcd(q, n) = 1$. *Se*

$$q^{n/2-1} > W(q^n - 1)W\left(\frac{x^n - 1}{x - 1}\right),$$

então existe elemento primitivo 1*-normal em* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$.

Teorema 2.7

Suponha que $\gcd(q, n) = 1$. *Se*

$$q^{n/2-1} > W(q^n - 1)W\left(\frac{x^n - 1}{x - 1}\right),$$

então existe elemento primitivo 1*-normal em* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$.

Teorema 2.8 (Teorema do elemento primitivo 1-normal-2018)

Seja q *uma potência de um primo e* $n \geq 3$ *um inteiro positivo. Existe um elemento primitivo* 1*-normal de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$. *Além disso, quando* $n = 2$ *não existe elemento primitivo* 1*-normal de* $\mathbb{F}_{q^2}$ *sobre* $\mathbb{F}_q$.

Caso geral

Como gerar elementos k-normais?

Proposição 3.1

Seja $\beta \in \mathbb{F}_{q^n}$ um elemento normal, $f \in \mathbb{F}_q[x]$ divisor de $x^n - 1$ de grau k. Então $L_f(\beta)$ é k-normal

Caso geral

Como gerar elementos k-normais?

Proposição 3.1

Seja $\beta \in \mathbb{F}_{q^n}$ um elemento normal, $f \in \mathbb{F}_q[x]$ divisor de $x^n - 1$ de grau k. Então $L_f(\beta)$ é k-normal

$$\sum_{w \in \mathbb{F}_{q^n}} \Omega(w) \cdot \omega(L_f(w)).$$

w normal; $L_f(w)$ primitivo

Contabiliza: $w \in \mathbb{F}_{q^n}$ tal que $L_f(w)$ é primitivo e k-normal.

Teorema 3.2

Se $x^n - 1$ *possui um divisor de grau* k *e*

$$q^{\frac{n}{2}-k} \geq W(q^n - 1)W(x^n - 1)$$

então existe pelo menos um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.

Teorema 3.2

Se $x^n - 1$ possui um divisor de grau k e

$$q^{\frac{n}{2}-k} \geq W(q^n - 1)W(x^n - 1)$$

então existe pelo menos um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.

$$k \leq n \cdot \underbrace{\left(\frac{1}{2} - \frac{0.96}{\log n + \log\log q} - \log_q 2\right)}_{h(n,q)}$$

Teorema 3.2

Se $x^n - 1$ possui um divisor de grau k e

$$q^{\frac{n}{2}-k} \geq W(q^n - 1)W(x^n - 1)$$

então existe pelo menos um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.

$$k \leq n \cdot \underbrace{\left(\frac{1}{2} - \frac{0.96}{\log n + \log\log q} - \log_q 2\right)}_{h(n,q)}$$

$$\lim_{q\to\infty} H(n,q) = \frac{1}{2} \Rightarrow q \gg 1,\ k \in [0, \frac{n}{2}) \quad \surd$$

Elementos primitivos 2-normais

Proposição 4.1

Seja $I_n(r)$ o número de fatores mônicos irredutíveis de $x^n - 1$ de grau r sobre $\mathbb{F}_q$. Temos

$$I_n(r) = \frac{1}{r} \sum_{d|r} t_d \cdot \mu\left(\frac{r}{d}\right),$$

onde $t_d = \gcd(q^d - 1, n)$.

Proposição 4.1

Seja $I_n(r)$ o número de fatores mônicos irredutíveis de $x^n - 1$ de grau r sobre $\mathbb{F}_q$. Temos

$$I_n(r) = \frac{1}{r} \sum_{d|r} t_d \cdot \mu\left(\frac{r}{d}\right),$$

onde $t_d = \gcd(q^d - 1, n)$.

Corolário 4.2

Existe elemento 2-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se $\gcd(q^3 - q, n) \neq 1$.

Proposição 4.1

Seja $I_n(r)$ o número de fatores mônicos irredutíveis de $x^n - 1$ de grau r sobre $\mathbb{F}_q$. Temos

$$I_n(r) = \frac{1}{r} \sum_{d|r} t_d \cdot \mu\left(\frac{r}{d}\right),$$

onde $t_d = \gcd(q^d - 1, n)$.

Corolário 4.2

Existe elemento 2-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se $\gcd(q^3 - q, n) \neq 1$.

Algum deles é primitivo?

Lembrando...

Teorema 4.3

Se $x^n - 1$ *possui um divisor de grau* k *e*

$$q^{\frac{n}{2}-k} \geq W(q^n - 1)W(x^n - 1)$$

então existe pelo menos um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.

