Teoria Aritmética de Números

notas de aula – 2024.02.20.12.37

Jerônimo C. Pellegrini

id: 8ea29d6349cfd718a995dce29fd9efab77f5fe31

Sumário

Sobre este texto

Este texto é uma primeira introdução à Teoria de Números. Presume-se do leitor familiaridade com demonstrações, especialmente por indução e com o conceito de número complexo. A partir do Capítulo 15, há a necessidade de rudimentos de Álgebra Linear.

Nomenclatura

Neste texto usamos marcadores para final de definições (⧫), exemplos (◀) e demonstrações (□). Em alguns Capítulos, vetores são denotados por variáveis em negrito (por exemplo, "$\mathbf{v}$").

(a, b, c) forma quadrática binária $ax^2 + bxy + cy^2$, página 212

$[E : F]$ grau extensão E sobre F, página 272

$[x_0; x_1, x_2, \ldots, x_n]$ Fração contínua $x_0 + 1/(x_1 + 1/(x_2 + \cdots + 1/(x_n)))$, página 243

$\lceil x \rceil$ função menor inteiro $\geq x$ (teto de x), página 137

$\overline{\alpha}$ conjugado complexo de α., página 56

$\overline{\alpha}$ conjugado em corpo quadrático, página 273

Δ discriminante de forma quadrática, página 212

$\lfloor x \rfloor, [x]$ função maior inteiro $\leq x$ (chão de x), página 137

Γ grupo modular, página 226

$\mathbb{Z}$ conjunto dos números inteiros, página 19

$\mathbb{Z}/n\mathbb{Z}$ Anel dos inteiros módulo n, página 88

$\mathbb{Z}[\omega]$ inteiros quadráticos, página 276

$\mathbb{Z}_n$ Anel dos inteiros módulo n, página 88

$\lambda(\cdot)$ Norma em domínio euclideano, página 59

$\left(\frac{a}{m}\right)$ Símbolo de Jacobi, página 175

$\left(\frac{a}{p}\right)$ Símbolo de Legendre, página 175

$\lfloor x \rceil$ Inteiro mais próximo de x, página 59

$\mathrm{mdc}(a,b)$ máximo divisor comum de a e b, página 40

$\mathrm{mmc}(a,b)$ mínimo múltiplo comum de a e b, página 48

$\mu(n)$ função μ de Moebius, página 129

$\mathbb{N}$ conjunto dos números naturais, página 6

ω $\sqrt{d}$ ou $(1+\sqrt{d})/2$ (conveniência de notação para inteiros quadráticos), página 276

$\mathrm{ord}_p(n)$ ordem de p em n, página 66

ϕ razão áurea, página 50

$\phi(n)$ quantidade de co-primos com n, menores ou iguais a n, página 121

$\pi(n)$ quantidade de primos menores ou iguais a n, página 141

$\mathcal{O}_F$ anel de inteiros quadráticos, página 277

$\mathcal{O}_F$ grupo de unidades de inteiros quadráticos, página 278

Q_n resíduos quadráticos módulo n, página 173

$\mathrm{rad}\, n$ radical do número n, página 147

$\mathbb{Q}$ conjunto dos números racionais, página 19

$\mathbb{Q}[\sqrt{d}]$ corpo quadrático, página 273

$\sigma(n)$ soma dos divisores de n, página 121

$\sim$ equivalência de formas quadráticas, página 211

$\sim$ equivalência de pontos em $\mathbb{H}$, página 227

$\mathrm{Tr}(\alpha)$ traço de elemento em corpo quadrático, página 273

$\mathbb{H}$ meio-plano superior, página 227

U_n grupo de unidades módulo n, página 168

$a \equiv b \pmod{m}$ a é congruente a b módulo m, página 88

$a \mid b$ a divide b, página 37

$a \nmid b$ a não divide b, página 37

$a^{(i)}$ i-ésimo convergente de irracional aproximado por fração contínua, página 247

$c(p)$ conteúdo de um polinômio p, página 81

$d(n)$ número de divisores de n, página 121

F_n número de Fermat, página 70

$GL(n, F)$ grupo linear geral, página 226

$h(\Delta)$ número de classe do discriminante fundamental Δ, página 221

$LR_m(x)$ menor resíduo congruente a x módulo m, página 178

$M(N)$ função de Merten, página 150

M_p número de Mersenne, página 68

$N(n)$ quantidade de soluções da congruência $a^2 \equiv -1 \pmod{n}$, página 198

$N(z)$ norma do inteiro Gaussiano z, página 55

$P(n)$ quantidade de representações próprias de n com $x > 0$, página 198

$p(n)$ quantidade de partições de um inteiro, página 236

p_i/q_i i-ésimo convergente de irracional aproximado por fração contínua, página 247

$R(n)$ quantidade de representações de n, página 198

$r(n)$ quantidade de representações próprias de n, página 198

$R[[x]]$ anel das séries formais de potências na variável x, sobre o anel R, página 235

$R_{n\times n}$ matriz de Redheffer de ordem n, página 150

$s(n)$ sucessor de número natural, página 6

$SL(n, F)$ grupo linear especial, página 226

u_n n-ésimo número de Fibonacci, página 49

$w(f)$ quantidade de automorfismos da forma quadrática f, página 220

Parte I

Capítulo 1

Introdução

O objeto de estudo da Teoria dos Números é o conjunto dos números inteiros, $\ldots, -2, -1, 0, +1, +2, \ldots$, e suas propriedades[1].

Como exemplo elementar, sabemos que um número escrito na base dez é divisível por dois quando seu último dígito é par; e que é divisível por cinco quando seu último dígito é zero ou cinco. Estas duas propriedades podem ser *demonstradas* sem grande dificuldade, embora demonstrações fáceis não sejam regra.

Muito do desenvolvimento da Teoria dos Números se dá a partir de *observações*: somente após observar em experimentos que há uma grande quantidade de números primos, perfeitos, de ternos Pitagóricos, e outros objetos, Matemáticos decidiram por conjecturar suas propriedades. Assim, embora muito do texto a seguir seja devotado a enunciar e demonstrar fatos sobre números, deve-se ter em mente que muitas das Definições e Teoremas que estudamos são fruto de longo e extenso trabalho de observação. Muito desse trabalho empírico foi realizado quando não havia computadores ou calculadoras – mas com a existência destes, a dificuldade deixa de ser o poder computacional para fazer observações, e sim a intuição para decidir *o que observar*.

É muito comum que enunciados sobre números inteiros sejam de muitíssimo simples expressão, passando a ilusão de que sua demonstração é, também, simples – e o oposto acontece! O conhecido Último Teorema de Fermat, por exemplo, afirma que para n inteiro maior que dois, a equação $x^n + y^n = z^n$ não tem soluções com $x \neq 0$. Esta afirmação foi feita sem demonstração[2] por Pierre de Fermat em 1637, e permaneceu sem demons-

[1] Também de números não inteiros, quando há relação entre eles e os inteiros.

[2] Fermat mencionou em uma margem de livro que tinha uma demonstração, mas não a deu porque "não cabia" ali (*"É impossível separar um cubo em cubos, ou uma quarta potência em quartas potências, ou, em geral, uma potência maior que dois em potências similares. Eu descobri uma prova maravilhosa disso, que esta margem é demasiado pequena para comportar"*). Dada a complexidade da demonstração que temos hoje, é crença comum entre Matemáticos

tração até 1994, quando Andrew Wiles conseguiu finalmente – usando um ferramental matemático longe de ser trivial – garantir que de fato a proposição é verdadeira.

que a demonstração de Fermat tivesse alguma falha sutil.

Capítulo 2

Números

Para se demonstrar o que quer que seja, precisamos partir de pressupostos anteriores. Tomando um exemplo qualquer dentro da Matemática: quando nosso foco de atenção é o Cálculo, demonstramos que a regra da cadeia para derivação é válida – mas aquela demonstração presume como certo que as operações que usamos ao demonstrar são bem definidas e que suas propriedades valem. É interessante lançar o olhar sobre estas operações e questionar *o que estamos presumindo*. Levando este raciocínio adiante, chegamos ao estudo de conjuntos de números e operações sobre eles, a que damos o nome de "estruturas algébricas". Um passo mais e podemos questionar se há alguma forma de definir rigorosamente o que chamamos de "números naturais" (e inteiros, racionais, e reais). É evidente que em algum momento teremos de parar e nos contentar em aceitar alguma quantidade de fatos e entidades fundamentais, de forma a poder trabalhar as demonstrações que precisamos. A estes fatos fundamentais damos o nome de *axiomas*[1].

Neste Capítulo abordamos os *Axiomas de Dedekind-Peano*, que definem o conjunto dos números naturais. A partir destes, é possível desenvolver tanto as operações aritméticas básicas em $\mathbb{N}$ como os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e, após desenvolver um ferramental mais elaborado, construir o conjunto dos reais e operações aritméticas nele.

2.1 Naturais

Os *Axiomas de Dedekind-Peano*, descritos por Dedekind e Peano, são uma maneira de definir os números naturais usando tres conceitos primitivos

[1] O que se toma como axioma e o que se define e demonstra varia conforme o objetivo. Em um curso de Cálculo aplicado, pode-se definir os números reais axiomaticamente, apresentando suas propriedades apenas. Já em outros cursos é interessante mostrar que é possível definir os reais e as operações sobre eles a partir dos racionais.

("número", "zero" e "sucessor") e cinco axiomas. Aqui reproduzimos os Axiomas de Dedekind-Peano que nos interessam (há quatro deles que tratam da relação de igualdade, mas presumimos aqui que esta já está bem definida). Este recorte é comum na apresentação destes axiomas.

(i) 0 é um número natural[2];

(ii) se n é um número natural, então o *sucessor de* n, denotado $s(n)$, é um número natural;

(iii) 0 não é sucessor de qualquer outro número natural;

(iv) se dois naturais p e q tem o mesmo sucessor, então p e q são iguais;

(v) se (i) 0 pertence a um conjunto X; e (ii) se sempre que $n \in X$ implicar que $s(n)$ também pertença a X – então $X = \mathbb{N}$.

Denotamos o conjunto dos número naturais por $\mathbb{N}$.

O quinto axioma de Dedekind-Peano expressa o *princípio da indução finita*.

2.1.1 Um modelo para $\mathbb{N}$

Os axiomas de Dedekind-Peano são uma *definição* do conjunto dos números naturais. Esta definição somente nos informa as propriedades que os naturais devem ter – mas não nos ajuda a construir um objeto que tenha essas propriedades. Se conseguirmos construir um conjunto que obedeça os axiomas de Dedekind-Peano, teremos construído um *modelo* para os números naturais.

Como parte do esforço de formalizar a Teoria dos Conjuntos como fundamento da Matemática, Ernst Zermelo, Abraham Fraenkel e Thoralf Skolem[3] desenvolveram o que se chama hoje de Teoria de Conjuntos de Zermelo-Fraenkel (chamada de ZF, ou ZFC quando inclui o Axioma da Escolha[4]). A partir da Teoria ZF houve várias construções do conjunto dos naturais. Um destes modelos, dado por John von Neumann, é apresentado aqui. Usamos apenas a existência do conjunto vazio e a operação de união. Determinamos

[2] A formulação original de Dedekind-Peano não incluia o zero como natural, e definia os naturais como $\{1, 2, \ldots\}$. É comum incluir o zero por ser o elemento neutro para a adição.

[3] Não juntos – Zermelo publicou seu trabalho inicialmente em 1908; Fraenkel e Skolem independentemente o modificaram em 1922

[4] O Axioma da Escolha diz que "dada uma coleção de conjuntos não vazios, pode-se *escolher* um elemento de cada conjunto da coleção". Há uma grande quantidade de enunciados equivalentes a este – por exemplo "todo espaço vetorial sobre um corpo tem uma base".

que

$$\begin{aligned} &\text{o número } 0 \text{ é} && \emptyset \\ &\text{o número } 1 \text{ é} && \{0\} = \{\emptyset\} \\ &\text{o número } 2 \text{ é} && \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ & && \vdots \end{aligned}$$

Observe que estamos naturalmente definindo o sucessor de qualquer número como

$$s(n) = n \cup \{n\},$$

e que o número n é definido como o conjunto de seus antecessores, $n = \{0, 1, 2, \ldots, n-1\}$.

É possível demonstrar que os axiomas de Dedekind-Peano valem para esta construção dos naturais.

2.1.2 Independência dos axiomas

Queremos que nossas definições não incluam mais do que o necessário – um conjunto menor de axiomas é usualmente mais elegante, e exige menos trabalho quando precisamos verificar se algum objeto está de acordo com aqueles axiomas.

Por exemplo, há cinco axiomas da Geometria Euclideana plana:

(i) pode-se traçar uma linha reta entre quaisquer dois pontos;

(ii) qualquer segmento de reta pode ser estendido indefinidamente;

(iii) um círculo pode ser traçado com qualquer ponto como centro e com qualquer raio;

(iv) todos os ângulos retos são iguais;

(v) dado qualquer ponto P fora de uma reta R, é possível traçar uma única reta paralela a R passando por P.

Por séculos, Matemáticos acreditaram que o quinto axioma (chamado de "axioma das paralelas") era desnecessário, e que poderia ser deduzido a partir dos outros – só não conseguiam encontrar a demonstração. No entanto, no século dezenove Nikolai Lobachevsky e János Bolyai mostraram que se o quinto axioma for modificado a Geometria resultante é completamente diferente da Geometria Euclideana. Ao trocar "uma reta paralela a R" por "ao menos duas retas paralelas a R", descrevemos os Axiomas da *Geometria Hiperbólica*.

Ao apresentar modelos diferentes que satisfazem todos os axiomas, exceto um deles, provamos que aquele axioma não pode ser deduzido a partir dos outros.

Os axiomas de Dedekind-Peano são *independentes*: nenhum deles pode ser demonstrado a partir dos outros. Se removermos um deles, teremos algo diferente dos números naturais.

Teorema 2.1. *Os axiomas de Peano são independentes.*

Demonstração. Construimos, para cada um dos cinco axiomas, um *modelo para* $\mathbb{N}$ que satisfaz todos os outros menos ele. Damos cinco destes modelos a seguir.

(i) Para o primeiro axioma, o conjunto vazio. Note que o primeiro axioma é o único que requer a *existencia* de um elemento – os outros são afirmações quantificadas com $\forall$, e portanto condicionais. Assim, para o conjunto vazio todos os outros axiomas são verdadeiros por vacuidade;

(ii) Para o segundo axioma, o conjunto $\{0\}$, com $s(0) = 1$;

(iii) Para o terceiro axioma, o conjunto $\{0\}$, com $s(0) = 0$;

(iv) Para o quarto axioma, o conjunto $\{0, 1\}$, sendo que um sucede tanto zero como um: $s(0) = s(1) = 1$;

(v) Para o quinto axioma, podemos incluir mais elementos no conjunto: $\{0, 1/2, 1, 3/2, 2, \ldots\}$, mas mantendo a função sucessor $s(n) = n + 1$. □

2.2 Indução

O quinto Axioma de Dedekind-Peano, chamado de "axioma da indução", é, mais que parte de uma definição, uma poderosa ferramenta para demonstrações, e é usualmente apresentado como tal. A seguir o axioma é apresentado novamente, desta vez como técnica e não como definição.

Dado um predicado P a respeito de número naturais, se

(i) $P(0)$ vale;

(ii) para todo natural k, a validade de $P(k)$ implica na validade de $P(k+1)$;

então $P(n)$ vale para qualquer $n \in \mathbb{N}$.

Dizemos que $P(0)$ é a "base"; que $P(k)$ é a "hipótese de indução"; e que demonstrar $P(k) \Rightarrow P(k+1)$ é o "passo de indução".

Exemplo 2.2. Como primeiro exemplo, tome o predicado

$$P(n) = \text{“}9^n - 2^n \text{ é divisível por } 7\text{”}$$

Começamos com a base, provando que $P(0)$ vale:

$$9^0 - 2^0 = 1 - 1 = 0, \text{ divisível por } 7$$

Agora realizamos o passo: provamos que $P(k) \Rightarrow P(k+1)$.

Hipótese: $9^k - 2^k$ é divisível por 7 (esta é $P(k)$)

Passo:

$$\begin{aligned} 9^{k+1} - 2^{k+1} &= 9(9^k - 2^k) + 2^k(9-2) \\ &= 9(7x) + 2^k(7) \qquad \text{(aqui usamos a hipótese de indução!)} \\ &= 7(9x + 2^k). \end{aligned}$$

Mostramos portanto que $9^{k+1} - 2^{k+1}$ é múltiplo de sete, *presumindo que* $9^k - 2^k$ *também é.* Ou seja, presumimos $P(k)$ e concluimos que $P(k+1)$ vale (note que a sequência de iguialdades acima expressa que $9^{k+1} - 2^{k+1}$ é múltiplo de 7 – ou seja, expressa que $P(k+1)$ é verdade). Isto completa a demonstração. ◀

Exemplo 2.3. Neste exemplo usaremos o princípio da indução de maneira um pouco diferente: provaremos a base para $n = 1$ (e não para $n = 0$), e teremos provado a validade da propriedade para todo natural *a partir de um*.

Os números de Fibonacci são definidos recursivamente da seguinte maneira.

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \end{aligned}$$

Provaremos que, para todo inteiro positivo n,

$$\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}.$$

Começamos com a base:

$$\begin{aligned} F_1^2 &= F_1 F_2 \\ 1^1 &= (1)(1) \end{aligned}$$

Hipótese: $\sum_{i=1}^{k} F_i^2 = F_k F_{k+1}$.

Passo:

$$\begin{aligned}\sum_{i=1}^{k+1} F_i^2 &= \left(\sum_{i=1}^{k} F_i^2\right) + F_{k+1}^2 \\ &= F_k F_{k+1} + F_{k+1}^2 && \text{(pela hipótese de indução)} \\ &= F_{k_1}(F_k + F_k + 1) \\ &= F_{k+1} F_{k+2}.\end{aligned}$$

Mostramos que a fórmula vale para $k+1$, usando a hipótese de que vale para k. Como também mostramos a base – que a fórmula vale para 1 – terminamos a demonstração de que ela vale para todo inteiro positivo. ◀

Exemplo 2.4. Para qualquer número real $x \neq 1$ e qualquer número natural $n \geq 1$,

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}.$$

A demonstração é por indução em n.

