

Corpos Finitos: uma ferramenta da Álgebra Abstrata

Juan Pablo Lins

Semana Olímpica 2026 - N3 - Vitória, ES

O objetivo dessa aula é mostrar a utilidade dos corpos finitos (principalmente dos com p^2 elementos) em certos problemas de Teoria dos Números. A primeira parte da aula será dedicada a provar que corpos finitos necessariamente têm cardinalidade igual a uma potência de primo, e na segunda parte veremos como aplicar esse conceito em problemas, de modo a encurtar (às vezes bastante) soluções.

1 Cardinalidade dos corpos finitos

Primeiramente, relembremos a definição de corpo:

Definição 1. Um conjunto F munido de duas operações binárias $+$ (soma) e \cdot (produto) é dito um *corpo* se

- i) $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todos $a, b, c \in F$ (associatividade);
- ii) $a + b = b + a$ e $a \cdot b = b \cdot a$, para todos $a, b \in F$ (comutatividade);
- iii) $(a + b) \cdot c = a \cdot c + b \cdot c$ e $a \cdot (b + c) = a \cdot b + a \cdot c$, para todos $a, b, c \in F$ (distributividade da soma pelo produto);
- iv) Existem elementos distintos $0, 1 \in F$ tais que $a + 0 = a$ e $a \cdot 1 = a$, para todo $a \in F$ (elementos neutros);
- v) Para cada $a \in F$, existe um único elemento $-a \in F$, chamado *inverso aditivo de a* , tal que $a + (-a) = 0$ (existência do inverso aditivo);
- vi) Para cada $a \in F$, $a \neq 0$, existe um único elemento $a^{-1} \in F$, chamado *inverso multiplicativo de a* , tal que $a \cdot a^{-1} = 1$ (existência do inverso multiplicativo).

O exemplo mais simples de corpo finito que conhecemos é o conjunto $\mathbb{Z}/p\mathbb{Z}$ dos inteiros módulo um primo p .

Uma propriedade importante dos corpos é que eles são *domínios*, isto é, dados $a, b \in F$ tais que $ab = 0$, então $a = 0$ ou $b = 0$.

Definição 2. A *característica* de um corpo F , denotada por $\text{char } F$, é o menor natural $n \in \mathbb{N}$ tal que $n \cdot 1_F = \underbrace{1_F + \dots + 1_F}_{n \text{ vezes}} = 0_F$. Se tal n não existir, definimos $\text{char } F = 0$.

A característica de $\mathbb{Z}/p\mathbb{Z}$, por exemplo, é p .

Proposição 1. Se F é um corpo finito, então $\text{char } F > 0$. Além disso, $\text{char } F$ é um número primo.

Demonstração. Se $\text{char } F = 0$, então os elementos da forma $n \cdot 1_F$, $n \in \mathbb{N}$, são dois a dois distintos e pertencem a F , logo F é infinito. Por fim, suponha que $\text{char } F = ab$, com $a, b > 1$. Como F é um domínio, segue que

$$(ab) \cdot 1_F = 0_F \implies (a \cdot 1_F) \cdot (b \cdot 1_F) = 0_F \implies a \cdot 1_F = 0_F \text{ ou } b \cdot 1_F = 0_F,$$

contradizendo a minimalidade de ab . Assim, $\text{char } F$ deve ser um número primo. \square

Agora vamos mostrar que $\mathbb{Z}/p\mathbb{Z}$ é o “menor” corpo de característica p , ou seja, qualquer outro corpo de característica p deve conter uma cópia de $\mathbb{Z}/p\mathbb{Z}$. Para isso, vamos formalizar o que significa “conter uma cópia” com a definição de *isomorfismo*.

Definição 3. Sejam K e F corpos. Uma função bijetiva $\varphi : K \rightarrow F$ é dita um *isomorfismo* se $\varphi(a + b) = \varphi(a) + \varphi(b)$ e $\varphi(ab) = \varphi(a)\varphi(b)$ para quaisquer $a, b \in K$.

Vejam os exemplos simples de isomorfismo. Considere o conjunto $\{a, b\}$. Nesse conjunto, definiremos as operações $+$ e \cdot de modo que sejam satisfeitas as seguintes tabelas.

$+$	a	b
a	a	b
b	b	a

\cdot	a	b
a	a	a
b	a	b

Observando atentamente, vemos que o conjunto se parece bastante com $\mathbb{Z}/2\mathbb{Z}$. Se parecem e são isomorfos! Basta definir $\varphi : \{a, b\} \rightarrow \mathbb{Z}/2\mathbb{Z}$ tal que $\varphi(a) = 0$ e $\varphi(b) = 1$.

Proposição 2. Se $\text{char } F = p$, então existe uma cópia isomorfa de $\mathbb{Z}/p\mathbb{Z}$ em F .