Lembrando...

Teorema 4.3

Se $x^n - 1$ possui um divisor de grau k e

$$q^{\frac{n}{2}-k} \geq W(q^n - 1)W(x^n - 1)$$

então existe pelo menos um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.

Teorema 4.4

Sejam $f, T \in \mathbb{F}_q[x]$ divisores de $x^n - 1$ tal que $\deg f = k$ e $\gcd\left(\frac{x^n-1}{f}, T\right) \neq 1$ e seja $m \in \mathbb{N}$ divisor de $q^n - 1$. Se

$$q^{n/2-k} \geq W(m)W(T)$$

logo existe $\alpha \in \mathbb{F}_{q^n}$ T-livre tal que $L_f(\alpha)$ é m-livre.

Proposição 4.5

Sejam $f, T \in \mathbb{F}_q[x]$ *divisores* $x^n - 1$ *tal que* $\deg f = k$ *e* $\gcd\left(\frac{x^n-1}{f}, T\right) \neq 1$ *e seja* $m \in \mathbb{N}$ *divisor de* $q^n - 1$. *Sejam* $Q_1, \ldots, Q_s$ *polinômios irredutíveis e* $p_1, \ldots, p_r$ *números primos tal que* $rad(x^n - 1) = rad(T) \cdot Q_1 \cdot Q_2 \cdots Q_s$ *e* $rad(q^n - 1) = rad(m) \cdot p_1 \cdot p_2 \cdots p_r$. *Suponha que* $\delta = 1 - \sum_{i=1}^{r} \frac{1}{p_i} - \sum_{j=1}^{s} \frac{1}{q^{\deg Q_j}} > 0$ *e seja* $\Delta = \frac{r+s-1}{\delta} + 2$. *Se*

$$q^{\frac{n}{2}-k} \geq W(m)W(T)\Delta,$$

então existe pelo menos um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.

Proposição 4.6

Suponha $n \geq 5$ *e* $q \geq (n-1)^2$. *Se* $x^n - 1$ *tem um fator de grau* $k \geq 2$ *em* $\mathbb{F}_q[x]$ *e* $q^{\frac{n}{2}-k} \geq 2(n+1)W(q^n-1)$, *logo existe um elemento primitivo k-normal em* $\mathbb{F}_{q^n}$.

Proposição 4.6

Suponha $n \geq 5$ *e* $q \geq (n-1)^2$. *Se* $x^n - 1$ *tem um fator de grau* $k \geq 2$ *em* $\mathbb{F}_q[x]$ *e* $q^{\frac{n}{2}-k} \geq 2(n+1)W(q^n-1)$, *logo existe um elemento primitivo k-normal em* $\mathbb{F}_{q^n}$.

Proposição 4.7

Seja $n \geq 8$ *um número natural. Existe elemento primitivo 2-normal em* $\mathbb{F}_{q^n}$ *para toda potência de primo* q *satisfazendo* $\gcd(q^3 - q, n) \neq 1$.

Condições

$$q^{\frac{n}{2}-k} \geq W(q^n-1)W(x^n-1) \qquad q^{\frac{n}{2}-k} \geq W(m)W(T)\Delta$$

Condições

$$q^{\frac{n}{2}-k} \geq W(q^n-1)W(x^n-1) \qquad q^{\frac{n}{2}-k} \geq W(m)W(T)\Delta$$

Conseguir "boas" cotas a função W !!!

Condições

$$q^{\frac{n}{2}-k} \geq W(q^n-1)W(x^n-1) \qquad q^{\frac{n}{2}-k} \geq W(m)W(T)\Delta$$

Conseguir "boas" cotas a função W !!!

$$n = 7, 6, 5 \quad \surd$$

Condições

$$q^{\frac{n}{2}-k} \geq W(q^n-1)W(x^n-1) \qquad q^{\frac{n}{2}-k} \geq W(m)W(T)\Delta$$

Conseguir "boas" cotas a função W !!!

$$n = 7, 6, 5 \quad \surd$$

Se $k = 2$ e $n = 4$...

Condições

$$q^{\frac{n}{2}-k} \geq W(q^n-1)W(x^n-1) \qquad q^{\frac{n}{2}-k} \geq W(m)W(T)\Delta$$

Conseguir "boas" cotas a função W !!!

$$n = 7, 6, 5 \quad \surd$$

Se $k = 2$ e $n = 4$... Precisamos outra condição!