Base: se $n = 1$, temos

$$\sum_{i=0}^{1-1} x^i = x^0 = 1 = \frac{x^1 - 1}{x - 1}.$$

Agora fazemos o passo de indução. A hipótese é que para n,

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}.$$

Então, para $n + 1$,

$$\begin{aligned}\sum_{i=0}^{[\mathbf{n+1}]-1} x^i &= \sum_{i=0}^{n} x^i \\ &= x^n + \sum_{i=0}^{n-1} x^i \\ &= x^n + \frac{x^n - 1}{x - 1} && \text{(usamos a hipótese de indução!)} \\ &= \frac{(x-1)x^n + x^n - 1}{x - 1} \\ &= \frac{x^{[\mathbf{n+1}]} - 1}{x - 1}.\end{aligned}$$

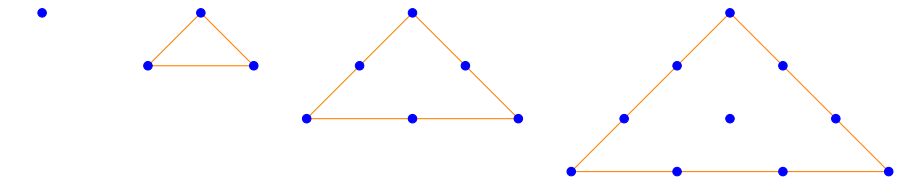
Ou seja,

$$\sum_{i=0}^{[\mathbf{n+1}]-1} x^i = \frac{x^{[\mathbf{n+1}]} - 1}{x - 1},$$

que é a forma exata da proposição, para $n + 1$. ◀

Exemplo 2.5. Números triangulares são números que representam uma quantidade de objetos organizados em um triângulo equilátero. Denotamos o n-ésimo número triangular por T_n:

$T_1 = 1$ $T_2 = 3$ $T_3 = 6$ $T_4 = 10$



A partir da figura fica claro que T_n é igual a T_{n-1} com mais uma linha contendo n elementos, portanto os números triangulares são

$$\begin{aligned} T_1 &= 1, \\ T_n &= T_{n-1} + n. \end{aligned}$$

Provaremos, por indução em n, que o n-ésimo número triangular é

$$T_n = \frac{n(n+1)}{2}.$$

Base: trivialmente, $n = 1$ é triangular.

Hipótese: $k(k+1)/2$ é triangular.

Passo: sabemos que T_k é triangular (pela hipótese de indução), e que

$$T_{k+1} = T_k + (k+1).$$

Usamos a hipótese de indução, e

$$\begin{aligned} T_{k+1} &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(\mathbf{k+1})(\mathbf{k+1}+1)}{2}, \end{aligned}$$

que a forma do enunciado para $k + 1$. ◀

2.2.1 Aritmética

Tendo definido o conjunto dos números naturais, precisamos de operações para que possamos computar com eles. Definimos a seguir soma e subtração para naturais, a partir somente de nossa construção (usamos somente o conceito de número natural e o de sucessor).

Definição 2.6 (soma e multiplicação en $\mathbb{N}$)**.** As operações de **soma** e **multiplicação** para naturais são:

$$n + 0 = n$$
$$n + s(m) = s(n + m)$$

$$n0 = 0$$
$$ms(n) = mn + m. \qquad \blacklozenge$$

Será útil também dar nome ao número um, para tornar mais confortável algumas demonstrações adiante:

Definição 2.7 (um)**.** $s(0) = 1$. $\blacklozenge$

Não presumimos nada, por mais intuitivo que seja, sem demonstrar – a seguir, por exemplo, provamos que $s(a) = a + 1$.

Lema 2.8. $\forall a \in \mathbb{N}, s(a) = a + 1$.

Demonstração. A demonstração é direta:

$$\begin{aligned} s(a) &= s(a + 0) && \text{(definição de soma)} \\ &= a + s(0) && \text{(definição de soma)} \\ &= a + 1. && \square \end{aligned}$$

Teorema 2.9. *As operações aritméticas que definimos para naturais tem as seguintes propriedades:*

(i) *a soma e a multiplicação são associativas e comutativas;*

(ii) *há elementos neutros únicos* $(0, 1)$ *para soma e multiplicação;*

(iii) *vale a distributividade da multiplicação sobre a soma;*

(iv) *vale o cancelamento tanto para adição como para multiplicação,* $a + c = b + c \Rightarrow a = b$, *e se* $c \neq 0$, $ac = bc \Rightarrow a = b$*;*

(v) $ab = 1 \Rightarrow a = 1$ *e* $b = 1$*;*

(vi) $a + b = 0 \Rightarrow a = b = 0$, *e* $ab = 0 \Rightarrow a = 0$ *ou* $b = 0$*;*

(vii) o zero aniquila $\mathbb{N}$*, ou seja,* $\forall n \in \mathbb{N},\ 0n = 0$.

Demonstração. Demonstramos parte das propriedades; outra parte servirá como exercício.

- A soma é associativa, $(a + b) + c = a + (b + c)$. Demonstramos por indução em c. O caso base é com $c = 0$:

$$\begin{aligned} (a+b)+0 &= a+b && ((\cdots)+0=\cdots)\\ &= a+(b+0) && (b = b+0)\end{aligned}$$

  Estabelecemos que $(a + b) + 0 = a + (b + 0)$ – ou seja, mostramos que o enunciado vale quando $c = 0$.

  Agora, partimos da hipótese de que a soma é associativa quando fixamos c, ou seja, que $(a + b) + c = a + (b + c)$, e mostramos que isto implica na validade para $s(c)$.

$$\begin{aligned} (a+b)+s(c) &= s((a+b)+c) && \text{(definição de soma)}\\ &= s(a+(b+c)) && \text{(pela hipótese de indução)}\\ &= a+s(b+c) && \text{(definição de soma)}\\ &= a+(b+s(c)) && \text{(definição de soma)}\end{aligned}$$

- A soma é comutativa, $a + b = b + a$. Esta demonstração é um pouco mais longa que a anterior. Primeiro provaremos que $a+1 = 1+a$ para todo $a \in \mathbb{N}$, e depois usaremos este fato para provar que $a+b = b+a$.

  Primeira parte, $\forall a \in \mathbb{N},\ \ a + 1 = 1 + a$.
  Base de indução: $a = 0$. Temos $a + 1 = 0 + 1 = 1 + 0 = 1 + a$.

  Hipótese de indução: $a + 1 = 1 + a$

  Passo:

$$\begin{aligned} s(a)+1 &= s(a)+s(0) && (1 = s(0))\\ &= s(s(a)+0) && \text{(definição de soma)}\\ &= s((a+1)+0) && \text{(Lema 2.8, } s(a) = a+1)\\ &= s(a+1) && \text{(definição de soma)}\\ &= s(1+a) && \text{(pela hipótese de indução)}\\ &= 1+s(a) && \text{(definição de soma)}\end{aligned}$$

  Provamos então que $a + 1 = 1 + a$.

  Agora demonstramos que $a + b = b + a$.

  Base: para $b = 1$, é exatamente o que provamos anteriormente ($a+1 = 1 + a$).

Hipótese de indução: $a + b = b + a$

Passo:

$$\begin{aligned}
a + s(b) &= a + (b + 1) && \text{(Lema 2.8)}\\
&= (a + b) + 1 && \text{(por associatividade)}\\
&= (b + a) + 1 && \text{(pela hipótese de indução)}\\
&= b + (a + 1) && \text{(por associatividade)}\\
&= b + (1 + a) && \text{(pelo caso base, } a + 1 = 1 + a)\\
&= (b + 1) + a && \text{(por associatividade)}\\
&= s(b) + a && \text{(Lema 2.8)}
\end{aligned}$$

- O zero é neutro para adição, como está na própria definição de adição ($n+0 = n$). Por comutatividade, temos também $0+n = n$. Temos ainda que mostrar que zero é o *único* elemento neutro para adição. Suponha que haja outro neutro aditivo, e, ou seja, $a + e = a$ para todo a. Então, para $a = 0$, temos

$$\begin{aligned}
a + e &= a && \text{(por suposição, } e \text{ é neutro)}\\
0 + e &= 0 && \text{(se vale para todo } a\text{, vale para zero)}\\
e + 0 &= 0 && \text{(por comutatividade)}\\
e &= 0. && \text{(definição de soma)}
\end{aligned}$$

  Se $a = 0$, então $e = 0$. Como e é constante (é um número, não uma variável), ele deve sempre ser igual a zero. □

2.2.2 Ordem

Além da aritmética, nos interessa definir alguma relação de ordem em $\mathbb{N}$. Isto pode ser feito de maneira bastante simples, mas não se pode esperar que seja sempre possível em qualquer estrutura (por exemplo, não há como definir para os números complexos uma relação de ordem que seja consistente com as operações aritméticas[5]).

Definição 2.10 (menor ou igual)**.** Definimos a relação $\leq$ (**menor ou igual**) para naturais de forma que $a \leq b$ se e somente se existe algum $m \in \mathbb{N}$ tal que $a + m = b$. ♦

Damos exemplos: $4 \leq 10$ porque $4 + 6 = 10$; também $0 \leq 2$ porque $0 + 2 = 2$.

[5]Embora possamos ordenar os complexos, por exemplo, por norma, não podemos escolher uma ordem que os torne um *corpo ordenado*. Se houvesse uma relação de ordem total $\prec$ para $\mathbb{C}$, teríamos necessariamente que $i \prec 0$ ou que $0 \prec i$, mas não ambos. No entanto, nos dois casos chegaríamos a contradições.

Vale observar que esta definição de $\leq$ depende da definição de soma – e que nossa noção de ordem, portanto, está fundamentada na operação que desenvolvemos para os naturais, e só faz sentido a partir dela.

Definição 2.11 (relação de ordem parcial)**.** Uma relação R em um conjunto X é dita *de ordem parcial não-estrita* se para todos $x, y, x \in X$,

i) R é reflexiva (xRx);

ii) R é antisimétrica (xRy e yRx implicam em $x = y$);

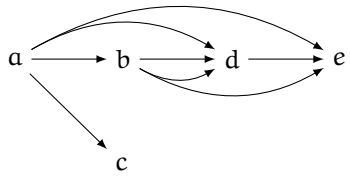
iii) R é transitiva (xRy e yRz implicam em xRz).

♦

Exemplo 2.12. Seja $X = \{a, b, c, d, e\}$, e seja $\prec$ uma relação em X tal que

$$\begin{array}{llll} a \prec a & & a \prec b & \\ b \prec b & & a \prec c & b \prec d \\ c \prec c & & a \prec d & b \prec e \\ d \prec d & & a \prec e & d \prec e \\ e \prec e & & & \end{array}$$

O grafo a seguir (chamado de *diagrama de Hasse*) representa a relação (uma aresta de x a y significa que $x \prec y$). Para maior clareza, não são mostrados no grafo o relacionamento de elementos com eles mesmos ($a \prec a$, $b \prec b$) etc.



Então $\prec$ é uma relação de ordem parcial não-estrita em X, porque $\prec$ é:

- reflexiva, porque todo elemento se relaciona com ele mesmo (vide primeira coluna na descrição da relação);
- antissimétrica, porque só vale $x \prec y$ e $y \prec x$ quando $x = y$;
- transitiva, porque sempre que $x \prec y$ e $y \prec z$, também vale $x \prec z$.

Há elementos que não são comparáveis: c só é comparável com a ($a \prec c$), mas não com os outros elementos. Se todos os elementos fossem comparáveis entre si, a relação seria de *ordem total*. ◄

Exemplo 2.13. Seja X um conjunto, e $P(X)$ o conjunto das partes de X. Então $\subseteq$ é uma relação de ordem parcial não-estrita em $P(X)$.

Verificamos, sem entrar em muitos detalhes: para todos os conjuntos $A, B, C \in P(X)$,

i) Reflexividade: $A \subseteq A$, trivialmente.

ii) Anti-simetria: $A \subseteq B$ e $B \subseteq A$ implica em $A = B$.

iii) Transitividade: $A \subseteq B$ e $B \subseteq C$ implica em $A \subseteq C$. ◀

Teorema 2.14. *$\leq$ é uma relação de ordem parcial não estrita em $\mathbb{N}$.*

A seguir enunciamos o *princípio da boa ordem*, que afirma haver um menor elemento em qualquer subconjunto dos naturais.

Princípio da boa ordem: *Todo subconjunto não vazio dos naturais tem um menor elemento – ou seja, se $S \in \mathbb{N}$, então existe um n tal que $\forall q \in S, n \leq q$.*

Teorema 2.15. *O princípio da indução (quinto axioma de Dedekind-Peano) e o da boa ordem são equivalentes.*

Demonstração. Demonstramos que cada um dos princípios pode ser deduzido a partir do outro.

($\Rightarrow$, indução implica em boa ordem)
Demonstramos o princípio da boa ordem usando indução. Aqui usamos o princípio da indução forte. Como este é equivalente ao da indução fraca, o resultado não é afetado.

Como 0 não é sucessor de ninguém, não existem números $a, b \neq 0$ tal que $a + b = 0$. Logo ninguém é menor que zero.

Suponha agora que haja algum $S \in \mathbb{N}$ onde não exista menor elemento.

Base: necessariamente $0 \notin S$, porque se 0 estivesse em S, ele seria o menor elemento de S.

Hipótese: supomos que nenhum $k \leq n$ está em S.

Passo: n também não pode estar em S, porque pela hipótese de indução não há ninguém menor que n em S, e n seria o menor elemento.

($\Leftarrow$, boa ordem implica em indução)
Supomos agora que vale o princípio da boa ordem, e provamos que deve valer o princípio da indução finita.

Suponha que uma proposição P valha para zero, e que sempre que vale para n, também vale para $n + 1$. Se o princípio da indução finita vale, isto significaria que $P(k)$ vale para todo natural k – mas *presumimos que não vale o princípio da indução*, e portanto deve existir pelo menos um k tal que $P(k)$ não vale.

Seja $S \subseteq \mathbb{N}$ o conjunto de naturais para os quais P *não* vale. *Pelo princípio da boa ordem*, S tem um menor elemento, que chamamos de k. Logo, $P(k)$ não vale. Como k é o menor elemento de S, e $k - 1 < k$, então $P(k - 1)$

vale. Mas se $P(k-1)$ vale, então $P(k-1+1) = P(k)$ deve valer. Como mostramos que $P(k)$ deve valer e que também não deve valer, chegamos a uma contradição, e negamos a suposição que fizemos de que deve haver algum k tal que $P(k)$ não vale. Demonstramos portanto o princípio da indução finita usando o princípio da boa ordem. □

Como o quinto axioma é equivalente ao da boa ordem, poderíamos reescrever os axiomas de Dedekind-Peano usando como quinto axioma o da boa ordem, e descartando o da indução, e o efeito seria o mesmo. No entanto, o princípio da boa ordem depende da relação de ordem, que por sua vez depende da definição de operações aritméticas, que tornariam a descrição dos naturais demasiado grande – é portanto mais interessante manter o axioma da indução.

2.3 Descida Infinita

Uma vez que o princípio da indução dá origem a uma técnica de demonstração, é natural questionar se o princípio da boa ordem também não teria a mesma consequência. Ocorre que o princípio da boa ordem é usado com grande frequência em demonstrações, e foi formalizado por Pierre de Fermat, com o nome de "método (ou princípio) da descida infinita".

O princípio da descida infinita é, essencialmente, o princípio da boa ordem, ligeiramente refraseado: "se algum processo iterativo gera, a partir de n, números naturais menores que n, então esse processo deve necessariamente parar".

As demonstrações dos Teoremas que seguem nesta seção ilustram o método.

Teorema 2.16. *$\sqrt{2}$ é irracional.*

Demonstração. (pelo método da descida infinita) Suponha que $\sqrt{2} \in \mathbb{Q}$. Então $\sqrt{2} = m/n$, sendo m/n uma fração reduzida: m e n são os menores números naturais tais que $m/n = \sqrt{2}$.

$$\begin{aligned} \sqrt{2} &= \frac{m}{n} \\ 2 &= \frac{m^2}{n^2} \\ 2n^2 &= m^2 \end{aligned}$$

O lado esquerdo é um quadrado par – e portanto o lado direito também é.

Como m^2 só pode ser par se m for par, então podemos denotar $m = 2M$, e

$$\begin{aligned} 2n^2 &= (2M)^2 \\ 2n^2 &= 4M^2 \\ n^2 &= 2M^2 \end{aligned}$$

Agora, o lado direito é par, o que significa que o esquerdo também deve ser, e $n = 2N$: como $n = 2N$ e $M = 2M$,

$$\begin{aligned} \sqrt{2} &= \frac{m}{n} \\ &= \frac{2M}{2N} \\ &= \frac{M}{N}. \end{aligned}$$

Isso contradiz o que determinamos inicialmente – que m/n seria uma fração reduzida. O argumento usado nesta demonstração é que para cada m, n, podemos gerar M e N, tais que $M < m$ e $n < N$, gerando uma quantidade infinita de números naturais cada vez menores.

Pelo princípio da descida infinita, essa sequência infinita não pode ser gerada, e a hipótese de $\sqrt{2}$ ser racional deve ser rejeitada.

Ou, da mesma forma, pelo princípio da boa ordem, o conjunto de números gerados neste processo é subconjunto de $\mathbb{N}$, e deve ter um menor elemento. Como o processo gera números cada vez menores, e não para, a hipótese deve ser rejeitada. □

Teorema 2.17. *Seja* $X = (x_1, x_2, \ldots, x_{2n+1})$ *uma sequencia com a seguinte propriedade: se* qualquer x_i *for removido, então a sequência resultante pode ser separada em duas sequências distintas* A *e* B*, cada um de tamanho* n*, tais que a soma de* A *e de* B *são iguais.*

Então $x_1 = x_2 = \cdots = x_{2n+1}$.

Por exemplo, em $(1, 2, 3, 3, 3)$ os elementos não são iguais. Se retirarmos 2, a sequência resultante é $(1, 2, 3, 3)$, que não pode ser particionada em duas sequências de mesma soma: quando a separarmos, teremos dois elementos em A e dois em B, e como são três ímpares e um par, as somas de A e B terão paridades diferentes, portanto serão diferentes:

A	B
$1 + 2 = 3$	$3 + 3 = 6$,
$1 + 3 = 4$	$2 + 3 = 5$.

Já a sequência $(2, 2, 2, 2, 2)$ tem todos os elementos iguais, e se removermos, por exemplo, o primeiro elemento, o resultado é $(2, 2, 2, 2)$, que pode

ser dividida em duas subsequências de mesma soma, $(2,2)$ e $(2,2)$, ambas com soma 4 – e não há ourta forma de separar a sequência em duas.

Demonstração. Presuma, sem perda de generalidade, que os índices estão de acordo com a ordem dos números: $x_1 \leq x_2 \leq \cdots \leq x_{2n+1}$.

Suponha que haja na sequência pelo menos um elemento diferente de x_1.

Se removermos x_1 de todos os elementos, teremos

$$(0, x_2 - x_1, \ldots, x_{2n-1} - x_1),$$

e esta sequência ainda teria a mesma propriedade, porque removemos nx_1 tanto da soma de A como da de B.

Assim, trabalhamos com esta nova sequência onde $x_1 = 0$.

Agora, a soma de uma subsequencia de tamanho $2n$ será sempre par, porque de outra forma teríamos como obter A e B com paridades diferentes, e portanto somas diferentes.

Por consequência, quaisquer dois números x_i, x_j devem ter a mesma paridade, porque se não for o caso podemos trocar elementos entre os conjuntos A e B obtendo somas com paridades diferentes.

Mas como $x_1 = 0$ é par, então todos os x_i são pares. Se dividirmos todos os elementos por 2, a sequência manterá a propriedade.

Retomamos o processo, e a sequencia será dividida por 2 repetidamente.