Demonstração. Defina $F_p = \{0_F, 1_F, 2 \cdot 1_F, \dots, (p-1) \cdot 1_F\} \subset F$. É fácil ver que a função $\varphi : F_p \rightarrow \mathbb{Z}/p\mathbb{Z}$ dada por $\varphi(j \cdot 1_F) = j$, $0 \leq j \leq p-1$ é um isomorfismo. □

A partir de agora, se F é um corpo de característica p , escreveremos $\mathbb{Z}/p\mathbb{Z} \subset F$ por abuso de notação. Nosso objetivo final é mostrar que $|F| = p^n$ para algum n .

Definição 4. Seja K um corpo. Um *K -espaço vetorial* V é um conjunto, cujos elementos são chamados de *vetores*, munido de duas operações binárias

$$+ : V \times V \rightarrow V \text{ (soma)} \quad \text{e} \quad \cdot : K \times V \rightarrow V \text{ (produto por escalar)}$$

que satisfazem, informalmente:

- V é fechado para soma e para multiplicação por *escalares* de K .
- a soma é comutativa, existe o vetor nulo, existe o vetor oposto, etc.

Há axiomas precisos que definem um espaço vetorial, mas o primeiro ponto destacado acima será suficiente para nossos propósitos.

Um exemplo de espaço vetorial é o conjunto $\mathcal{P}_2(\mathbb{R}) = \{ax^2 + bx + c : a, b, c \in \mathbb{R}\}$ dos polinômios de grau ≤ 2 com coeficientes reais (ou em qualquer corpo). De fato, podemos somar quaisquer polinômios desse conjunto e obter outro polinômio dele e podemos multiplicar um polinômio por uma constante real c e obter um outro polinômio dele.

Observe que o conjunto $\{1, x, x^2\}$ cumpre um papel crucial no exemplo acima: todo elemento de $\mathcal{P}_2(\mathbb{R})$ pode ser escrito de maneira *única* como combinação linear de $1, x$ e x^2 .

Definição 5. Uma *base* para um K -espaço vetorial é um conjunto $B \subset V$ tal que todo vetor $v \in V$ pode ser escrito de maneira única como combinação linear (finita) de vetores de B com coeficientes em K , isto é,

$$v = a_1v_1 + \dots + a_nv_n, \quad a_i \in K, v_i \in B \quad \forall i.$$

É possível mostrar que todo espaço vetorial possui base utilizando o Lema de Zorn. Além disso, fixado um espaço vetorial V , pode-se provar que qualquer base de V sempre tem mesma cardinalidade, seja ela finita ou não. A **dimensão** de um espaço vetorial é a cardinalidade de uma base dele.

Uma *extensão de corpos* é simplesmente uma inclusão $K \subset F$ entre dois corpos. Dada uma extensão de corpos $K \subset F$, podemos ver F como K -espaço vetorial! De fato, F é fechado para soma e para multiplicação, em particular, é fechado para multiplicação por elementos de K . Vendo os elementos de K como escalares e os de F como vetores, segue direto da definição.

Teorema 1. *Se F é um corpo finito com $\text{char } F = p$, então existe um inteiro positivo n tal que $|F| = p^n$.*

Demonstração. Se $\text{char } F = p$, então vale a extensão de corpos $\mathbb{Z}/p\mathbb{Z} \subset F$, logo podemos ver F como $\mathbb{Z}/p\mathbb{Z}$ -espaço vetorial. Como F é finito, é óbvio que qualquer base deve ser finita, então seja $\{x_1, \dots, x_n\}$ uma base (isto é, n é a dimensão de F sobre $\mathbb{Z}/p\mathbb{Z}$). Desse modo,

$$F = \{a_1x_1 + \dots + a_nx_n : a_1, \dots, a_n \in \mathbb{Z}/p\mathbb{Z}\}.$$

Temos p escolhas para cada a_i , portanto $|F| = p^n$. □

Bom, nesse ponto é natural se perguntar: para qualquer potência de primo p^n , existe um corpo de cardinalidade p^n ? A resposta é sim, mas foge do escopo desse material.

2 Como construir corpos finitos úteis?

Para motivar essa parte, pensemos nos números complexos. O que motivou os matemáticos a criar (ou descobrir, você decide) e estudar o conjunto dos números complexos \mathbb{C} ? Queríamos resolver $x^2 + 1 = 0$, mas não existe tal número real x . Teve-se então que pensar num corpo maior que \mathbb{R} que contivesse uma raiz desse polinômio! Esse é o espírito que motivará os corpos finitos que estudaremos agora.

Considere $\mathbb{Z}/3\mathbb{Z}$. Sabemos que 2 não é resíduo quadrático módulo 3, isto é, o polinômio $x^2 - 2$ não tem raiz em $\mathbb{Z}/3\mathbb{Z}$. Assim, vamos definir o conjunto

$$\mathbb{Z}/3\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}/3\mathbb{Z}\}.$$

Aqui não devemos pensar em $\sqrt{2}$ como o número irracional $1,4142\dots$, mas simplesmente como um novo símbolo que elevado ao quadrado é 2. Munindo nosso novo conjunto com as operações de soma e produto módulo 3, é fácil provar que ele é um corpo. Mais do que isso, é um corpo com 9 elementos! Além disso, é um corpo que contém uma raiz quadrada de 2 módulo 3.

