Existência de pares de elementos primitivos sobre corpos finitos

João Paulo Guardieiro Sousa & Guilherme Chaud Tizziotti
Universidade Federal de Uberlândia
joaopaulosousa20@gmail.com

Resumo

No estudo de corpos finitos, alguns elementos desempenham um papel fundamental na determinação dessas estruturas. Entre eles, estão os elementos primitivos: os geradores do grupo multiplicativo associado ao corpo. Determinado um tal elemento, podemos obter todos os outros facilmente tomando potências adequadas. Mas às vezes pode ser útil relacioná-los a partir de polinômios, [3] nos traz um estudo aprofundado nesse tema, e é nesse artigo que baseamos o trabalho.

Introdução

Em um corpo finito $\mathbb{F}_q$ com $q = p^k$ elementos, dizemos que $\alpha \in \mathbb{F}_q$ é *primitivo* se α for um gerador do grupo multiplicativo $\mathbb{F}_q^*$, isto é, se a ordem multiplicativa de α for $q-1$. Seja $N_{2\times 3}(\mathbb{F}_q) := \{A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q) : a, d \neq 0, \text{posto}(A) = 2\}$. Dada $A \in N_{2\times 3}(\mathbb{F}_q)$, defina $f_A(x) = \frac{ax^2+bx+c}{dx^2+ex+f}$.

Dizemos que (α, β) é um *par* primitivo em $\mathbb{F}_q$ se α e β forem elementos primitivos de $\mathbb{F}_q$ e definimos $\mathcal{M} = \{q : \mathbb{F}_q$ contém um par primitivo $(\alpha, f_A(\alpha))$ para todo $A \in N_{2\times 3}(\mathbb{F}_q)\}$ (nessa definição, o par primitivo pode variar para cada matriz A).

Ao final desse trabalho, teremos provado o seguinte.

Teorema 1. $2^k \in \mathcal{M}$ *para todo* k *natural, com exceção de* $k \in \{1, 2, 3, 4, 6, 8, 9, 10, 12\}$.

Os casos $k = 1, 2, 3, 4$ possuem contra-exemplos, os demais casos foram inconclusivos a partir dos resultados desse trabalho.

Resultados

Dizemos que um elemento $\alpha \in \mathbb{F}_q^*$ é *s-livre* para algum divisor s de $q-1$ se, para qualquer $d|s$, toda vez que pudermos escrever $\alpha = \beta^d$, com $\beta \in \mathbb{F}_q$, isso implicar $d = 1$, em outras palavras, α não pode ser uma d-ésima potência de algum elemento com $d \neq 1$ se $d|s$. Note que α é primitivo se, e somente se, α for $q-1$ livre.

Usaremos $q = 2^k$ e l_1 e l_2 denotarão divisores positivos de $q-1$. Queremos encontrar valores k para os quais $q \in \mathcal{M}$, isto é, tais que $\mathbb{F}_q$ contém um par primitivo $(\alpha, f_A(\alpha))$ para todo $A \in N_{2\times 3}(\mathbb{F}_q)$. Para isso, seja $N_A(l_1, l_2)$ o número de pares $(\alpha, f_A(\alpha))$ tais que α é l_1-livre e $f_A(\alpha)$ é l_2-livre. Dessa forma, para termos $q \in \mathcal{M}$, devemos ter $N_A(q-1, q-1) > 0$ para todo $A \in N_{2\times 3}(\mathbb{F}_q)$. $\omega(l)$ denotará o número de divisores primos de l e $W(l)$ denotará o número de divisores livres de quadrados de l. Não é difícil ver que $W(l) = 2^{\omega(l)}$.

Um resultado simples nos fornece alguns valores de k tais que $2^k \in \mathcal{M}$.

Proposição 1. *Se* $2^k - 1 \geq 8$ *for um primo de Mersenne, então* $2^k \in \mathcal{M}$.

Dessa forma, temos $2^k \in \mathcal{M}$ para $k = 5, 7, 13, 17, 19$, bem como todos os outros (grandes) primos de Mersenne.

Lema 1. *Seja* $A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in N_{2\times 3}(\mathbb{F}_q)$, $q \geq 4$. *Se* $q^{\frac{1}{2}} > 4W(l_1)W(l_2)$, *então* $N_A(l_1, l_2) > 0$.

O lema anterior nos deu uma condição suficiente para termos $q \in \mathcal{M}$. Entretanto, precisaríamos calcular $W(q-1)$ para cada $q = 2^k$. Mas, em [1], encontramos a seguinte cota superior para esse valor, visto que $q-1$ é um número ímpar.

Lema 2. *Se* m *for um inteiro positivo ímpar, então* $W(m) < 6.46m^{\frac{1}{5}}$.

Usando a cota dada no Lema 1, encontramos o seguinte.

Proposição 2. $q = 2^k \in \mathcal{M}$ *para* $k \geq 21$, *com exceção de* $k = 24, 28, 36$.

Precisamos, agora, decidir se $2^k \in \mathcal{M}$ para $6 \leq k \leq 20$ e $k = 24, 28, 36$. Para os valores de k restantes, usaremos o seguinte lema, adaptado de um resultado de [4].

Lema 3. *Seja* $l|q-1$ *e* $\{p_1, ..., p_r\}$ *o conjunto dos primos que dividem* $q-1$, *mas não* l. *Suponha que* $\delta = 1 - 2\sum_{i=1}^{r} \frac{1}{p_i} > 0$ *e seja* $\Delta = \frac{2r-1}{\delta} + 2$. *Se* $2^{\frac{k}{2}} > 4W(l)^2\Delta$, *então* $2^k \in \mathcal{M}$.

Proposição 3. $2^k \in \mathcal{M}$ *para* $k \in \{11, 14, 15, 16, 18, 20, 24, 28, 36\}$.

Conclusão

As Proposições 1, 2 e 3 combinadas provam o Teorema 1.

Referências

[1] Stephen D COHEN. Pairs of primitive elements in fields of even order. *Finite Fields and Their Applications*, 28:22–42, 2014.

[2] Lei FU and Daqing WAN. A class of incomplete character sums. *arXiv preprint arXiv:1303.3650*, 2013.

[3] AWASTHI Ambrish SHARMA, Rajendra K. and Anju GUPTA. Existence of pair of primitive elements over finite fields of characteristic 2. *Journal of Number Theory*, 193:386–394, 2018.

[4] R. K. et al SHARMA. Existence of some special primitive normal elements over finite fields. *Finite Fields and Their Applications*, 46:280–303, 2017.

Agradecimentos

Agradeço à CAPES e ao CNPq pela oportunidade de realizar esse estudo.