Isso significa que os números serão divisíveis por 2, 2^2, 2^4, e por 2^k para qualquer k natural, gerando números pares cada vez menores. O único número divisível por 2^k para qualquer k (e que sempre geraria o zero, e não um natural menor) é o próprio zero, mas como havia algum elemento diferente de x_1, os x_i não poderão jamais ser todos iguais a zero.

Assim, todos os elementos são iguais a x_i. □

É comum expor explicitamente quando se pretende usar o método da indução, iniciando a demonstração dizendo que ela se dará “por indução na variável i”, ou afirmação semelhante. Isso já não é tão comum quando se usa o princípio da descida infinita.

2.4 Inteiros e Racionais

Construiremos agora os números inteiros. Podemos tentar fazê-lo de maneira muito simples: um inteiro é a diferença entre dois naturais. Temos $-2 = 0 - 2$ e $-5 = 10 - 15$, por exemplo. No entanto, isto não é aceitável, porque não definimos a operação de subtração para naturais (e se o tivéssemos feito, ela não seria fechada em $\mathbb{N}$).

Tentamos então construir inteiros como pares de naturais, e dois inteiros (a, b) e (p, q) são iguais se existe um número k tal que $b + k = a$ e $q + k = p$.

Permanece, entretanto, um problema: não podemos dizer que um inteiro é *um par ordenado de naturais* porque relacionamos mais de um par de naturais com o mesmo inteiro: tanto $(2,3)$ como $(10,11)$ seriam o mesmo inteiro, que usualmente denotamos por -1 (na verdade, desta forma obtivemos infinitos pares de naturais para cada inteiro).

Abraçamos a idéia do inteiro como vários pares ordenados, então. Para descrever quais pares ordenados de naturais definem o mesmo inteiro, usamos uma relação de quivalência.

Definição 2.18 (partição)**.** Seja X um conjunto. Os conjuntos $X_1, X_2, \ldots, X_k$ são uma **partição** de X se

i) todo X_i é subconjunto de X;

ii) quando $i \neq j$, $X_i \cap X_j = \emptyset$;

iii) A união de todos os X_i é igual a X.

♦

Exemplo 2.19. Seja P o conjuntos dos naturais pares, e I o conjunto dos ímpares. Os conjuntos P e I formam uma partição de $\mathbb{N}$, porque

i) $P \subset \mathbb{N}$, $I \subset \mathbb{N}$;

ii) $P \cap I = \emptyset$ (não existe número que seja par e também ímpar);

iii) $P \cup I = \mathbb{N}$.

O mesmo vale trivialmente para "primos e não primos", "quadrados perfeitos e não-quadrados", e também para partições em mais de dois subconjuntos, como no exemplo a seguir. ◄

Exemplo 2.20. Podemos particionar $\mathbb{N}$ de forma que os números com k primos distintos em sua fatoração fiquem na k-ésima partição (admitindo 0 e 1 como suas próprias fatorações):

i) Na partição P_1 temos 0, 1, os primos e potências de primo:

$$P_1 = \{0, 1, 2, 2^2, 2^3, 2^4, \ldots, 3, 3^2, 3^2, 3^4, \ldots, 5, 5^2, 5^3, 5^4, \ldots\}$$

ii) Na partição P_2 temos $6, 10, 12, 15$, e os números com dois primos na fatoração:

$$6 = (2)(3), 10 = (2)(5), 12 = (2^2)(3), 15 = (3)(5), \ldots$$

...) E assim sucessivamente.

Esta separação de $\mathbb{N}$ em conjuntos é uma partição (facilmente verificável). Aqui, $\mathbb{N}$ é particionado em infinitos subconjuntos. ◄

Definição 2.21 (relação de equivalência)**.** Uma relação R em um conjunto X é **de equivalência** se, para todos $x, y, z \in X$,

i) xRx (R é reflexiva);

ii) xRy implica em yRx (R é simétrica);

iii) xRy e yRz implica em xRz (R é transitiva).

♦

Exemplo 2.22. Em $\mathbb{N}$, seja $\sim$ a relação definida tal que $a \sim b$ se e somente se, ao serem divididos por 3, tanto a como b deixam o mesmo resto. Assim,

- $5 \sim 17$, porque o resto de 5 por 3 é um, assim como o de 17 por 3;
- $2 \sim 35$, porque o resto de 2 por 3 é 2, assim como o de 35 por 3.

A relação $\sim$, aqui definida, é de equivalência: para todos $m, n, o \in \mathbb{N}$,

i) $m \sim m$ (é reflexiva);

ii) se $m \sim n$, então $n \sim m$ (é simétrica);

iii) e se $m \sim n$, $n \sim o$, então $m \sim o$ (é transitiva).

Mais adiante este tipo de relação será tratada mais extensivamente. ◄

Exemplo 2.23. Dois triângulos são **similares** se as proporções de seus lados são iguais – ou seja, se os comprimentos dos lados dos triângulos, *listados em ordem crescente* são a, b, c para o primeiro e x, y, z para o segundo, então os dois triângulos são similares se

$$a/b = x/y$$
$$b/c = y/z$$
$$a/c = x/y$$

O conceito de simiaridade captura o que informalmente chamamos de "forma", abstraindo (ignorando) o tamanho dos triângulos.

Quando dois triângulos T_1 e T_2 são similares, denotamos $T_1 \sim T_2$.

Seja T o conjunto de todos os triângulos. Então a relação de similaridade (a relação $\sim$ definida no parágrafo anterior) é de equivalência.

Para cada três triângulos $A, B, C \in T$,

i) $A \sim A$;

ii) Se $A \sim B$, então $B \sim A$;

iii) Se $A \sim B$ e $B \sim C$, então $A \sim C$,

sendo os três itens trivialmente verificáveis. ◀

Teorema 2.24. *Seja $\sim$ uma relação de equivalência em um conjunto X, Então $\sim$* define uma partição em X, *ou seja: se $x \not\sim y$, então x e y estão em partições diferentes; se $x \sim y$, estão na mesma partição. Todo elemento está em alguma partição, e as interseções entre partições são vazias.*

Exemplo 2.25. A relação de similaridade entre triangulos, definida no Exemplo 2.23, é de equivalência, portanto define uma partição no conjunto T de todos os triangulos:

i) toda partição é subconjunto de T;

ii) nenhum triângulo pode estar em duas classes diferentes de equivalência;

iii) a união de todas as classes de equivalência é T. ◀

Podemos agora voltar ao trabalho da definição dos inteiros.

Definição 2.26. A relação $\sim_+$ entre números naturais é tal que $(a, b) \sim_+ (p, q)$ se e somente se $a + q = p + b$. ♦

Teorema 2.27. *$\sim_+$ é relação de equivalência.*

Definição 2.28 (números inteiros)**.** Sendo uma relação de equivalência, $\sim_+$ define uma partição em $\mathbb{N} \times \mathbb{N}$. Cada classe de equivalência nesta partição é um **número inteiro**. ♦

Denotamos o conjunto dos números inteiros por $\mathbb{Z}$:

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim_+$$

Isto significa[6] que $\mathbb{Z}$ é igual a $\mathbb{N} \times \mathbb{N}$, mas com a relação de igualdade dada por $\sim_+$.

Temos agora números inteiros. Nos faltam as operações de soma e multiplicação, que não apresentam dificuldade:

$$(a, b) \oplus (p, q) = (a + p, b + q)$$
$$(a, b) \otimes (p, q) = (ap + bq, aq + bp)$$

Nesta definição, para evitar ambiguidade, usamos os símbolos $\oplus$ e $\otimes$ para operações com inteiros e $+$ para operações com naturais.

Os racionais são construídos de maneira semelhante, partindo de pares de inteiros. O Exercício 5 pede a definição da relação de equivalência $\sim_\times$ tal que os racionais possam ser construídos como $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}) / \sim_\times$.

[6] Dizemos que A/R é conjunto das partições de A, definido por R, e tem o nome de "conjunto quociente de A por R".

2.4.1 Definições e Modelos

Há um problema que pode facilmente passar despercebido quando apresentamos a construção de um modelo para inteiros e racionais a partir dos naturais. Definimos inteiros como conjuntos, tendo como ponto de partida ao conjunto vazio. Mas os inteiros são pares ordenados. O natural dois é $\{0,1\} = \{\emptyset, \{\emptyset\}\}$, e o inteiro dois é uma classe de equivalência inteira, $\{(2,0),(3,1),(4,2),\ldots\}$. Como podemos considerá-los "iguais", se são entidades evidentementes diferentes? Não apenas são diferentes: um é finito e o outro não!

Diferenciamos a *definição* da *construção*. O que define os naturais são suas *propriedades*. As propriedades dos naturais são a de um semianel comutativo, que é o que precisamos para contar objetos e realizar operações aritméticas básicas com as quantidades que contamos. A partir do conjunto vazio, mostramos *uma* construção que tem as propriedades dos naturais. Se tomarmos os inteiros positivos apenas, teremos classes de equivalência que se comportam exatamente como os naturais – e portanto teremos uma outra construção dos naturais, *que depende da primeira*, porque afinal de contas, os pares ordenados contém os naturais-como-conjuntos de von Neumann.

2.5 Anéis e Corpos

Demonstramos a seguir um teorema simples a respeito de inteiros, e mais adiante esta demonstração nos servirá de motivação para definir uma generalização de $\mathbb{Z}$, chamada *anel*.

Teorema 2.29. *Em $\mathbb{Z}$, o inverso aditivo de qualquer elemento é único, ou seja, se $a + b = 0$ e $a + c = 0$ então $b = c$.*

Demonstração. Sejam $a, b, c \in \mathbb{R}$, onde tanto b como c são inversos de a: $a + b = 0$ e $a + c = 0$. Então

$$\begin{aligned}
b &= b + 0 && \text{(0 é neutro aditivo)}\\
&= b + (a + c) && \text{(premissa: $a + c = 0$)}\\
&= (b + a) + c && \text{(associatividade da soma)}\\
&= 0 + c && \text{(premissa: $b + a = 0$)}\\
&= c + 0 && \text{(comutatividade da soma)}\\
&= c, && \text{(0 é neutro aditivo)}
\end{aligned}$$

e quaisquer dois inversos aditivos para a serão iguais. Logo, os inversos aditivos em $\mathbb{Z}$ são únicos. □

Listamos as propriedades que usamos na demonstração:

- associatividade da soma;
- comutatividade da soma;
- existência de neutro aditivo (zero).

Isto significa que a demonstração deve valer sem mudanças para racionais, matrizes quadradas, polinômios, funções reais e outras estruturas que tenham as propriedades acima[7].

Uma *estrutura algébrica* é um conjunto adicionado de operações sobre seus elementos. Definimos estruturas algébricas para generalizar estruturas que encontramos na Matemática, abstraindo aquilo que elas tem em comum.

Uma estrutura algébrica que tem as propriedades usadas na demonstração acima – e outras que nos interessam para tratar de inteiros – é o *anel*.

Definição 2.30 (anel)**.** Um **anel** é um conjunto R com duas operações $\otimes$ e $\oplus$, que denominamos "produto" e "soma", de forma que

- as duas operações são associativas;
- a operação de soma é comutativa;
- a multiplicação distribui sobre a soma;
- todo elemento tem um inverso para soma;
- existe um elemento neutro para soma.

Se o anel tem elemento neutro para multiplicação, dizemos que é um *anel com identidade*[8]. ⧫

Usamos a notação $\otimes$ e $\oplus$ na definição apenas para deixar claro que não é necessário que sejam a multiplicação e soma usuais.

Os inteiros, racionais e reais são claramente um anel. Além de conjuntos numéricos, há outros anéis relevantes:

- **Polinômios em uma variável:** o conjunto de todos os polinômios forma um anel.
- **Funções de $\mathbb{R}$ em $\mathbb{R}$:** com as operações usuais de soma e multiplicação de funções, o conjunto de *todas* as funções $f : \mathbb{R} \to \mathbb{R}$ é um anel. Vários subconjuntos deste também são anéis. Por exemplo, o conjunto das funções reais contínuas.

[7] Na verdade, nossa demonstração tratou de uma única operação, mas continuaremos trabalhando com estruturas com duas operações, para simplificar a exposição. O leitor interessado poderá procurar a definição de *grupo*, estrutura algébrica com somente uma operação onde a demonstração acima também vale.

[8] É mais comum o nome "anel com unidade", mas o termo "unidade" também é usado para elementos com inverso multiplicativo.

- **Matrizes quadradas de ordem n:** dado n, o conjunto de todas as matrizes quadradas de ordem n é um anel não comutativo, com identidade.

Definição 2.31 (unidade)**.** Uma **unidade** em um anel é um elemento com inverso multiplicativo. Ou seja, a é unidade se existe b tal que $ab = 1$, onde 1 é a identidade multiplicativa. ⧫

As unidades em $\mathbb{Z}$ são $+1$ e -1. No anel de matrizes quadradas, são as matrizes invertíveis. No anel de polinômios $\mathbb{R}[x]$, são os polinômios constantes não nulos.

A demonstração do Teorema 2.29 pode ser reescrita usando "um anel R" ao invés de "$\mathbb{Z}$", e vale portanto para qualquer anel.

Agora demonstramos outro teorema, desta vez sobre anéis.

Teorema 2.32. *Sejam R um anel e $0 \neq a \in R$. Suponha que haja um único $b \in R$ tal que $aba = a$. Então $ab = ba = 1$, ou seja, a é unidade (tem inverso multiplicativo igual a b).*

Se olharmos apenas para o anel dos inteiros, o Teorema não parece interessante, já que em $\mathbb{Z}$ somente o um tem inverso multiplicativo. Mas há outros anéis, portanto seguimos com a demonstração.

Demonstração. Suponha que $ax = 0$ para algum $x \in R$. Então

$$\begin{aligned} a(b+x)a &= (ab + ax)a && \text{(distributividade)} \\ &= aba + axa && \text{(distributividade)} \\ &= aba && \text{(ax=0)} \\ &= a && \text{(premissa: } aba = a\text{)} \end{aligned}$$

Ou seja, $a(b+x)a = a$. Como dissemos que b é o único tal que $aba = a$, então $b + x = b$, e $x = 0$.

Acima presumimos que $ax = 0$ e chegamos em $x = 0$ – ou seja, *sempre que* $ax = 0$, *teremos* $x = 0$.

Agora, reescrevemos ax com $x = (ba - 1)$:

$$\begin{aligned} a(ba-1) &= aba - a \\ &= a - a \\ &= 0 \end{aligned}$$

Como $a(ba-1) = 0$, é necessário que $ba - 1 = 0$ – ou seja, $ba = 1$.

O argumento pode ser repetido, mostrando que $xa = 0$ implica em $x = 0$, e concluindo que $ab = 1$.

Demonstramos que $ab = ba = 1$, e consequentemente que a tem inverso multiplicativo b. □

Listamos as propriedades que usamos na demonstração:

- distributividade da multiplicação sobre a soma;
- associatividade da multiplicação (poderíamos ter expandido a primeira linha multiplicando os dois fatores da direita, mas fizemos com os dois da esquerda – o resultado é o mesmo);
- existência de neutro aditivo (zero);
- existência de neutro multiplicativo (um);
- $0x = x0 = 0$ para todo $x \in R$ (ou seja, o neutro aditivo aniquila R).

Não usamos comutatividade em nenhum momento. Isto significa que a demonstração deve valer para anéis não comutativos, como os anéis de matrizes quadradas!

Definição 2.33 (corpo)**.** Um anel comutativo onde todo elemento diferente de zero tem inverso multiplicativo é um **corpo**. ♦

Exemplo 2.34. $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ são três corpos: são todos anéis comutativos, e em todos eles qualquer elemento diferente de zero tem inverso multiplicativo. ◀

Exemplo 2.35. O conjunto $\{0, 1\}$ com a operação de multiplicação usual, e com a soma definida como

$$a \oplus b = \begin{cases} 0 & \text{se } a + b \text{ é par} \\ 1 & \text{se } a + b \text{ é ímpar} \end{cases}$$

é um corpo. ◀

Exemplo 2.36. Embora $\mathbb{Z}$ seja um anel, *não é um corpo*, porque somente 1 tem inverso multiplicativo.

O anel de matrizes quadradas de ordem n *não é um corpo*, porque nem toda matriz quadrada tem inversa. ◀

Exercícios

Ex. 1 — Usando os Axiomas de Dedekind-Peano, prove que nenhum número natural pode ser seu próprio sucessor.

Ex. 2 — Usando os Axiomas de Dedekind-Peano, prove que todo número diferente de zero é sucessor de algum outro.

Ex. 3 — A partir da relação $\leq$, defina $\geq$, $<$ e $>$ para naturais.

Ex. 4 — Prove o Teorema 2.14.

Ex. 5 — Construa os racionais usando pares de inteiros, como sugerido no final da seção 2.4: defina a relação de equivalência $\sim_\times$ e construa $\mathbb{Q} = \mathbb{Z}^2/\sim_\times$. Depois mostre as operações de soma e multiplicação para racionais, e mostre que as duas tem inversa em $\mathbb{Q}$.

Ex. 6 — Prove:

(a) $\forall n \geq 1,\ \ 3^n - 1$ é par.

(b) $\forall n \geq 1,\ \ n^3 + 2n$ é divisível por 3.

(c) $\forall n \geq 4,\ \ n! > 2^n$.

(d) $\forall n \geq x, \forall x \in \mathbb{R}$, se $x > -1$, então $(1+x)^n \geq 1 + nx$.

(e) $\forall n \geq 1,\ \ \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.

(f) $\forall n \geq 2,\ \ \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$.

Ex. 7 — Determine uma forma fechada para a soma dos n primeiros cubos ($1^3 + 2^4 + \cdots + n^3$), e demonstre sua validade usando indução.

Ex. 8 — Para cada caso, determine k e prove a afirmação, usando indução:

(a) Existe um número natural k tal que $n(n+1)(n+5)$ sempre é múltiplo de k, para todo n natural.

(b) Existe um número natural k tal que $9^n + 3$ sempre é múltiplo de k, para todo n natural.

Ex. 9 — Se a, b são naturais, denotamos "b é múltiplo de a", ou "a divide b" por $a \mid b$, significando que existe algum k tal que $b = ka$. Prove que em $\mathbb{N}$, a relação $\mid$ é de ordem parcial não-estrita.

Ex. 10 — Prove que em qualquer anel, $-(-x) = x$.

Ex. 11 — Prove que em qualquer anel, o neutro aditivo é único.

Ex. 12 — Verifique se as estruturas a seguir são anéis (para cada uma, prove que é ou que não é). Quando não especificadas, as operações de soma e multiplicações são as usuais.

(a) $\mathbb{N}$.

(b) $\mathbb{C}$.

(c) Os inteiros pares.

(d) Os inteiros ímpares.

(e) Os reais não-negativos (está incluído o zero).

(f) O conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$ tais que $f(x) = 0$ quando $x \in [3, 4]$.

(g) O conjunto de todas as funções reais integráveis em $[0, \infty]$.

(h) O conjunto de todas as funções reais ímpares (ou seja, $f(x) = -f(-x)$).

(i) O conjunto de todas as matrizes quadradas de ordem n, com determinante diferente de zero.

(j) O conjunto de todas as matrizes quadradas de ordem n, com determinante igual a ± 1.