Caso $n = 4$

$$q \equiv 1 \pmod 4$$

Caso $n = 4$

$$q \equiv 1 \pmod 4$$

Proposição 4.8

Sejam $u, v \in \mathbb{F}_q^*$ *e* $f(x) = (x+1)(x+b) \in \mathbb{F}_q[x]$ *onde* $b \in \mathbb{F}_q$ *satisfaz* $b^2 = -1$. *Se* $\gamma = uL_f(\alpha) + v$ *é primitivo em* $\mathbb{F}_{q^4}$ *logo* γ *é 2-normal em* $\mathbb{F}_{q^4}$.

Caso $n = 4$

$$q \equiv 1 \pmod 4$$

Proposição 4.8

Sejam $u, v \in \mathbb{F}_q^*$ *e* $f(x) = (x+1)(x+b) \in \mathbb{F}_q[x]$ *onde* $b \in \mathbb{F}_q$ *satisfaz* $b^2 = -1$. *Se* $\gamma = uL_f(\alpha) + v$ *é primitivo em* $\mathbb{F}_{q^4}$ *logo* γ *é 2-normal em* $\mathbb{F}_{q^4}$.

$$q^{\frac{1}{2}} > 3W(q^4 - 1), \quad q^{\frac{1}{2}} > 3W(m)\Delta$$

Caso $n = 4$

$$q \equiv 1 \pmod 4$$

Proposição 4.8

Sejam $u, v \in \mathbb{F}_q^*$ *e* $f(x) = (x+1)(x+b) \in \mathbb{F}_q[x]$ *onde* $b \in \mathbb{F}_q$ *satisfaz* $b^2 = -1$. *Se* $\gamma = uL_f(\alpha) + v$ *é primitivo em* $\mathbb{F}_{q^4}$ *logo* γ *é 2-normal em* $\mathbb{F}_{q^4}$.

$$q^{\frac{1}{2}} > 3W(q^4 - 1), \quad q^{\frac{1}{2}} > 3W(m)\Delta \Rightarrow \textit{Existe } \gamma \textit{ primitivo}$$

Teorema 4.9 (Teorema do elemento primitivo 2-normal-2020)

Seja q a potência de um primo e n um número natural. Existe elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ se, e somente se $n \geq 5$ e $\gcd(q^3 - q, n) \neq 1$ ou $n = 4$ e $q \equiv 1 \pmod 4$.

AGORA???

Problemas abertos

1. Encontrar uma "boa" fórmula para contar os elementos k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para valores particulares de (q, n, k).

Problemas abertos

1. Encontrar uma "boa" fórmula para contar os elementos k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para valores particulares de (q, n, k).
2. Determine a existência de elementos $\alpha \in \mathbb{F}_{q^n}$ k-normais "de ordem alto". Onde ordem alto significa $\mathbb{F}_q\text{-ord}(\alpha) = N$, onde N é um divisor de $x^n - 1$ de grau "alto".

Problemas abertos

1. Encontrar uma "boa" fórmula para contar os elementos k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para valores particulares de (q, n, k).
2. Determine a existência de elementos $\alpha \in \mathbb{F}_{q^n}$ k-normais "de ordem alto". Onde ordem alto significa $\mathbb{F}_q\text{-ord}(\alpha) = N$, onde N é um divisor de $x^n - 1$ de grau "alto".
3. Determine os pares (n, k) tal que existe elementos primitivos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Problemas abertos

1. Encontrar uma "boa" fórmula para contar os elementos k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para valores particulares de (q, n, k).
2. Determine a existência de elementos $\alpha \in \mathbb{F}_{q^n}$ k-normais "de ordem alto". Onde ordem alto significa $\mathbb{F}_q$-ord$(\alpha) = N$, onde N é um divisor de $x^n - 1$ de grau "alto".
3. Determine os pares (n, k) tal que existe elementos primitivos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

4. Encontrar fórmula para contar os elementos primitivos k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Bibliografia

- S. Huczynska, G.L. Mullen, D. Panario and D. Thomson, *Existence and properties of k-normal elements over finite fields*, Finite Fields Appl. 24 (2013), 170–183
- L. Reis: *Existence results on k-normal elements over finite fields*, Rev. Mat. Iberoam. 35(3) (2019), 805–822
- L. Reis, D. Thompson, *Existence of primitive* 1*-normal elements in finite fields*, Finite Fields and Their Applications 51 (2018) 238-269.
- Newmann V., Aguirre J. *Existence of primitive* 2*-normal elements in finite fields*, arXiv:2007.11169 (2020).

Gracias!