Em geral, se $\left(\frac{k}{p}\right) = -1$, isto é, k não é resíduo quadrático módulo p primo, podemos definir

$$\mathbb{Z}/p\mathbb{Z}[\sqrt{k}] = \{a + b\sqrt{k} : a, b \in \mathbb{Z}/p\mathbb{Z}\},$$

que se trata de um corpo de p^2 elementos. Observe que se $\left(\frac{k}{p}\right) = 1$, então $\mathbb{Z}/p\mathbb{Z}[\sqrt{k}] = \mathbb{Z}/p\mathbb{Z}$.

Ao trabalhar nesse corpo de p^2 elementos, é útil saber calcular ordens de elementos, mas não estamos mais em $\mathbb{Z}/p\mathbb{Z}$. Para fazer isso, utilizaremos o Teorema de Lagrange. Antes disso, um pouco de terminologia:

Definição 6. Um conjunto G munido com uma operação binária \cdot é um *grupo* se

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todos $a, b, c \in G$ (associatividade);
- existe $e \in G$ tal que $a \cdot e = e \cdot a = a$ para todo $a \in G$ (elemento neutro);
- para todo $a \in G$, existe $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$ (elemento inverso).

Observe que se F é um corpo, então $F^* = F \setminus \{0\}$ é um grupo. Definimos a *ordem* de um elemento $g \in G$ como o menor natural $d \geq 1$ tal que $g^d = e$. Se tal n não existe, dizemos que g tem ordem infinita. Denotamos a ordem de g por $\text{ord } g$. É fácil mostrar que se $g^n = e$, então $\text{ord } g \mid n$.

Para simplificar as contas, iremos supor a partir de agora que G é um grupo *abeliano* ou *comutativo*, isto é, $a \cdot b = b \cdot a \forall a, b \in G$.

Vejam agora uma generalização do Pequeno Teorema de Fermat:

Proposição 3. *Se G é um grupo finito, então $g^{|G|} = e \forall g \in G$.*

A prova é muito parecida com a do Pequeno Teorema de Fermat e fica como exercício. E note que tal resultado é de fato uma generalização do PTF, pois no caso em que $G = \mathbb{Z}/p\mathbb{Z}^*$, concluímos que $a^{p-1} \equiv 1 \pmod{p}$.

Teorema 2 (Teorema de Lagrange). *Seja G um grupo finito e $g \in G$, então $\text{ord } g$ divide $|G|$.*

A prova segue diretamente da Proposição 3.

Agora voltamos aos corpos finitos. Se $\left(\frac{a}{p}\right) = -1$, então $\mathbb{Z}/p\mathbb{Z}[\sqrt{a}]^*$ é um grupo multiplicativo com $p^2 - 1$ elementos. Assim, dado $x \neq 0$ em $\mathbb{Z}/p\mathbb{Z}[\sqrt{a}]$, temos que $\text{ord } x \mid p^2 - 1$.

Observação 1. É possível provar que existe (a menos de isomorfismo) apenas um corpo finito de p^n elementos, denotado por \mathbb{F}_{p^n} . No caso específico (e mais útil para nós) em que $n = 2$, \mathbb{F}_{p^2} contém raízes quadradas de elementos de $\mathbb{Z}/p\mathbb{Z}$. Em geral, não sabemos se um polinômio de grau 2 tem raiz em $\mathbb{Z}/p\mathbb{Z}$, mas temos certeza que tem raiz em \mathbb{F}_{p^2} .

3 Problemas

Problema 1 (China TST). A sequência (x_n) é definida por $x_1 = 2$, $x_2 = 12$ e $x_{n+2} = 6x_{n+1} - x_n$ para cada $n \geq 1$. Seja p um primo ímpar e q um divisor primo de x_p . Prove que se $q \neq 2, 3$, então $q \geq 2p - 1$.

Problema 2 (OBM 2017). Seja a um inteiro positivo e p um divisor primo de $a^3 - 3a + 1$, com $p \neq 3$. Prove que $p \equiv \pm 1 \pmod{9}$.

Problema 3 (IMOSL 2003). Seja $a_0 = 2$ e $a_{k+1} = 2a_k^2 - 1$. Prove que se um primo p divide a_n , então $2^{n+3} \mid p^2 - 1$.

Problema 4 (Teste de primalidade de Lucas-Lehmer). Defina a sequência de inteiros dada por $x_0 = 4$ e $x_{i+1} = x_i^2 - 2$. Dado $m \in \mathbb{N}$ ímpar, mostre que $n = 2^m - 1$ é primo se, e somente se, $n \mid x_{m-2}$.

Problema 5 (Vingança Olímpica de Israel 2026). Seja n um inteiro positivo. Prove que qualquer primo $p > 2$ que divide $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n$ deve ser da forma $p = 3k + 1$ para algum inteiro k .