(k) O conjunto de todas as matrizes quadradas com elementos inteiros.

(l) $\mathbb{R}$, mas com a operação de soma $a \oplus b = (a + b)/2$, onde $\oplus$ é a soma a ser usada na estrutura, e $+$ é a soma usual, que usamos apenas para definir $\oplus$.

(m) Tendo fixado um conjunto qualquer X, a estrutura que é composta do conjunto das partes de X, e das operações de diferença simétrica como adição e de interseção como multiplicação.

Ex. 13 — Matrizes quadradas de ordem n não formam um corpo, porque nem toda matriz tem inversa. E quanto ao conjunto das matrizes invertíveis?

Capítulo 3

Bases

O sistema que usualmente empregamos para representar números é *posicional* usando *base dez* – um número n é representado por dígitos concatenados, $n = d_k d_{k-1} \ldots d_1 d_0$, com $0 \leq d_i < 10$, de forma que o valor de n é igual a

$$10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + 10^0 d_0.$$

Por exemplo,

$$\begin{aligned} 2371 &= 10^3(2) + 10^2(3) + 10^1(7) + 10^0(1) \\ &= 2000 + 300 + 70 + 1 \end{aligned}$$

3.1 Naturais

Mantendo o sistema posicional, podemos usar qualquer base maior ou igual a dois[1] para representar números naturais[2]. Por exemplo, o número 10011 representa, na base dois, o natural dezenove:

$$\begin{aligned} & 2^4(1) + 2^3(0) + 2^2(0) + 2^1(1) + 2^0(1) \\ =& 16 + 0 + 0 + 2 + 1 \\ =& 19 \end{aligned}$$

Perguntamos agora se qualquer número natural pode ser representado em qualquer base. A resposta é sim[3], conforme o Teorema 3.1.

[1] Mas veja o Exercício 15.

[2] Além de ser teoricamente interessante, o uso de bases diferentes é de grande relevância em Engenharias e Computação – as bases dois e dezesseis são particularmente importantes.

[3] A resposta é a mesma para inteiros, racionais e reais. Para reais, o leitor familiar com Álgebra Linear identificará que o conceito de "base" para representação de reais é exatamente o de "base" para o espaço vetorial $\mathbb{R}$, de dimensão um.

Teorema 3.1. *Seja* b *um número natural maior que um. Então todo número natural* n *pode ser descrito unicamente como*

$$n = a_0 b^0 + a_1 b^1 + \cdots + a_k b^k,$$

com $a_k \neq 0$ *e* $0 \leq a_i < b$. *Dizemos que esta é a* representação de n na base b.

Demonstração. Primeiro demonstramos a *existência* de representação de n na base b; depois trataremos da *unicidade* dessa demonstração.

A existência de representação de n na base b é realizada por indução em n.

A base se dá com $n = 1$,

$$n = 1b^0 + 0b^1 + \cdots + 0b^k.$$

A hipótese de indução é

$$z = a_0 b^0 + a_1 b^1 + \cdots + a_k b^k, \quad \text{para } z = 1, 2, \ldots, n-1.$$

Como presumimos que $b > 1$, então $b^0 < b^1 < b^2 < \cdots$, e todo natural maior que um está entre duas potências de b, ou seja, para todo $k \in \mathbb{N}$, quando $m > 0$, existe um *único* $u \in \mathbb{N}$ tal que

$$b^u \leq m < b^{u+1}.$$

Agora, seja $n > 1$ natural. Logo, existe um único q tal que

$$b^q \leq n < b^{q+1}.$$

Dividindo[4] n por b^q, obtemos quociente a_q e resto r:

$$n = a_q b^q + r, \quad 0 \leq r \leq b^q. \tag{3.1}$$

Observamos que

$a_q > 0$, porque $a_q b^q = n - r > 0$.

$a_q < b$, porque $a_q b^q < n < b^{q+1}$.

Quando $r = 0$, $n = 0b^0 + 0b_1 + 0b^2 + \ldots + a_q b^q$, e a existencia da representação fica estabelecida para este caso.

Quando $r > 0$, sabemos que $r < n$ e portanto, pela hipótese de indução, r tem representação na base b:

$$r = d_0 b^0 + d_1 b_1 + d_2 b^2 + \ldots + d_t b^t,$$

[4] Por ora presumimos que quociente e resto inteiros existem, e que o resto é menor que n. A dmonstração rigorosa disso é dada no Capítulo 4

com $0 \leq d_i < b$ e $t \leq a$. Retomamos a Equação 3.1,

$$\begin{aligned} n &= r + a_q b^q, \\ &= \left(d_0 b^0 + d_1 b_1 + d_2 b^2 + \ldots + d_t b^t \right) + a_q b^q, \end{aligned}$$

que é a representação de n na base b – e a existência fica estabalecida para todos os casos.

Para a unicidade, presuma que n tem duas representações na base b,

$$\begin{aligned} n &= e_0 + e_1 b + e_2 b^2 + \ldots + e_g b^g, + \ldots + f_h b^h \quad 0 \leq e_i < b \\ n &= f_0 + f_1 b + f_2 b^2 + \ldots + f_h b^h, \quad 0 \leq f_i < b. \end{aligned}$$

onde evidentemente (e sem perda de generalidade) que $g \leq h$.

Subtraímos as duas representações, e devemos obter zero:

$$(e_0 - f_0) + (e_1 - f_1)b + (e_2 - f_2)b^2 + \ldots + (e_h - f_h)b^h = 0.$$

Denotamos $e_i - f_i$ por w_i, e temos

$$w_0 + w_1 b + w_2^2 + \ldots + w_h b^h = 0. \tag{3.2}$$

Considere o maior índice s tal que $e_s \neq f_s$ (ou seja, descarte a parte direita da soma onde os coeficientes são idênticos).

Se $s = 0$ (se descartamos todos os termos menos o primeiro), então $e_0 = f_0 = 0$, e as representações são idênticas.

Presumimos portanto $s > 0$. Como $0 \leq e_i < b$ e $0 \leq f_i < b$, temos

$$|w_i| = |e_i - f_i| \leq b - 1, \tag{3.3}$$

e reescrevemos a Equação 3.2 como

$$w_h b^h = -\left(w_0 + w_1 b + w_2^2 + \ldots + w_{h-1} b^{h-1} \right).$$

$$\begin{aligned} b^h &\leq \left| w_h b^h \right| \\ &= \left| w_0 + w_1 b + \cdots + w_{h-1} b^{h-1} \right| \\ &\leq |w_0| + |w_1 b| + \cdots + \left| w_{h-1} b^{h-1} \right| \\ &\leq (b-1) + (b-1)b + \cdots + (b-1)b^{h-1} \qquad \text{(por 3.3)} \\ &\leq (b-1)(1 + b + \cdots + b^{h-1}) \\ &= b^h - 1, \end{aligned}$$

o que é uma contradição. Concluímos que $g = h$ e $e_i = f_i$ para todo i, e as representações são idênticas. □

3.2 Racionais

A representação em diferentes bases também é possível para racionais, bastando que usemos expoentes negativos. Na base dez, um número racional é representado por

$$\underbrace{10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + 10^0 d_0}_{\text{parte inteira}} + \underbrace{10^{-1} f_1 + 10^{-2} f_2 + \cdots + 10^{-r} f_r}_{\text{parte fracionária}}.$$

Por exemplo,

$$\begin{aligned}(2)10^2 + 0(10^1) + 3(10) \ + \ (5)10^{-1} + (1)10^{-2} &= 200 + 0 + 3 \ + \ (5)\frac{1}{10} + \frac{1}{100} \\ &= 203,51 \\ &= \frac{20351}{100}\end{aligned}$$

Na base dois, o número $110,01$ representa

$$\begin{aligned}(1)2^2 + (1)2^1 + (0)2^0 \ + \ (0)2^{-1} + (1)2^{-2} &= 4 + 2 + 0 \ + \ (0)\frac{1}{2} + \frac{1}{4} \\ &= 6,25 \\ &= \frac{625}{100} \\ &= \frac{25}{4}\end{aligned}$$

Exercícios

Ex. 14 — Escreva o número 543 na base 4 e o número 111 na base 5.

Ex. 15 — Mostre como é possível representar qualquer número natural em base 1, desde que se abra mão do dígito zero (o que inclui abrir mão de representar a quantidade zero também).

Ex. 16 — Um número com mais de um dígito pode ter a mesma representação em duas bases? Mostre exemplo ou prove que não é possível.

Ex. 17 — Prove que, na base dez, o último dígito de um quadrado perfeito só pode ser $0, 1, 4, 5, 6$ ou 9.

Ex. 18 — Para quais valores de n, inteiro positivo, o número $1! + 2! + 3! + \cdots + n!$ é quadrado perfeito?

Ex. 19 — Prove que qualquer número palíndromo na base dez, com quantidade par de dígitos, é divisível por onze.

Ex. 20 — Desenvolva a prova do Teorema 3.1.

Ex. 21 — Há um sistema posicional não padrão chamado de *ternário balanceado*. A base é 3, mas os coeficientes (dígitos) usados são $-1, 0, 1$. Pode-se denotar o dígito -1 por $\underline{1}$. Por exemplo:

$$\begin{aligned} \underline{1}1\underline{1}0 &= (-1)3^3 + (1)3^2 + (-1)3^1 + 0(3^0) \\ &= -27 + 9 - 3 + 0 \\ &= -21 \end{aligned}$$

A tabela a seguir dá outros exemplos.

base 10	ternário balanceado
$\vdots$	
-5	$\underline{1}11$
$\vdots$	
-1	$\underline{1}$
0	0
1	1
2	$1\underline{1}$
3	10
4	11
5	$1\underline{11}$
$\vdots$	

(a) Escreva os números $-3, -8, +8, +11$ em representação ternária balanceada.

(b) Prove que se a representação ternária balanceada de $-n$ é igual à de n, trocando-se apenas os sinais dos coeficientes (ou seja, trocando 1 por $\underline{1}$ e vice-versa).

(c) Prove que esta representação permite expressar todos os inteiros.

(d) Prove que a representação ternária balanceada de um número inteiro é única.

(e) É possível representar racionais em base ternária balanceada? Mostre como, ou prove que não é possível.

Ex. 22 — Quantos dígitos são necessários para representar o número $n \in \mathbb{N}$ na base k?

Ex. 23 — A representação de racionais em sistema posicional com vírgula é única em qualquer base? Se há exceções, quais são?

Ex. 24 — Que números são representáveis, usando o sistema posicional, por uma base racional (e não inteira) m/n, com $m, n \in \mathbb{Z}$? Por exemplo, se a base é $2/3$, números seriam da forma

$$a_0 + a_1\frac{2}{3} + a_2\left(\frac{2}{3}\right)^2 + a_3\left(\frac{2}{3}\right)^3 + \cdots$$

O conjunto é infinito, mas é igual a $\mathbb{R}$? Igual a $\mathbb{Q}$? Ou, pode-se pelo menos determinar algum conjunto de números que certamente é (ou não é) representável?

Ex. 25 — Usando dez dígitos, $0, 1, \ldots, 9$, e vinte e seis letras, $A, B, \ldots, Z$, é possível escrever números em base 36, usando um dos 36 símbolos em cada posição. Assim, os dígitos tem seus valores usuais, e as letras valem

A	B	C	$\cdots$	X	Y	Z
10	11	12	$\cdots$	33	34	35

Desta forma, a representação do número 157 em base 36, usando o esquema descrito, é 4D, porque

$$\begin{aligned}(4)36^1 + (D)36^0 &= (4)36^1 + (13)36^0\\ &= 144 + 13\\ &= 157.\end{aligned}$$

Agora, na base 36, o quadrado de

$$\underbrace{11111111111111111111111111111111111}_{35\text{ uns}}$$

é o palíndromo

$$1234567\,89ABCDE\,FGHIJKL\,MNOPQRS\,TUVWXY\,Z$$
$$YXWVUT\,SRQPONM\,LKJIHGF\,EDCBA98\,7654321$$

Isso pode ser generalizado para qualquer base? Se não for verdade, mostre contraexemplo. Se for verdade, formalize e demonstre.

Ex. 26 — Seja $111\ldots111$ a representação de um natural n na base k, sendo k maior que a quantidade de uns na representação de n. Qual é a representação de n^3 na mesma base? Demonstre.

Ex. 27 — Existe um sistema de representação de números chamado de *representação binária com ponto fixo*, que é uma variante da representação de racionais que abordamos neste capítulo. A representação usa zeros e uns; um número tem n dígitos antes do ponto decimal, e m dígitos depois

dele. O número

$$a_{n-1} \dots a_2 a_1 a_0 \, . \, a_{-1} a_{-2} \dots a_{m-1} a_{-m}$$

é igual (da mesma forma que na representação binária de inteiros) a

$$\sum_{-m \leq i \leq n-1} a_i 2^i$$

Por exemplo, com $n = 3$ e $m = 2$,

$$\begin{aligned} 101.011 &= 1(2^2) + 0(2^1) + 1(2^0) \;\; + \;\; 0(2^{-1}) + 1(2^{-2}) + 1(2^{-3}) \\ &= 4 + 0 + 1 \;\; + \;\; 0 + \frac{1}{4} + \frac{1}{8} \\ &= 5 + \frac{3}{8} \\ &= 5.375. \end{aligned}$$

a) Mostre que se m e n forem fixos, as operações de soma e multiplicação não são associativas.

b) Tome $m = 3$ e $n = 6$. Tente dar uma estimativa do erro, $|(ab)c - a(bc)|$, em função de a, b.

Ex. 28 — Há uma *Lei de Newcomb-Benford*, que afirma que os números em certos conjuntos de dados que surgem naturalmente apresentam a seguinte propriedade: a distribuição do **primeiro** dígito é dada pela *distribuição de Newcomb-Benford*[5]

$$\Pr(d) = \log_{10}\left(1 + \frac{1}{d}\right),$$

ou seja,

$$\begin{aligned} \Pr(1) &\approx 0.301 \\ \Pr(2) &\approx 0.176 \\ \Pr(3) &\approx 0.125 \\ \Pr(4) &\approx 0.097 \\ &\vdots \end{aligned}$$

[5] Em 1881 o astrônomo Simon Newcomb observou que os livros com tabelas de logaritmos tinham páginas iniciais muito mais desgastadas do que as finais, e que portanto os números iniciando com 1 eram mais frequentemente buscados – e portanto ocorriam mais frequentemente. Newcomb chegou a determinar as probabilidades para os primeiros e segundos dígitos de números, e terminou seu artigo mencionando que "É curioso observar que esta lei nos permitiria decidir se uma grande coleção de resultados numéricos independentes foi composta por números naturais ou logaritmos.". Observações semelhantes foram feitas em 1938 por Frank Benford, com números de diferentes origens.

Prove que esta propriedade, quando presente em um conjunto de números, é invariante por base (ou seja, se um conjunto de números apresenta esta propriedade, e todo o conjunto for reescrito em base diferente da base 10, a Lei de Benford continuará valendo, exceto que o logaritmo deverá ser tomado na nova base, e não na base dez).

Capítulo 4

Divisibilidade

Neste Capítulo, após definir divisão, tratamos do conhecido conceito de "máximo denominador comum", e apontamos um caso onde ele é relevante fora do anel dos inteiros.

Nos enunciados deste Capítulo não incluímos a usual qualificação de elementos como inteiros ("$a, b \in \mathbb{Z}$"). Podemos presumir que *todos* os elementos são inteiros, a não ser que determinemos o contrário. Mais ainda, pode-se ler o Capítulo como se todos estes elementos fossem membros de um anel ordenado comutativo com unidade. Eventualmente damos exemplos usando o anel $\mathbb{R}[x]$ sem abordar ordem. Na Seção 4.6 trataremos de outras estruturas.

4.1 Divisão

A noção de divisibilidade é fundamental.

Definição 4.1 (divisibilidade)**.** Dizemos que a **divide** b (denotamos $a \mid b$) se existe c tal que $ac = b$. Quando a não divide b, denotamos $a \nmid b$. ♦

Da definição concluímos que *zero divide zero* ($0 \mid 0$), porque existem infinitos c tal que $0c = 0$. No entanto, justamente por haver infinitas possibilidades para c, não definimos *a operação de divisão* de zero por zero. Isto pode ficar mais claro se não lermos "$a \mid b$" como "a divide b", mas como "a tem múltiplo b".

Como exemplo em $\mathbb{Z}$, $3 \mid 15$ porque $3(5) = 15$; já $4 \nmid 10$, porque não existe inteiro k tal que $4k = 10$.

Para um exemplo no anel $\mathbb{R}[x]$ (polinômios na variável x com coeficientes em $\mathbb{R}$), temos $(x-1) \mid (x^3 - x^2)$, porque

$$(x-1)x^2 = x^3 - x^2.$$

Em $\mathbb{Z}$, $4 \mid 20$, porque $4(5) = 20$.

O seguinte Teorema trata de alguns fatos básicos a respeito de divisibilidade, e é deixado como exercício.

Teorema 4.2. *Para todos* a, b, c*:*

(i) *Se* $a \mid b$ *então* $a \mid bc$.

(ii) *A relação* $\mid$ *é transitiva.*

(iii) *Se* $a \mid b$ *e* $b \mid a$*, então* $a = \pm b$.

(iv) *Se* $b \neq 0$ *e* $a \mid b$ *então* $|a| \leq |b|$.

(v) *Se* $m \neq 0$ *então* $a \mid b$ *se e somente se* $ma \mid mb$.

(vi) *Se* $a \neq 0$ *e* $a \mid (b + c)$*, então* $a \mid b$ *se e somente se* $a \mid c$

O Lema a seguir é simples, mas bastante útil.

Lema 4.3. *Se* $a \mid b$ *e* $a \mid c$*, então* $a \mid (xb + yc)$.

Demonstração. Pela definição de divisibilidade, se $a \mid b$ e $a \mid c$ então há m, n tais que $ma = b$ e $na = c$. Então

$$\begin{aligned} xb + yc &= x(ma) + y(na) \\ xb + yc &= a(xm + yn) \\ a &\mid (xb + yc) \end{aligned}$$

□

O Teorema a seguir trata da divisibilidade de somas e diferenças de potências, e será importante mais adiante.

Teorema 4.4. *Para todo* $n \in \mathbb{N}$ *e para todos* a, b, c*,*

(i) $(a - b) \mid (a^n - b^n)$

(ii) $(a + b) \mid a^{2^n+1} + b^{2^n+1}$

(iii) $(a - b) \mid a^{2n} - b^{2n}$

Demonstração. Demonstramos apenas (i); os outros dois itens são exercícios.
(i) Por indução em n: $(a - b) \mid (a^0 - b^0) = 0$, porque todos dividem o zero; A hipótese é $(a - b) \mid (a^n - b^n)$.

$$\begin{aligned} a^{n+1} - b^{n+1} &= aa^n - bb^n \\ &= aa^n - ba^n + ba^n - bb^n \\ &= (a - b)a^n + b(a^n - b^n) \\ &= X(a - b) + Y(a^n - b^n) \\ &= X(a - b) + Z(a - b) \qquad \text{(por hipótese, } (a - b) \mid (a^n - b^n)\text{)} \\ &= (X + B)(a - b), \end{aligned}$$

e portanto $(a-b) \mid (a^{n+1}-b^{n+1})$. □

O Teorema da Divisão garante que sempre há como efetuar a divisão com resto de a por b, resultando em um quociente q e resto r.

Teorema 4.5 (da Divisão)**.** $\forall b \neq 0, a$*, existem* q, r *únicos tais que* $a = qb+r$*, com* $0 \leq r < |b|$.

Demonstração. Primeiro determinamos a existência de r e q. O resto, r, deve ser não-negativo e da forma $a - qb$; considere então todos os números da forma $a + kb$,

$$S = \{\ldots, a-3b, a-2b, a-b, a, a+b, a+2b, a+3b, \ldots\} \tag{4.1}$$

Tome o subconjunto de S contendo somente os elementos não-negativos. Este conjunto é subconjunto de $\mathbb{N}$, e portanto, pelo princípio da boa ordem, contém um menor elemento, a quem chamamos de r. A partir de r podemos imediatamente computar o quociente q.

Provamos que $r < |b|$: suponha que o r encontrado seja maior ou igual a $|b|$. Então

$$r' = r - |b|$$

também seria da mesma forma, e não é negativo (porque $r \geq |b|$). Logo, r não era o menor não-negativo do conjunto, como presumido inicialmente.

Falta demonstrar a unicidade de q e r. Presumiremos que também há q'' e r'' tais que $a = qb'' + r''$, e mostraremos que $r'' = r$, o que por sua vez implica que $q'' = q$.

Se há dois restos r, r'', então sem perda de generalidade, presumimos que $r < r''$, e portanto

$$0 < r'' - r < |b|.$$

Agora, temos duas expressões para a:

$$a = qb + r, \quad a = q''b + r''.$$

Estas nos dão fórmulas para r e r'':

$$r = a - qb, \quad r'' = a - q''b.$$

Calculamos $r'' - r$, e obtemos $(a-q''b)-(a-qb) = qb-q''b = b(q-q'')$, e portanto $b \mid (r''-r)$. como sabemos que tanto r como r'' são nào-negativos e estritamente menores que $|b|$, então

$$-b < r'' - r < b,$$

e o único múltiplo de b que poderia ser $r'' - r$ é zero. Logo, $r'' = r$ e $q'' = q$. □

Tendo provado que sempre é possível dividir dois inteiros (ou dois elementos de um anel comutativo), podemos definir a operação de divisão.

Definição 4.6 (divisão)**.** Dizemos que a **divisão** de a por b resulta em **quociente** q com **resto** r quando $a = qb + r$. ♦

Exemplo 4.7. A divisão de 13 por 5 resulta em quociente 2, com resto 3, porque $13 = 2(5) + 3$. ◀

4.2 Máximo Divisor Comum

Definimos agora o máximo divisor comum entre dois ou mais elementos, e apresentamos o algoritmo de Euclides para calculá-lo. O MDC é o maior elemento que divide um conjunto de elementos – isto fica definido com mais clareza a seguir.

Definição 4.8 (máximo divisor comum)**.** d é o **máximo divisor** comum de a e b se

(i) d não é negativo;

(ii) $d \mid a$, $d \mid b$;

(iii) se $k \mid a$ e $k \mid b$, então $k \mid d$. ♦

Exemplo 4.9. Em $\mathbb{Z}$, temos $\operatorname{mdc}(28, 12) = 4$, porque $4 \mid 28$, $4 \mid 12$, mas os únicos outros números que dividem 28 e 12 são 1 e 2 – e ambos dividem 4. ◀

Teorema 4.10. *Se* a, b *são não nulos, então* $\operatorname{mdc}(a, b)$ *é único.*

Demonstração. Suponha que existam dois números satisfazendo a definição de $\operatorname{mdc}(a, b)$, d_1 e d_2. Pela mesma definição, como $d_2 \mid a$ e $d_2 \mid b$, então $d_2 \mid d_1$. Mas semelhantemente, $d_1 \mid d_2$. Como os dois são positivos, $d_2 \mid d_1$ e $d_1 \mid d_2$ implica que $d_1 = d_2$. □

Note que o final da demonstração não é válido para qualquer anel: em $\mathbb{R}[x]$, considere os polinômios x e $2x$. Temos $x \mid 2x$, também $2x \mid x$, e $x \neq 2x$. Neste caso, não valerá a unicidade do MDC.

Definição 4.11 (combinação linear inteira)**.** Uma **combinação linear inteira** de dois elementos a e b é $xa + yb$, onde $x, y \in \mathbb{Z}$. ♦

Lema 4.12 (de Bezout)**.** *Para todos* $a, b \in \mathbb{Z}$*,* $\operatorname{mdc}(a, b)$ *é combinação linear inteira de* a *e* b *– ou seja, existem* $x, y \in \mathbb{Z}$ *tais que* $\operatorname{mdc}(a, b) = xa + yb$*.*

Demonstração. Seja $S = \{xa + yb \ : \ x, y \in \mathbb{Z}\}$. Seja z menor elemento positivo de S. Então existem $x, y \in \mathbb{Z}$ tais que $z = xa + yb$.

Agora presuma que $z \nmid b$. Então a divisão de b por z deve ter resto diferente de zero, ou seja, $b = qz + r$, $0 < r < z$. Logo,

$$\begin{aligned} r &= b - qz \\ &= b - q(xa + yb) \\ &= b - qxa - qyb \\ &= (1 - qy)b - (qx)a \\ &\in S. \end{aligned}$$

Mas como $r \in S$, e $r < z$, temos uma contradição, porque havíamos tomado z como o *menor* elemento positivo de S. Desta forma negamos nossa suposição e concluímos que $z \mid b$. O argumento que fizemos para b pode ser repetido para a, obtendo $z \mid a$.

Agora temos um elemento (z) que divide tanto a como b, e que é não negativo. Falta mostrar que se $k \mid a$ e $k \mid b$, então $k \mid z$, o que segue imediatamente porque $z = xa + yb$. □

Exemplo 4.13. O MDC de 24 e 36 é 12, que é combinação linear de 24 e 36:

$$(-1)24 + (+1)36 = 12,$$

onde os coeficientes de Bezout são -1 e $+1$.

O MDC de 93 e 306 é 3, que é combinação linear de 93 e 306:

$$(-23)93 + (+7)306 = 3,$$

e os coeficientes de Bezout são -23 e $+7$. ◄

Corolário 4.14. $\mathrm{mdc}(a, b)$ *é o menor valor dentre todas as combinações lineares inteiras de* a *e* b*:*

$$\mathrm{mdc}(a, b) = \min_{x,y \in \mathbb{Z}} \{xa + yb\}.$$

Corolário 4.15. *A equação* $ax + by = c$ *tem solução se e somente se* $\mathrm{mdc}(a, b) \mid c$.

Demonstração. Suponha que $ax + by = c$, e que $d = \mathrm{mdc}(a, b)$. Como $d \mid a$ e $d \mid b$, então $d \mid (ax + by) = c$.

Agora, se $\mathrm{mdc}(a, b) = d \mid c$, então $c = nd$. Mas pelo Corolário 4.14 deve haver w, z tais que $aw + bz = d$, e portanto $a(wn) + b(zn) = nd = c$. □

O Exercício 44 pede a demonstração do Teorema 4.16, que nos será útil adiante.

Teorema 4.16. *Para todos* a, b, m, $\mathrm{mdc}(ma, mb) = m\big(\mathrm{mdc}(a, b)\big)$.

Exemplo 4.17. Sejam $a = 10$, $b = 25$ e $m = 3$.

$$\mathrm{mdc}(a, b) = \mathrm{mdc}(10, 25) = 5,$$

portanto

$$\begin{aligned}\mathrm{mdc}(ma, mb) &= \mathrm{mdc}((3)10, (3)25)\\ &= \mathrm{mdc}(30, 75)\\ &= 15\\ &= (3)(5)\\ &= m(\mathrm{mdc}(ma, mb)).\end{aligned}$$ ◀

Teorema 4.18. *Se* $\mathrm{mdc}(b, c) = 1$ *e* $c \mid ab$ *então* $c \mid a$.

Demonstração. Do enunciado,

$$\begin{aligned}\mathrm{mdc}(b, c) &= 1\\ a\,\mathrm{mdc}(b, c) &= a\\ \mathrm{mdc}(ab, ac) &= a \qquad \text{(Teorema 4.16)}\end{aligned}$$

O enunciado determina que $c \mid ab$; temos também que $c \mid ac$, pela definição de divisibilidade; logo, c é divisor de ab e ac. Mas $\mathrm{mdc}(ab, ac)$ é a, e pela definição de MDC, todos os outros divisores de ab dividem a. Logo, $c \mid a$. □

Exemplo 4.19. Sejam $b = 15$ e $c = 14$. Os dois números são coprimos – $\mathrm{mdc}(a, b) = 1$, portanto para todo a, se $c \mid ab$ então $c \mid a$. Tomamos como exemplo $a = 28$:

$$c \mid (ab) \quad \text{ou seja,} \quad (\ 14 \mid 28(b)\ ),$$

portanto $c \mid a$, ou ainda, $14 \mid 28$ (sim, $2(14) = 28$). ◀

Lema 4.20 (de Euclides)**.** *Se* p *é primo e* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$.

Demonstração. Suponha que $p \mid ab$. Se $p \mid a$, o resultado é imediato. Então, suponha que $p \nmid a$, e considere $d = \mathrm{mdc}(a, p)$. Pela definição de MDC, $d \mid p$, portanto d só pode ser 1 ou p. Se $d = p$, então teríamos, pela definição de MDC, $d \mid a$, ou seja, $p \mid a$ – mas já presumimos que $p \nmid a$, portanto $d = \mathrm{mdc}(a, p) = 1$.

Assim, tendo presumido que $p \nmid a$, pelo Teorema 4.18, $p \mid b$. □

Lema 4.21. *Se* $\mathrm{mdc}(a, b) = 1$*, então* $\mathrm{mdc}(a, bc) = \mathrm{mdc}(a, c)$.

A seguir apresentamos duas demonstrações, idênticas exceto por um parágrafo, onde uma delas usa o Lema de Euclides (Lema 4.20) e a outra usa coeficientes de Bezout (Lema 4.12).

Demonstração. (usando o Lema de Euclides). Se $\mathrm{mdc}(a, bc) = 1$ terminamos. Presuma, portanto, que $\mathrm{mdc}(a, bc) > 1$ (ou seja, existe inteiro maior que um, dividindo a e bc).

Seja $d > 1$, tal que $d = \mathrm{mdc}(a, bc)$. Temos que $d \mid a$, e $d \mid bc$.

> De acordo com o Lema de Euclides, uma vez que $d \nmid b$ é necessário que $d \mid c$.

Também fica claro que, se algum $e \mid a$ e $e \mid c$, então $d \mid e$ (porque definimos $d = \mathrm{mdc}(a, b)$), e portanto se houver algum e que divida a e c, ele deve dividir d. □

Demonstração. (usando coeficientes de Bezout). Se $\mathrm{mdc}(a, bc) = 1$ terminamos. Presuma, portanto, que $\mathrm{mdc}(a, bc) > 1$ (ou seja, existe inteiro maior que um, dividindo a e bc).

Seja $d > 1$, tal que $d = \mathrm{mdc}(a, bc)$. Temos que $d \mid a$, e $d \mid bc$.

> Agora, pelo Lema de Bezout, se $\mathrm{mdc}(a, b) = 1$ então existem X, Y, tais que
>
> $$aX + bY = 1$$
> $$aXc + bYc = c$$
>
> Como $d \mid a$ e $d \mid bc$, o Lema 4.3 determina que d divide o lado esquerdo. Sendo o lado esquerdo igual ao direito, $d \mid c$.

Também fica claro que, se algum $e \mid a$ e $e \mid c$, então $d \mid e$ (porque definimos $d\,\mathrm{mdc}(a, b)$), e portanto se houver algum e que divida a e c, ele deve dividir d. □

4.3 Algoritmo de Euclides para cálculo do MDC

Passamos agora ao algoritmo de Euclides, usado para calcular o MDC de dois (ou mais) números. O algoritmo é dado na forma de função recursiva.

Teorema 4.22 (algoritmo de Euclides)**.** *Sem perda de generalidade, presuma que* $a > b$*, e que* $a = qb + r$*. Então*

$$\mathrm{mdc}(a, b) = \begin{cases} |b| & \text{se } b \mid a \\ \mathrm{mdc}(b, r) & \text{se } b \nmid a \end{cases}$$

Note que usamos o valor absoluto de b, que pode não fazer sentido em qualquer anel (mas é definido em $\mathbb{Z}$).

Demonstração. Começamos pelo primeiro caso, $b \mid a$. Temos também $b \mid b$. Falta mostrar que para todo k, se $k \mid a$ e $k \mid b$, então $k \mid b$ – o que é evidente.

No segundo caso, $b \nmid a$, logo $r \neq 0$. Se calcularmos

$$d = \text{mdc}\,(b, r)$$

temos

(I) $d \mid b$ e $d \mid r$;

(II) se $k \mid b$, $k \mid r$, então $k \mid d$.

Agora analisamos:

(i) de (I), temos $d \mid (qb + r)$, logo $d \mid a$. Também de (I), $d \mid b$;

(ii) suponha que $k \mid a$ e $k \mid b$. Então

$$\begin{aligned} k &\mid (qb + r) \\ kS &= qb + r && \text{(definição de } \mid) \\ kS &= q(kT) + r && (k \mid b) \\ k(S - qkT) &= r \\ k &\mid r && \text{(definição de } \mid) \end{aligned}$$

e portanto, $k \mid a$ e $k \mid b$ implica que $k \mid r$. Mas por (II), se $k \mid b$, $k \mid r$ então $k \mid d$.

Os itens (i) e (ii) acima mostram que $\text{mdc}\,(b, r)$ será igual a $\text{mdc}\,(a, b)$. □

Este Teorema nos dá um algoritmo recursivo para calcular o MDC de dois números. No entanto, não está claro que o algoritmo para. O exercício 39 pede esta demonstração. Pode-se usar o fato de que o maior resto possível em cada divisão é menor que no passo anterior, e que não pode haver restos não-inteiros ou não-positivos.

Exemplo 4.23. Calculamos o MDC de 624 e 162 usando o algoritmo de Euclides.

$$\begin{aligned} \text{mdc}\,(162, 624) &= \text{mdc}\,(162, 138) && \text{(624 = (3)162+138)} \\ &= \text{mdc}\,(138, 24) && \text{(162 = (1)138+24)} \\ &= \text{mdc}\,(24, 18) && \text{(138 = (5)24+18)} \\ &= \text{mdc}\,(18, 6) && \text{(24 = (1)18+6)} \\ &= 6. && \text{(6|18)} \end{aligned}$$

O algoritmo precisou de quatro passos. ◀

Teorema 4.24. *A quantidade de iterações do algoritmo de Euclides para cálculo do MDC é finita.*

Há outro algoritmo para cálculo do MDC, que não usa a operação de divisão.

Teorema 4.25. *Para quaisquer* a, b*,*

$$\operatorname{mdc}(a,b) = \begin{cases} |a| & \text{se } a = b \\ \operatorname{mdc}(a\text{-}b, b) & \text{se } a > b \\ \operatorname{mdc}(a, b\text{-}a) & \text{se } a < b \end{cases}$$

Exemplo 4.26. Calculamos o MDC de 624 e 162 usando o algoritmo com subtrações.

$$\begin{aligned} \operatorname{mdc}(162, 624) &= \operatorname{mdc}(162, 624) \\ &= \operatorname{mdc}(162, 462) \\ &= \operatorname{mdc}(162, 300) \\ &= \operatorname{mdc}(138, 24) \\ &= \operatorname{mdc}(114, 24) \\ &= \operatorname{mdc}(90, 24) \\ &= \operatorname{mdc}(66, 24) \\ &= \operatorname{mdc}(42, 24) \\ &= \operatorname{mdc}(18, 24) \\ &= \operatorname{mdc}(18, 6) \\ &= \operatorname{mdc}(12, 6) \\ &= \operatorname{mdc}(6, 6) \\ &= 6. \end{aligned}$$

◀

4.3.1 Coeficientes de Bezout: algoritmo estendido de Euclides

O Lema 4.12 (Lema de Bezout) afirma que se $\operatorname{mdc}(a, b) = d$, então existem inteiros x e y tais que $ax + by = d$. Uma modificação no algoritmo de Euclides para cálculo do MDC pode identificar os coeficientes x e y, como vemos a seguir.

O algoritmo de Euclides pode ser descrito da seguinte forma: iniciando

com

$$\begin{aligned} r_0 &= a, \\ r_1 &= b, \end{aligned}$$

calculamos

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n + 0. \end{aligned}$$

O MDC de a e b (ou seja, o MDC de r_0 e r_1) é r_n.

Podemos usar a penúltima linha para escrever $\text{mdc}\,(a, b) = r_n$ em função de a e b, realizando substituições para trás. Por exemplo, para calcular o MDC de 108 e 33 fazemos

$$\begin{aligned} 108 &= 3(33) + 9 \\ 33 &= 3(9) + 6 \\ 9 &= 1(6) + 3 \\ 6 &= 2(3) + 0 \end{aligned}$$

e concluímos que $\text{mdc}\,(108, 33) = 3$. Queremos os coeficientes de Bezout na equação $108x + 33y = 3$. Notamos que da penúltima linha de nosso cálculo podemos extrair uma expressão do MDC, 3:

$$3 = 9 - 1(6)$$

Continuamos agora, usando as linhas anteriores para expressar 9 e $1(6)$, até chegarmos a uma expressão de 3 em função de 108 e 33:

$$\begin{aligned} 3 &= 9 - 1(6) \\ &= 108 - 3(33) - 1(6) \\ &= 108 - 3(33) - 1[33 - 3(9)] \\ &= 108 - 3(33) - 33 + 3(9) \\ &= 108 - 4(33) + 3[108 - 3(33)] \\ &= 4(108) - 13(33). \end{aligned}$$

Os coeficientes de Bezout são 4 e -13:

$$4(108) - 13(33) = 3.$$

No entanto, podemos fazer melhor que isso. Observando o algoritmo de Euclides e o processo de substituição para trás que fizemos, percebemos que sempre podemos escrever o i-ésimo resto, r_i, em função de valores obtidos anterioremente.

$$\begin{aligned} r_{i-1} &= qr_i + r_{i+1} \\ r_{i+1} &= r_{i-1} - qr_i \end{aligned}$$

Se tentarmos manter, desde o início, r_i em função de a e b, no final do cálculo teremos os coeficientes de Bezout.

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \\ &= (ax_{i-1} + by_{i-1}) - q_i(ax_i + bx_i) \\ &= ax_{i-1} - qax_i + by_{i-1} - qby_i \\ &= a(x_{i-1} - q_i x_i) + b(y_{i-1} - qy_i) \\ &= ax_{i+1} + by_{i+1} \end{aligned}$$

Então, como $r_{i+1} = ax_{i+1} + by_{i+1}$, os coeficientes de Bezout na iteração $i+1$ devem ser

$$x_{i+1} = x_{i-1} - q_i x_i \tag{4.2}$$

$$y_{i+1} = y_{i-1} - q_i y_i \tag{4.3}$$

Os valores iniciais de x e y podem ser $x_0 = 1, x_1 = 0$ e $y_1 = 0, y_1 = 1$, porque

$$\begin{aligned} r_0 &= a = 1a + 0b && (x_0 = 1, y_0 = 0) \\ r_1 &= b = 0a + 1b && (x_1 = 0, y_1 = 1) \end{aligned}$$

Calculamos o MDC de 48 e 26. No desenvolvimento a seguir, o lado esquerdo mostra o algoritmo básico de Euclides. O lado direito tem os coeficientes x_i e y_i, que são atualizados conforme as equações 4.2 e 4.3.

r_{i-1}	$= q_i r(i)$	$+ r_{i+1}$	x_i	y_i	i
		48	1	0	0
48	$= 1(26)$	$+22$	0	1	1
26	$= 1(22)$	$+4$	1	-1	2
22	$= 5(4)$	$+2$	-1	2	3
4	$= 2(2)$	$+0$	6	-11	4

A última linha tem $r_4 = 2$, que é o MDC de 48 e 26; dali também extraímos

os coeficientes de Bezout, $x_4 = 6$ e $y_4 = -11$. Confirmamos:

$$6(48) - 11(26) = 2.$$

Este cálculo pode ser simplificado em uma tabela como a próxima, que mostra o índice das cinco iterações, i, e os valores r_i, q_i, x_i e y_i.

$$\longrightarrow$$

i	0	1	2	3	4	5
r_i	48	26	22	4	2	
q_i		1	1	5	2	
x_i	1	0	1	-1	6	
y_i	0	1	-1	2	-11	

Obtivemos novamente os mesmos coeficientes de Bezout, $x = 6$ e $y = -11$.

4.4 Mínimo Múltiplo Comum

O conceito de mínimo múltiplo comum é simétrico ao de máximo múltiplo comum.

Definição 4.27 (mínimo múltiplo comum)**.** O **mínimo múltiplo comum** de a e b, denotado $\mathrm{mmc}(a, b)$, é o menor m positivo (exclui-se o zero) que é divisível tanto por a como por b. ♦

Excluímos o zero porque de outra forma, ele seria o mínimo múltiplo comum de todos os pares de números: 0 sempre é divisível por a e b, e é o menor natural.

Teorema 4.28. *Para quaisquer* a, b*, fixe* $m = a$ *e* $n = b$*. Então*

$$\mathrm{mmc}(a, b) = \begin{cases} a & \text{se } a = b \\ \mathrm{mmc}(a + m, b) & \text{se } a > b \\ \mathrm{mmc}(a, b + n) & \text{se } a < b \end{cases}$$

Exemplo 4.29. O MMC dos inteiros 15 e 20 é

$$\begin{aligned}
\operatorname{mmc}(15,20) &= \operatorname{mmc}(15+15,20)\\
&= \operatorname{mmc}(30,20)\\
&= \operatorname{mmc}(30,20+20)\\
&= \operatorname{mmc}(30,40)\\
&= \operatorname{mmc}(30+15,40)\\
&= \operatorname{mmc}(45,40)\\
&= \operatorname{mmc}(45,40+20)\\
&= \operatorname{mmc}(45,60)\\
&= \operatorname{mmc}(45+15,60)\\
&= \operatorname{mmc}(60,60)\\
&= 60.
\end{aligned}$$

◀

O Teorema 4.30 determina uma relação importante entre o MDC e o MMC de dois números. Sua demonstração é pedida no Exercício 53.

Teorema 4.30. $\operatorname{mmc}(a,b)\operatorname{mdc}(a,b) = |ab|$.

Corolário 4.31. *Se* a *e* b *são co-primos,* $\operatorname{mmc}(a,b) = |ab|$.

Corolário 4.32. *Se* $a > 0$*,* $\operatorname{mmc}(a,a+1) = a(a+1)$.

4.5 Números de Fibonacci

A chamada "sequência de Fibonacci" é uma sequência definida recursivamente, descrevendo um fenômeno de crescimento populacional. É conhecida por ter sido descrita por Leonardo Fibonacci (ou "Leonardo de Pisa") em 1202, em seu "Liber Abaci", e de outras maneiras na Grécia e Índia. A alegoria de Fibonacci consistia em coelhos que se reproduziam de maneira cadenciada, mês a mês, sem nunca morrer. Presume-se que há inicialmente um casal de coelhos, e que cada casal fica pronto para reprodução em dois meses. A cada mês, cada casal produz um novo casal. A sequência de números dando as quantidades de casais em cada mês é a chamada *sequência de Fibonacci*.

Definição 4.33 (número de Fibonacci)**.** Seja uma sequência (u_n) definida

da seguinte maneira[1]:

$$\begin{aligned} u_1 &= 1, \\ u_2 &= 1, \\ u_n &= u_{n-1} + u_{n-2}. \end{aligned}$$

Os u_n são chamados de **números de Fibonacci**, e a sequência (u_n) é chamada de **sequência de Fibonacci**. ♦

Lema 4.34. $u_{m(k+1)} = u_{mk+m}$,

Demonstração. Por indução em n. □

Números de Fibonacci podem ser descritos por uma forma fechada, usando a razão áurea, através da fórmula de Euler-Binet.

Definição 4.35 (razão áurea)**.** Denotamos por ϕ a **razão áurea**, solução positiva da equação $x^2 - x - 1 = 0$:

$$\phi = \frac{1+\sqrt{5}}{2}.$$

A segunda raiz da equação é negativa, e denotada $\hat{\phi}$:

$$\hat{\phi} = \frac{1-\sqrt{5}}{2}.$$ ♦

Teorema 4.36 (fórmula de Euler-Binet)**.** *Seja ϕ a razão áurea, e*

$$\hat{\phi} = 1 - \phi = -\frac{1}{\phi}.$$

Então

$$u_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}}.$$

Demonstração. Para a base, usamos u_0 e u_1:

$$\begin{aligned} \frac{\phi^0 - \hat{\phi}^0}{\sqrt{5}} &= \frac{1-1}{\sqrt{5}} = u_0 \\ \frac{\phi^1 - \hat{\phi}^1}{\sqrt{5}} &= \frac{\phi - \hat{\phi}}{\sqrt{5}} \\ &= \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} \\ &= 1 = u_1 \end{aligned}$$

[1] Alguns autores definem de forma alternativa, mas equivalente: $u_0 = 0$; $u_1 = 1$; $u_n = u_{n-1} + u_{n-2}$.

A hipótese de indução é: para todo $i < n$,

$$u_i = \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}}, \quad \text{ou}$$
$$u_i\sqrt{5} = \phi^i - \hat{\phi}^i.$$

Precedemos ao passo. Como tanto ϕ como $\hat{\phi}$ são soluções de $x^2 - x - 1 = 0$, então

$$\phi^2 = 1 + \phi,$$
$$\hat{\phi}^2 = 1 + \hat{\phi}.$$

Agora verificamos que

$$\begin{aligned}
\phi^n - \hat{\phi}^n &= \phi^2\phi^{n-2} - \hat{\phi}^2\hat{\phi}^{n-2} \\
&= (1+\phi)\phi^{n-2} - (1+\hat{\phi})\hat{\phi}^{n-2} \\
&= \phi^{n-2} + \phi^{n-1} - \hat{\phi}^{n-2} - \hat{\phi}^{n-1} \\
&= \left(\phi^{n-2} - \hat{\phi}^{n-2}\right) + \left(\phi^{n-1} - \hat{\phi}^{n-1}\right) \\
&= (u_{n-2} + u_{n-1})\sqrt{5} && \text{(hipótese de indução)} \\
&= u_n\sqrt{5},
\end{aligned}$$

e $u_n = \left(\phi^n - \hat{\phi}^n\right)/\sqrt{5}$. □

A seguir demonstramos diversas propriedades de números de Fibonacci. Dois números consecutivos de Fibonacci são coprimos.

Teorema 4.37. $\text{mdc}(u_n, u_{n+1}) = 1$.

Demonstração. Por indução em n.

A base é, trivialmente, com $n = 1$, já que $\text{mdc}(u_1, u_2) = 1$.

A hipótese de indução é $\text{mdc}(u_n, u_{n\text{-}1}) = 1$.

O passo é muito simples,

$$\begin{aligned}
\text{mdc}(u_{n+1}, u_n) &= \text{mdc}(u_n + u_{n\text{-}1}, u_n) \\
&= \text{mdc}(u_{n\text{-}1}, u_n) \\
&= 1, && \text{(pela hipótese de indução)}
\end{aligned}$$

finalizando a demonstração. □

O Lema 4.38 determina uma propriedade simples de números de Fibonacci. Sua demonstração é bastante simples, e é pedida no Exercício 46

Lema 4.38. *Se* $m, n \geq 1$, $u_m \mid u_{mn}$.

A igualdade de Honsberger será útil na demonstração de um Teorema a respeito do MDC de números de Fibonacci.

Lema 4.39 (igualdade de Honsberger)**.** $u_{m+n} = u_m u_{n+1} + u_{m-1} u_n$.

Demonstração. Por indução em n.

Para a base, fixamos m, e verificamos, para $n = 1$ e $n = 2$ que:

$$\begin{aligned} u_m u_{n+1} + u_{m-1} u_n &= u_m u_{1+1} + u_{m-1} u_1 \\ &= u_m(1) + u_{m-1}(1) && (u_1 = 1, u_2 = 1) \\ &= u_m + u_{m-1} \\ &= u_{m+1} \\ &= u_{m+n}. \end{aligned}$$

$$\begin{aligned} u_m u_{n+1} + u_{m-1} u_n &= u_m u_{2+1} + u_{m-1} u_2 \\ &= u_m(2) + u_{m-1}(1) && (u_2 = 1, u_3 = 2) \\ &= u_m + u_m + u_{m-1} \\ &= u_m + u_{m+1} \\ &= u_{m+2} \\ &= u_{m+n}. \end{aligned}$$

A base é dupla, porque durante o passo usaremos a hipótese duas vezes, uma usando n e outra usando $n-1$, e a validade do passo depende da validade da afirmação para *dois* valores anteriores.

A hipótese de indução, para $n-1$ e n, é

$$u_{m+n-1} = u_m u_n + u_{m-1} u_{n-1}, \tag{4.4}$$

$$u_{m+n} = u_m u_{n+1} + u_{m-1} u_n. \tag{4.5}$$

$$\begin{aligned} u_{m+(n+1)} &= u_{m+n} + u_{m+n-1} \\ &= u_{m+n} + (u_m u_n + u_{m-1} u_{n-1}) && \text{(por 4.4)} \\ &= (u_m u_{n+1} + u_{m-1} u_n) + (u_m u_n + u_{m-1} u_{n-1}) && \text{(por 4.5)} \\ &= u_m (u_{n+1} + u_n) + u_{m-1} (u_n + u_{n-1}) \\ &= u_{m-1} u_{n+1} + u_m u_{n+1}. && \square \end{aligned}$$

Teorema 4.40. $\operatorname{mdc}(u_m, u_n) = u_{\operatorname{mdc}(m,n)}$.

Demonstração. Presumimos, sem perda de generalidade, que $n \geq m$. Então

sejam q, r o quociente e o resto da divisão de n por m:

$$n = qm + r, \quad 0 \leq r < m.$$

Então

$$\begin{aligned} \operatorname{mdc}(u_m, u_n) &= \operatorname{mdc}(u_m, u_{mq+1}u_r + u_{qm}u_{r\text{-}1}) \\ &\qquad\qquad \text{(igualdade de Honsberger 4.39)} \\ &= \operatorname{mdc}(u_m, u_{qm+1}u_r) \qquad (u_m \mid u_{qm}) \\ &= \operatorname{mdc}(u_m, u_r). \qquad \text{(Lema 4.21, Teorema 4.37)} \end{aligned}$$

Se, neste processo, substituirmos $u_m \to m$, $u_n \to n$, $u_q \to q$, $u_r \to r$, teremos uma iteração do algoritmo de Euclides, que eventualmente terminará com o último resto igual ao MDC dos dois números: haverá um passo em que

$$\operatorname{mdc}(u_a, u_b) = \operatorname{mdc}(u_d, 0),$$

e neste momento teremos determinado $\operatorname{mdc}(u_m, u_n) = u_d = u_{\operatorname{mdc}(m,n)}$. □

A demonstração do Teorema 4.41 é tema do Exercício 47. A representação de inteiros como soma de quadrados é, por si mesma, tópico suficientemente relevante para merecer um capítulo inteiro (o Capítulo 10 trata exclusivamente da representação de inteiros como soma de dois, três ou quatro quadrados).

Teorema 4.41. $u_{2n+1} = u_n^2 + u_{n+1}^2$.

Teorema 4.42. $2 \mid u_n$ *se e somente se* $3 \mid n$.

Demonstração. A demonstração é extremamente simples, por indução em n, com passo de três em três.

A base é $2 \nmid u_1 = 1$; $2 \nmid u_2 = 1$; $2 \mid u_3 = 2$.

Por hipótese, suponha que o enunciado valha para todo u_i anterior a u_n. Então, se $3 \mid k$, temos

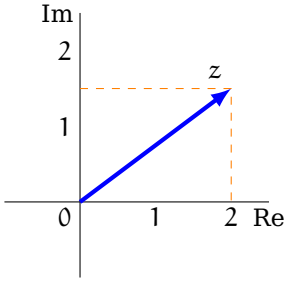
$$\begin{aligned} 2 \mid u_k &= u_{k-1} + u_{k-2}, && \text{(ímpar + ímpar)} \\ 2 \nmid u_{k+1} &= u_k + u_{k-1}, && \text{(par + ímpar)} \\ 2 \nmid u_{k+2} &= u_{k+1} + u_k, && \text{(ímpar + par)} \end{aligned}$$

E o Teorema está demonstrado. □

4.6 Domínios Euclideanos: Inteiros Gaussianos e Polinômios

A demonstração do Teorema da divisão depende de uma relação de ordem (escolhemos o "menor positivo" dentre os números $a - qb$). Em anéis sem ordem total, a demonstração não é válida. Ainda assim, podemos determinar uma ordem parcial em um anel não-ordenado, de forma a tentar obter resultado semelhante.

Identificamos cada número complexo $a + bi$ com o vetor (a, b) em $\mathbb{R}^2$. Assim, a projeção de um vetor (número complexo) no eixo das abscissas identifica a parte real do número; a projeção no eixo das ordenadas identifica a parte imaginária. Damos a este plano o nome de *plano complexo*. A figura a seguir mostra a representação do número $z = 2 + (3/2)i$.



Teorema 4.43. *A multiplicação de um complexo por i resulta em rotação de sua representação no plano por um ângulo de $\pi/2$.*

Demonstração. Usando coordenadas polares, um complexo $re^{i\theta}$, com raio r e ângulo θ no plano. Assim, $i = (1)e^{i(\pi/2)}$, e

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1+\theta_2)},$$

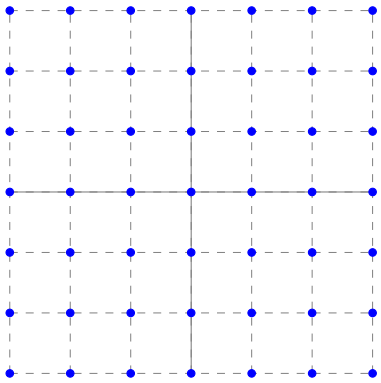
logo

$$\begin{aligned} i\left(re^{i\theta}\right) &= e^{i(\pi/2)}\left(re^{i\theta}\right) \\ &= re^{i(\theta+\pi/2)}. \end{aligned}$$

□

Definição 4.44 (inteiros Gaussianos)**.** Os **inteiros Gaussianos**, denotados $\mathbb{Z}[i]$, são as combinações lineares inteiras de 1 e i, ou seja, números da forma $a + bi$ onde a e b são inteiros e $i^2 = -1$. ♦

Os inteiros Gaussianos são um anel, subconjunto de $\mathbb{C}$ (ou seja, um subanel). No plano complexo, ocupam as coordenadas inteiras.



A noção de divisibilidade em $\mathbb{Z}[i]$ é a mesma para qualquer anel – podemos manter a definição que já temos. Daremos, no entanto, alguns exemplos.

- $-i \mid (-1-2i)$, porque $-i(2-i) = -1-2i$;
- $4-12i \mid 20-20i$, porque $(2+i)(4-12i) = 20-20i$;
- $(3-5i) \nmid (1-i)$, porque $(3-5i)/(1-i) = 11/2+5i/2$, que não tem coeficientes inteiros, e portanto não está em $\mathbb{Z}[i]$.

Claramente, um inteiro n divide um inteiro Gaussiano $a+bi$ se e somente se $n \mid a$ e $n \mid b$.

Definição 4.45 (norma)**.** Definimos **norma**[2] para números complexos como $N(a+bi) = a^2+b^2$. ♦

Exemplo 4.46. A norma de $-3+4i$ é $(-3)^2+(4)^2 = 9+16 = 25$. ◀

Teorema 4.47. *A norma para inteiros Gaussianos é multiplicativa:* $N(\alpha\beta) = N(\alpha)N(\beta)$.

A verificação deste Teorema, pedida no exercício 62, consiste de simples manipulação de fórmulas, sem passos não-triviais.

[2] Usualmente, para vetores em $\mathbb{R}^2$ e para números complexos, define-se a norma como $\sqrt{a^2+b^2}$, *para que o valor da norma coincida com a distância da origem até o ponto associado ao vetor.* No entanto, em Teoria de Números é mais importante *que a norma seja um valor inteiro* – daí a ausência da raiz quadrada.

Exemplo 4.48. Sejam $z = -3 + 4i$ e $w = 2 - 8i$. Então $zw = 26 + 32i$.

$$\begin{aligned} N(-3+4i) &= (-3)^2 + (4)^2 = 9 + 16 = 25 \\ N(2-8i) &= (2)^2 + (-8)^2 = 68 \\ N(zw) &= N(26+32i) \\ &= 26^2 + 32^2 \\ &= 1700 \\ &= (25)(68) \\ &= N(z)N(w). \end{aligned}$$

◀

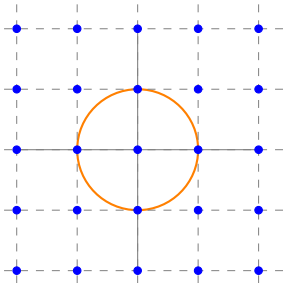
Corolário 4.49. *Há exatamente quatro unidades no anel dos inteiros Gaussianos:* ± 1 *e* $\pm i$.

Demonstração. Da multiplicatividade da norma: para que $\alpha\beta = 1$, é necessário que $N(\alpha)N(\beta) = N(1)$, e como $N(1) = 1$, α e β devem ter norma um. Assim,

$$\begin{aligned} (1)(1) &= 1, \\ (-1)(-1) &= 1, \\ (-i)(i) &= 1. \end{aligned}$$

E temos os inversos $1^{-1} = 1$; $(-1)^{-1} = -1$; e $i^{-1} = -i$. □

As unidades – que tem norma um – são os vetores com coordenadas inteiras no círculo unitário no plano complexo, já que a norma é[3] $a^2 + b^2$.



Teorema 4.50. $\alpha\overline{\alpha} = N(\alpha)$, *para todo inteiro Gaussiano* α, *onde* $\overline{\alpha}$ *é o conjugado complexo de* α.

Exemplo 4.51. Seja $z = -2 + 5i$. A norma de z é $N(z) = (-2)^2 + 5^2 = 29$

[3] Para outros valores, a norma *não* é a distância até a origem, porque abrimos mão da norma Euclideana!

Então

$$\begin{aligned} z\bar{z} &= (-2+5i)(-2-5i) \\ &= 4-25i^2 \\ &= 29 \\ &= N(z). \end{aligned}$$ ◀

A demostração do teorema da divisão não pode ser usada para inteiros Gaussianos, porque nela escrevemos os elementos da forma "$a + kb$", e escolhemos o resto r como o *menor positivo* dentre eles. Não há o conceito de "menor positivo" em $\mathbb{Z}[i]$.

A norma em $\mathbb{Z}[i]$ poderá ser útil, mas precisamos de cuidado: nos inteiros podemos contar com $a \mid b \Rightarrow -a \mid b$, mas isto não é válido para norma de inteiros Gaussianos. Como exemplo: $-2 \mid 10$ e $5 \mid -25$ nos inteiros. Mas em $\mathbb{Z}[i]$, tanto $2-3i$ como $2+3i$ tem norma 13, mas nenhum divide o outro: Os múltiplos de $2-3i$ com a mesma norma são

$$\begin{aligned} (1)(2-3i) &= 2-3i \\ (-1)(2-3i) &= -2+3i \\ (i)(2-3i) &= 3+2i \\ (-i)(2-3i) &= -3-2i \end{aligned}$$

e $2+3i$ não está entre eles! Ou seja, se dois números α e β tem a mesma norma, não necessariamente diferem por multiplicação por unidade ($\alpha = \pm\beta$ ou $\alpha \pm i\beta$). Tomar a norma de um inteiro Gaussiano tem efeito maior sobre um número do que tomar o valor absoluto de um número inteiro.

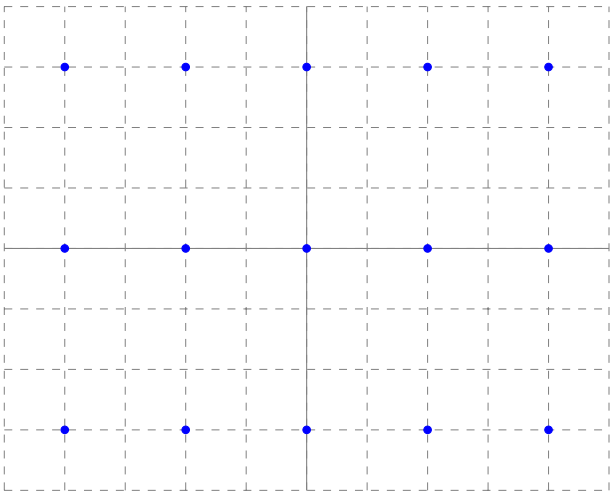
No entanto, podemos demonstrar um resultado para inteiros Gaussianos que é análogo ao Teorema da Divisão para $\mathbb{Z}$ (e anéis ordenados).

Teorema 4.52. *Sejam $\alpha, \beta \in \mathbb{Z}[i]$, com $\beta \neq 0$. Então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que $\alpha = \gamma\beta + \rho$, tal que $N(\rho) < N(\beta)$.*

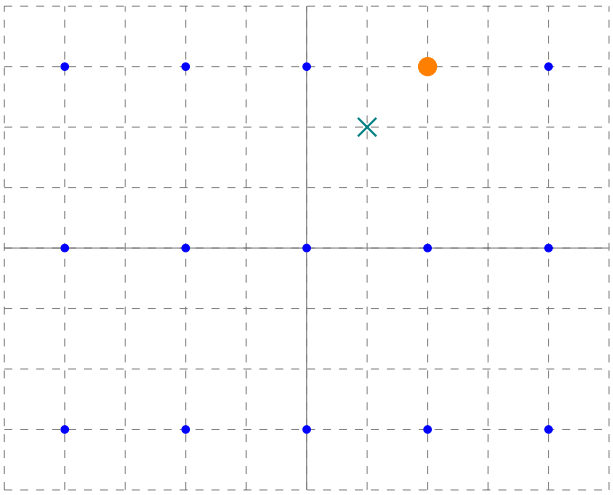
Claramente, γ e ρ são quociente e resto no enunciado do Teorema.

Demonstração. (informal)

Os múltiplos do inteiro gaussiano β formam um reticulado, que podemos visualizar como infinitos retângulos. Se $\beta = a + bi$, os lados destes retângulos tem comprimento a e b. A figura a seguir mostra os múltiplos de um inteiro Gaussiano β $(2+3i)$.



O inteiro Gaussiano α tem coordenadas inteiras, mas não necessariamente no reticulado gerado por β. Identificamos no reticulado de β um ponto mais próximo de α, e como este ponto está no reticulado de β, ele representa um ponto $\gamma\beta$. A figura a seguir ilustra a divisão de $1+2i$ por $2+3i$.



O ponto $\beta = 2+3i$ é representado por um círculo, e $\alpha = 1+2i$ por uma cruz. Note que pode haver mais de um ponto mais próximo. de α.

Temos α é $\gamma\beta + \rho$, onde ρ é, também, inteiro Gaussiano.

Resta mostrar que $N(\rho) < N(\beta)$. Se $\beta = a+bi$ e $\rho = x+yi$, temos $x \leq a/2$

e $y \leq b/2$, logo

$$\begin{aligned} N(\rho) &= x^2 + y^2 \\ &\leq \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 \\ &= \frac{a^2}{4} + \frac{b^2}{4} \\ &= \frac{N(\beta)}{4}. \end{aligned}$$

□

Corolário 4.53. *Podemos realizar algo semelhante a divisão em* $\mathbb{Z}[i]$ *de maneira simples usando aritmética racional: para dividir* $\alpha = a + bi$ *por* $\beta = c + di$*, calculamos os inteiros mais próximos de* a/c *e* d/b*:*

$$\begin{aligned} &a + bi \div c + di = q(c + di) + r \\ &q = \left\lfloor \frac{a}{c} \right\rceil + \left\lfloor \frac{b}{d} \right\rceil \\ &r = \alpha - q\beta, \end{aligned}$$

onde $\lfloor x \rceil$ *é o inteiro mais próximo de* x*. O resultado não é necessariamente único, e o resto pode ser negativo.*

O que fizemos com os inteiros Gaussianos foi usar uma norma que nos permitiu usar o algoritmo de Euclides. O mesmo algoritmo funcionará em qualquer anel que, mesmo não sendo totalmente ordenado, admita uma função λ com papel semelhante a esta norma, para que possamos definir a divisão como $a = qb + r$, com $\lambda(r)$ menor que $\lambda(b)$. Isto é a definição de um *domínio Euclideano* – que é, informalmente, um anel onde é possível usar o algoritmo de Euclides.

Definição 4.54 (domínio Euclideano)**.** Um **domínio Euclideano** é um anel comutativo R onde se pode definir uma função $\lambda : R \setminus \{0\} \to \mathbb{N}$, tal que para todos $a, b \in R$, com b não nulo,

(i) $\lambda(a) \leq \lambda(ab)$

(ii) existem $q, r \in R$, com $a = qb + r$, tais que $r = 0$ ou $\lambda(r) < \lambda(b)$.

A função λ é uma **norma** neste domínio Euclideano. ♦

Dizemos que λ é *uma* norma, porque não é única. A propriedade (ii) diz essencialmente que vale o algoritmo da divisão, mas não há a necessidade de q e r serem únicos.

Além dos inteiros Gaussianos, o anel $\mathbb{R}[x]$ pode ser tratado como Domínio Euclideano, se usarmos uma norma apropriada.

Exemplo 4.55. O anel $\mathbb{R}[x]$ é domínio Euclideano, se tomarmos $\lambda(p)$ dando o grau do polinômio: $\lambda(2x^3 - 4x + 10) = 3$. Claramente, (i) vale, porque o grau do polinômio st é o produto dos graus de s e t. (ii), o algoritmo da divisão também vale para polinômios em uma variável. ◀

Uma vez que tenhamos o algoritmo da divisão, podemos usar o algoritmo de Euclides para computar máximos divisores comuns.

Teorema 4.56. *Em todo domínio Euclideano*[4]*, é possível calcular algum máximo divisor comum para quaisquer dois elementos.*

A demonstração do Teorema 4.56 é a mesma da existência do MDC para inteiros, exceto que não podemos garantir unicidade do MDC em domínios Euclideanos (e é este o motivo do uso da palavra "algum" ao invés de "o" no enunciado).

Em domínios Euclideanos, vale também o Lema 4.12, que determina que o MDC de dois elementos é combinação linear inteira deles.

Exemplo 4.57. Em $\mathbb{R}[x]$, procuramos $\operatorname{mdc}\left(x^2, x^3\right)$. O MDC não é x, que divide tanto x^2 como x^3, porque $x \mid x^2$, e x^2 também divide ambos. Também não é simplesmente "x^2", porque os múltiplos de x^2 também são:

$$\left(\frac{1}{k}\right) kx^2 = x^2, \qquad (kx^2 \mid x^2)$$

$$\left(\frac{x}{k}\right) kx^2 = x^3. \qquad (kx^2 \mid x^3)$$

Isso acontece porque a ordem que impusemos em $\mathbb{R}[x]$ é parcial, e não total: dois polinômios de mesmo grau podem ter diferentes coeficientes na variável de mais alta potência.

Ainda em $\mathbb{R}[x]$, $\operatorname{mdc}\left(x^3\text{-}x^2, x^2\text{-}1\right)$ contém todos os múltiplos do polinômio $x - 1$: para todo k,

$$\left(\frac{x^2}{k}\right)\Big(k(x-1)\Big) = x^3 - x^2, \qquad (k(x-1) \mid x^3 - x^2)$$

$$\left(\frac{x+1}{k}\right)\Big(k(x-1)\Big) = x^2 - 1. \qquad (k(x-1) \mid x^2 - 1)$$

No entanto, a não ser por multiplicação por constante, o MDC de polinômios em $\mathbb{R}[x]$ é único. ◀

É interessante que uma tentativa de usar "tanto o grau do polinômio como o coeficiente líder" levaria a uma situação semelhante à de $\mathbb{C}$, onde essencialmente estaríamos tentando obter ordem total para o produto cartesiano de dois conjuntos infinitos ordenados ($\mathbb{R} \times \mathbb{R}$ para complexos, $\mathbb{Z} \times \mathbb{R}$

[4] Na verdade, pode-se definir MDCs em estruturas mais gerais que domínios Euclideanos, mas não tratamos disso.

para $\mathbb{R}[x]$, porque o grau é inteiro e o coeficiente líder é real) – estas relações de ordem, no entanto, não existem.

Retomando o MDC para inteiros, observamos que temos na definição uma exigência de que o MDC de dois números seja positivo. Esta restrição garante a unicidade do MDC – de outra forma, teríamos $\text{mdc}(8, 12) = \pm 4$, já que $\pm 4 \mid 8$, $\pm 4 \mid 12$, e se houver algum c que divida 8 e 12, (por exemplo, 2) então $c \mid \pm 4$.

Exercícios

Ex. 29 — Prove que, quando restrita a inteiros não-negativos, "divide" ($\mid$) é uma relação de ordem. Explique o que acontece se incluirmos os negativos.

Ex. 30 — Mostre que para qualquer inteiro não negativo n, o número $n(2n+1)(n+1)/6$ é inteiro.

Ex. 31 — Mostre que se $7 \mid (a^2 + b^2)$, então $7 \mid a$ e $7 \mid b$.

Ex. 32 — Mostre que para todo n,

(a) $3 \mid (10^n - 7^n)$

(b) $9 \mid (10^n - 1)$

(c) $8 \mid (3^{2n} + 7)$

Ex. 33 — Mostre que todo quadrado é da forma $3k$ ou $3k + 1$.

Ex. 34 — Mostre que todo cubo é da forma $9k$ ou $9k + 1$ ou $9k + 8$.

Ex. 35 — Mostre que todo número natural tem algum múltiplo positivo que, quando escrito na base dez, tem somente dígitos um e zero.

Ex. 36 — Sorteie dois números a, b, ambos entre dois e N. Qual é a probabilidade de $a \mid b$?

Ex. 37 — Calcule $\text{mdc}(294, 306)$, $\text{mdc}(96, 36)$ e $\text{mdc}(45, 67)$.

Ex. 38 — Determine todos os $152 \geq n \in \mathbb{N}$ tais que $\text{mdc}(n, 152) = 8$. Explique seu método.

Ex. 39 — Prove o Teorema 4.24.

Ex. 40 — Quando apresentamos o algoritmo de Euclides, mencionamos que o valor absoluto pode ser definido facilmente em qualquer anel com relação de ordem total. Mostre uma possível definição.

Ex. 41 — Prove que $\forall x \in \mathbb{Z},\ \ \mathrm{mdc}\,(a, b) = \mathrm{mdc}\,(a, xa + b)$.

Ex. 42 — Prove o Teorema 4.25.

Ex. 43 — Fazendo uso estritamente das definições dadas neste Capítulo,

(a) determine $\mathrm{mdc}\,(0, 0)$;

(b) já que, como dito no Exercício 29, a relação "divide" é de ordem, determine o maior e o menor elemento de $\mathbb{N}$, usando esta relação de ordem. Esboçe o diagrama de Hasse;

(c) comente a idéia de trocar a definição de $\mathrm{mdc}\,(a, b)$ para "o maior (usando '$\leq$') elemento que divide tanto a como b", relacionando com os itens (a) e (b) deste exercício.

Ex. 44 — Prove o Teorema 4.16. Dica: use o Corolário 4.14.

Ex. 45 — Demos duas demonstrações do Teorema 4.21, uma delas usando o Lema de Euclides, e uma usando o Lema de Bezout. Isso imediatamente levanta uma questão: o Lema de Euclides seria consequência simples do Lema de Bezout?
(Ou – tente demonstrar o Lema de Euclides usando o Lema de Bezout)

Ex. 46 — Demonstre o Lema 4.38.

Ex. 47 — Demonstre o Teorema 4.41.

Ex. 48 — Se trocarmos os dois valores iniciais na sequência de Fibonacci, teremos uma sequência diferente (por exemplo, com o primeiro número igual a 1 e o segundo igual a 3 tem-se a *sequência de Lucas*). Ainda valem o Lema de Honsberger (Lema 4.39) e os Teoremas 4.37, 4.40? Para quais pares de valores iniciais?

Ex. 49 — (Fácil) A *fórmula de Euler-Binet*, mencionada no Teorema 4.36, é uma forma fechada para o n-ésimo número de Fibonacci. Apresentamos a fórmula novamente, mas expandindo a razão áurea:

$$\begin{aligned} u_n &= \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}} \\ &= \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}. \end{aligned}$$

Seja $B(p, n)$ uma generalização da fórmula de Binet, onde o primo é parametrizável:

$$B(p, n) = \frac{(1+\sqrt{p})^n - (1-\sqrt{p})^n}{2^n\sqrt{p}}.$$

Prove que $B(p, n)$ sempre é racional.

Ex. 50 — Prove que $\text{mdc}\,(a+b, a\text{-}b) \geq \text{mdc}\,(a,b)$.

Ex. 51 — Calcule $\text{mmc}(22,24)$, $\text{mmc}(31,34)$, $\text{mmc}(20,32)$.

Ex. 52 — Prove o Teorema 4.28.

Ex. 53 — Prove o Teorema 4.30

Ex. 54 — Prove que para $k > 0$, $\text{mmc}(ka, kb) = k\,\text{mmc}(a,b)$.

Ex. 55 — Prove que $n^3 - n$ é divisível por 6 para todo inteiro n.

Ex. 56 — Prove que se $\text{mmc}(a,b) = \text{mdc}\,(a,b)$ então $a = \pm b$.

Ex. 57 — Prove que se $\text{mdc}\,(a,b) + \text{mmc}(a,b) = a + b$ então $a \mid b$ ou $b \mid a$.

Ex. 58 — Prove que $\text{mdc}\,(a, 2+a)$ sempre é 1 ou 2, para todo inteiro a.

Ex. 59 — Para quais números $\text{mmc}(a,b) - \text{mdc}\,(a,b) = a + b$?

Ex. 60 — Prove que são equivalentes:

- $a \mid b$
- $\text{mdc}\,(a,b) = |a|$
- $\text{mmc}(a,b) = |b|$

Ex. 61 — Resolva o sistema:

$$\begin{aligned} \text{mmc}(a,b) &= 360 \\ \text{mdc}\,(a,b) &= 30 \end{aligned}$$

Ex. 62 — Prove o Teorema 4.47.

Ex. 63 — Prove que para dois inteiros Gaussianos α e β, se $\alpha \mid \beta$ então $N(\alpha) \mid N(\beta)$.

Ex. 64 — Prove que um inteiro Gaussiano tem norma par se e somente se é múltiplo de $1+i$.

Ex. 65 — Quantos inteiros Gaussianos existem com norma 13?

Ex. 66 — Dê um exemplo de par de inteiros Gaussianos que tenham mais de um MDC.

Ex. 67 — Prove que para quaisquer inteiros Gaussianos α e β, se δ e γ são MDCs de α, β, então $\delta = u\gamma$, onde u é uma unidade $(\pm 1, \pm i)$.

Ex. 68 — A função de valoração usada em $\mathbb{R}[x]$ poderia ser "o valor do polinômio no zero"? A ordem resultante seria parcial? Se a função de valoração puder ser esta, os MDCs calculados seriam os mesmos que usando "grau do polinômio" como função de valoração? Responda novamente para "o valor do polinômio em 1".

Ex. 69 — Prove que todo corpo é um domínio Euclideano.

Ex. 70 — Seja X um domínio Euclideano com função de valoração λ. Sejam $a, b \in X$, e suponha que d um máximo divisor comum de a e b. Prove que, se d' é algum divisor comum de a e b, então $\lambda(d') \leq \lambda(d)$; e que, se d' for *máximo* divisor comum de a e b, então $\lambda(d') = \lambda(d)$.

Ex. 71 — Construa um domínio Euclideano com matrizes quadradas de ordem dois e entradas inteiras. Comece com matrizes da forma

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

com $a, b \in \mathbb{Z}$.
Defina divisão para estas matrizes: dadas A, B, deve ser possível obter Q, *que é matriz da mesma forma que* A *e* B, tal que

$$A = QB + R.$$

Finalmente, escolha uma função de valoração e verifique que ela vale.
Use o algoritmo de Euclides para obter um MDC de

$$A = \begin{pmatrix} 2 & 7 \\ 7 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 1 \\ 1 & 4 \end{pmatrix}$$

Ex. 72 — Prove que o Lema de Bézout vale em qualquer domínio Euclideano.

Capítulo 5

Primos

Tratamos agora de números primos e irredutibilidade. Definimos inicialmente números inteiros primos, e mais adiante tratamos dos análogos em domínios Euclideanos.

Definição 5.1 (número primo, números co-primos)**.** Um número inteiro positivo é **primo** se e somente se é divisível apenas por 1 e por ele mesmo.

Dois números a e b são co-primos se o único inteiro positivo que divide ambos é um – ou seja, se $\text{mdc}(a, b) = 1$. ⧫

5.1 Fatoração Única em $\mathbb{Z}$

Esta seção trata do Teorema Fundamental da Aritmética, que afirma a existência da fatoração em primos para todos os inteiros.

Lema 5.2. *Todo inteiro diferente de zero pode ser escrito como produto de primos e uma unidade (*$+1$ *ou* -1*).*

Demonstração. Seja n o menor inteiro positivo que não seja primo, mas que não possa ser escrito como produto de primos. Então, como n não é primo, $n = ab$, e necessariamente $0 < a, b < n$. Mas, como n é o *menor* inteiro positivo que não pode ser decomposto em primos, então a e b podem. Mas se a e b podem ser decompostos em primos, $n = ab$ também pode, porque o produto das fatorações de a e de b é a fatoração de n – o que contradiz o que presumimos no início da demonstração.

Tendo provado para os positivos, temos os negativos. Como cada inteiro negativo $-n$ é igual a $(-1)n$, e n positivo tem fatoração em primos, terminamos a demonstração. □

Teorema 5.3 (Fundamental da Aritmética)**.** *Todo inteiro* $n \neq 0$ *pode ser escrito como produto de primos, e este produto é único, a não ser pela ordem.*

Demonstração. Que existe uma fatoração o Lema 5.2 garante. Falta mostrar que é única. Suponha, portanto, que haja mais de uma fatoração para um inteiro. Retiramos das fatorações os elementos primos comuns às duas, e temos n:

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_r,$$

onde não há qualquer elemento comum nos dois lados. Mas pelo Lema de Euclides (Lema 4.20), como $p_1 \mid n$, teríamos $p_1 \mid q_1 q_2 \dots q_r$, e um dos q_i teria que ser igual a p_1, portanto temos uma contradição. □

Exemplo 5.4. O inteiro 4410 é fatorado em

$$4410 = (2)(3^2)(5)(7^2). \quad \blacktriangleleft$$

Definição 5.5 (ordem de p em n)**.** Damos o nome de **ordem** de p em n ao expoente do primo p na fatoração de n, e denotamos $\mathrm{ord}_p(n)$. ♦

Exemplo 5.6. A fatoração de 1400 é $2^3 5^2 7$, portanto temos $\mathrm{ord}_2(1400) = 3$, $\mathrm{ord}_5(1400) = 2$, $\mathrm{ord}_7(1400) = 1$. ◀

Para primos não constantes na fatoração de um número a ordem é zero: por exemplo, $\mathrm{ord}_3(1400) = 0$, $\mathrm{ord}_{11}(1400) = 0$, etc – o que nos permite escrever n como

$$\prod_{p \in \mathrm{PRIMOS}} p^{\mathrm{ord}_p(n)},$$

já que para todo primo q fora da fatoração de n teremos $\mathrm{ord}_q(n) = 0$ e $q^{\mathrm{ord}_q(n)} = 1$.

Lema 5.7. *Todo inteiro* n *pode ser escrito como produto de um quadrado perfeito* a^2 *e um natural livre de quadrados* b*:* $n = a^2 b$.

Demonstração. Sabemos que n tem fatoração em primos, $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_r}$.

Para cada expoente a_i, se a_i é ímpar, reescreva $p_p^{a_i}$ como $p_i p_i^{a_i - 1}$. Agora todos os expoentes são ou pares, ou iguais a um. Por exemplo, reescrevemos $p_1^7 p_2^4 p_3^{11} p_4$ como $(p_1)(p_1^6) p_2^4 (p_3)(p_3^{10}) p_4$.

Escreva a fatoração com os expoentes pares à esquerda e os outros à direita. Renomeando os índices, temos

$$n = \left(p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s}\right)\left(p_{s+1} \cdots p_t\right),$$

com c_i par. O lado esquerdo é claramente um quadrado perfeito, e o direito

é livre de quadrados:

$$\begin{aligned} a^2 &= p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ b &= p_{s+1} \cdots p_t. \end{aligned}$$ □

Exemplo 5.8. A fatoração do número 396000 é

$$396000 = 2^5\, 3^2\, 5^3\, 11,$$

que reescrevemos

$$\begin{aligned} 396000 &= (2)(2^4)\, 3^2\, (5)(5^2)\, 11 \\ &= (2^4)(3^2)(5^2)\, (2)(5)(11) \\ &= \Big[(2^2)(3)(5)\Big]^2\, (2)(5)(11) \\ &= a^2 b, \end{aligned}$$

com $a = (2^2)(3)(5) = 60$ e $b = (2)(5)(11) = 110$. Para uma verificação trivial, $a^2 b = 60^2 110 = 396000$. ◀

5.2 Números de Mersenne e de Fermat

Potências de qualquer número são evidentemente compostas ($a^b = a \cdot c^{b-1}$, quando $a, b > 1$), mas somando ou subtraindo um de cada potência identificamos números ($a^b + 1$, $a^b - 1$) que merecem alguma atenção.

Investigaremos brevemente estes dois casos, verificando quando cada um desses números pode ser primo, e para cada um deles demonstraremos um teorema simples.

Primeiro, olhamos para o caso $a^b - 1$.

Teorema 5.9. *Se* $a^b - 1$ *é primo, então* $a = 2$ *e* b *é primo.*

Demonstração. Suponha que $b > 1$ e $a^b - 1$ é primo. Então a deve necessariamente ser dois, porque Usando a identidade $(x^n - y^n) = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$ com $x = a$, $y = 1$ e $n = b$, temos

$$a^b - 1 = (a - 1)(a^{b-1}a^{b-2} + \cdots + a + 1).$$

Como $(a - 1) \mid a^b - 1$ e $a^b - 1$ é primo, então necessariamente $a - 1 = 1$, e $a = 2$.

Agora suponha que b seja composto; $b = cd$. Então $2^{cd} = (2^c)^d$, e

$$\begin{aligned} 2^b - 1 &= (2^c)^d - 1 \\ &= (2^c - 1)\Big[(2^c)^{d-1} + \cdots + 1\Big], \end{aligned}$$

e (2^c-1) dividirá 2^b-1, que é primo – portanto b não pode ser composto. □

Os números investigados por Mersenne eram, portanto, da forma 2^p-1, com p primo.

Definição 5.10 (Números de Mersenne)**.** Um número natural da forma 2^p-1, com p primo, é um **número de Mersenne** e denotado M_p. Quando M_p é primo, é chamado de **primo de Mersenne**. ⧫

Números de Mersenne apresentam uma interessante relação com números perfeitos.

Definição 5.11 (número perfeito)**.** n é um **número perfeito** se é igual à soma de seus divisores próprios. ⧫

Exemplo 5.12. O menor número perfeito é 6, porque $1+2+3=6$.

O número 28 também é perfeito, porque seus divisores próprios são $1,2,4,7,14$, e $1+2+4+7+14=28$. ◀

Teorema 5.13. *Seja 2^p-1 um primo de Mersenne. Então $(2^p-1)2^{p-1}$ é perfeito.*

Demonstração. Seja $q=2^{p-1}$ um primo de Mersenne, e considere o número $r=q(2^{p-1})$. Separe os divisores de r em dois conjuntos: as potência de dois e os outros divisores próprios:

$$A=\{1,2,2^2,\ldots,2^{p-1}\},$$
$$B=\{q,2q,2^2q,\ldots,2^{p-2}q\}.$$

Ao descrever o conjunto B, excluímos o expoente $p-1$, porque queremos apenas os divisores próprios (que também são usados na definição de números perfeitos). Se tivéssemos incluído $p-1$, teríamos incluído o próprio r.

Sabemos que

$$1+x+x^2+\cdots+x^{k-1}=\frac{x^k-1}{x-1},$$

portanto a soma de A é

$$\begin{aligned}\sum_{a\in A} a &= 1+2^2+\cdots+2^{p-1}\\ &= \frac{2^p-1}{2-1}\\ &= 2^p-1\\ &= q.\end{aligned}$$

A soma de B é

$$\begin{aligned}\sum_{b\in B} &= q + 2q + 2^2q + \cdots + 2^{p-2}q \\ &= q(1 + 2^2 + \cdots + 2^{p-2}) \\ &= q\left(\frac{2^{p-1}-1}{2-1}\right) \\ &= q(2^{p-1}-1).\end{aligned}$$

Então, a soma de todos os divisores (soma de $A \cup B$) é

$$\begin{aligned}q + q(2^{p-1}-1) &= q + q(2^{p-1}) - 1 \\ &= q(2^{p-1}),\end{aligned}$$

e r é perfeito. □

Exemplo 5.14. Para $p = 2, 3, 5$, temos

$$\begin{aligned}(2^p-1)2^{p-1} &= (2^2-1)2^{2-1} = 3\cdot 2 = 6 \\ (2^p-1)2^{p-1} &= (2^3-1)2^{3-1} = 7\cdot 4 = 28 \\ (2^p-1)2^{p-1} &= (2^5-1)2^{5-1} = 127\cdot 64 = 8128\end{aligned}$$

Já mostramos no Exemplo 5.12 que 6 e 28 são perfeitos. Os divisores de 8128 são

$$1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, 4064.$$

A soma destes é

$$1+2+4+8+16+32+64+127+254+508+1016+2032+4064 = 8128. \blacktriangleleft$$

Passamos aos números da forma $a^b + 1$.

Teorema 5.15. *Se $a^b + 1$ é primo, com $a > 1$ e $b > 1$, então a é par e b é potência de dois.*

Demonstração. Suponha que a é ímpar Então $a > 2$ e a^b deve ser ímpar, o que implica que $a^b + 1$ é par, e maior que dois – uma contradição. Logo, a é necessariamente par.

Agora suponha que b não é potência de dois. Então $b = cq$, sendo q ímpar e $c > 0$.

Usando a identidade

$$(x^n - y^n) = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

com $x = a^c$, $y = -1$ e $n = q$, temos

$$\begin{aligned}
(a^c)^q - (-1)^q &= (a^c - (-1)^q)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right] \\
(a^c)^q - (-1)^q &= (a^c + 1)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right] \\
a^{cq} + 1 &= (a^c + 1)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right] \\
a^n + 1 &= (a^c + 1)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right],
\end{aligned}$$

ou seja, $(a^c + 1)$ divide $a^n + 1$. Mas $a^n + 1$ é primo, e chegamos a uma contradição. Dessa forma, b não tem fatores ímpares – ou seja, é potência de dois. □

O Teorema 5.15 dá uma motivação para a definição de númeos de Fermat (que são da forma $2^{2n} + 1$). Pierre de Fermat conjecturou que todos ou números dessa forma fossem primos, mas Euler posteriormente mostrou que o quinto número de Fermat, F_5, é composto:

$$\begin{aligned}
641 &= 2^4 + 5^4 \\
&= 5 \cdot 2^7 + 1,
\end{aligned}$$

portanto $2^4 = 641 - 5^4$. Agora, $F_5 = 2^{32} + 1$. e

$$\begin{aligned}
2^{32} &= 2^{28} \cdot 2^4 \\
&= 2^{28} \cdot (641 - 5^4) \\
&= 2^{28}641 - 2^{28}5^4 \\
&= 2^{28}641 - (2^7 5)^4 \\
&= 2^{28}641 - (641 - 1)^4 \\
&= 641Q - 1,
\end{aligned}$$

e $641 \mid 2^{32} + 1$.

Tendo um fator, dividimos F_5 por ele e obtemos $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ (interessantemente, o outro fator, 6700417, é primo)[1].

[1] Vale observar que calcular 2^{32} para obter F_5 não era difícil para Fermat e Euler: basta iniciar com 1 e multiplicar repetidamente por 2. Dividir 4294967297 por 641 também não era difícil. Fatorar inteiros já não é simples, e embora $2^{32} + 1$ seja um número fácil de fatorar para computadores atuais, o problema de fatorar inteiros serviu de base para a Criptografia de chave pública por décadas (o tamanho recomendado para chave em 1974, quando o criptossistema RSA foi criado, era de 512 bits, que se traduz em inteiros da ordem de 2^{512}, mas sem computadores, fatorar um número próximo de 2^{32} certamente não é tarefa simples). Por isso é interessante Euler ter encontrado um caminho para obter esse fator, ainda que não tenha encontrado método geral de fatoração rápida.

Definição 5.16 (Números de Fermat)**.** Um número natural da forma $2^{2^n}+1$, com $n \in \mathbb{N}$, é um **número de Fermat** e denotado F_n. Quando F_n é primo, é chamado de **primo de Fermat**. ⧫

Teorema 5.17. *Para* $n > 0$, $F_n = F_0 \cdots F_{n-1} + 2$.

Demonstração. Por indução em n.

Para a base, $n = 1$. Observamos que $F_0 = 3$ e $F_1 = 5$, e temos trivialmente $F_1 = F_0 + 2 = 5$.

Para o passo, presuma $F_n = F_0 \cdots F_{n-1} + 2$.

$$\begin{aligned} F_0 \cdots F_n + 2 &= F_0 \cdots F_{n-1} F_n + 2 \\ &= (F_n - 2) \cdot F_n + 2 && \text{(hipótese de indução)} \\ &= (2^{2^n} - 1)(2^{2^n} + 1) + 2 \\ &= (2^{2^{n+1}} + 1) + 1 \\ &= F_{n+1}. \end{aligned}$$ □

Teorema 5.18. *Se* $m \neq m$*, então* $\operatorname{mdc}(F_m, F_n) = 1$.

Demonstração. Presuma $m < n$, e seja d um divisor comum de F_m e F_n.

Se $d \mid F_m$, pelo Teorema 5.17,

$$d \mid F_0 \cdots F_{n-1} + 2.$$

Note que, como $m < n$, F_m está no produto, por isso a afrimação vale.

Mas se d divide F_m, então temos

$$\begin{aligned} &d \mid F_0 \cdots \mathbf{d} \cdots F_{n-1} + 2 \\ &d \mid (F_0 \cdots F_{n-1})\mathbf{d} + 2 \\ &d \mid 2. && \text{(subtraímos múltiplo de d)} \end{aligned}$$

Mas como todo número de Fermat é ímpar e d é divisor de F_m, d é ímpar, e portanto só pode ser um. □

5.3 Infinitos primos

Mostramos a seguir três demonstrações diferentes para a infinitude dos números primos. Há diversas outras, e a elaboração de uma delas é pedida no Exercício 90.

Teorema 5.19. *Há infinitos inteiros primos.*

Demonstração. (de Euclides) Suponha que não. Seja $p_1, p_2, \ldots, p_n$ a lista finita de todos os primos. Seja

$$q = 1 + p_1 p_2 \ldots p_n.$$

Seja p um fator primo de q. p não pode ser nenhum dos $p_1, \ldots, p_n$, porque se fosse, p dividiria 1. Assim, existe um primo não listado. □

Demonstração. (de Hermite) Tome um natural qualquer n. Seja p um primo divisor de $n! + 1$. Mostraremos que $p > n$ – e como isso vale para *qualquer* n, há infinitos primos (dado um $n \in \mathbb{N}$, existe primo maior que n).

Suponha, por absurdo, que $p \leq n$. Então $p \mid n!$. Mas presumimos que p é divisor de $n! + 1$. Pelo Lema 4.3, p deve dividir a diferença entre eles, $(n!+1)-(n!)$. Então $p \mid 1$ – absurdo. Portanto $p > n$, e há infinitos primos. □

Demonstração. (de Erdös, adaptada) Paul Erdös desenvolveu uma demonstração combinatória muito simples para o Teorema da infinitude dos primos.

Suponha que há um conjunto finito de primos, $p_1, p_2, \ldots, p_k$. Pelo Lema 5.7, cada número inteiro positivo n pode ser escrito como o produto de um quadrado perfeito e um não-quadrado ($n = a^2 b$). Disso seguem alguns fatos:

- Como $a \leq \sqrt{n}$, há no máximo $\sqrt{n}$ possibilidades para a
- Como b é produto de primos *distintos* (não contém quadrados na fatoração), e há k primos, então há 2^k possibilidades para b.
- Há, portanto, $2^k\sqrt{n}$ possibilidades para $a^2 b$. Como evidentemente existem n inteiros positivos entre 1 e n, então

$$\begin{aligned} n &\leq 2^k \sqrt{n} \\ n^2 &\leq (2^k)^2 n \\ n &\leq (2^k)^2. \end{aligned}$$

Assim, todo inteiro positivo n seria menor ou igual que 2^{2k}, e os naturais seriam finitos. □

Teorema 5.20. *Há distâncias arbitrariamente grandes entre primos consecutivos.*

Demonstração. Considere a sequência de inteiros consecutivos (com $n > 1$):

$$\begin{aligned}
&(n+1)!+2,\\
&(n+1)!+3,\\
&\quad\vdots\\
&(n+1)!+n,\\
&(n+1)!+(n+1),
\end{aligned}$$

O primeiro é divisível por 2; o segundo é divisível por 3, e assim por diante, até o último, que é divisível por $n+1$. Nenhum deles, portanto, é primo. □

A distância na demonstração é um mínimo – pode haver compostos antes de $(n+1)!+2$ e depois de $(n+1)!+(n+1)$.

Podemos ilustrar o Teorema escolhendo um número qualquer. Tomamos $n = 4$ (escolhemos um número pequeno porque teremos que calcular o fatorial de $n+1$). Assim, $n+1 = 5$, e $(n+1)! = 120$.

k	$(n+1)!+k$
2	122
3	123
4	124
5	125

Todos são compostos ($2 \mid 122, 3 \mid 123, 4 \mid 124, 5 \mid 125$). Observe que $120, 121$ (antecessores da sequencia) e 126 (sucessor) também são compostos, embora isto não fosse garantido pelo enunciado do Teorema.

O único inteiro primo par é o número dois, portanto todos os outros primos, quando divididos por quatro, devem resultar em resto um ou três. Dizemos que estes primos são *da forma* $4n+1$ ou *da forma* $4n+3$.

Inicialmente observamos que os números (não apenas primos) da forma $4n+1$ são fechados para multiplicação:

$$(4a+1)(4b+1) = 4(ab+a+b)+1 \tag{5.1}$$

Teorema 5.21. *Há infinitos primos da forma* $4n+3$.

Demonstração. Suponha que haja um número finito de primos da forma $4k+3$, e que estes sejam $3, p_1, p_2, \ldots, p_k$ (observe que listamos o 3, primeiro número da forma $4k+3$, explicitamente). Então seja

$$q = 4(p_1 p_2 \ldots p_r) + 3.$$

Aqui o primo 3 foi explicitamente excluído do produto entre parênteses.

Um primeiro fato evidente é que q é da forma $4k+3$, porque foi construído assim. Agora, como $q > p_k$, ele não pode ser primo, já que presumimos que p_k é o último primo dessa forma. Mostraremos agora que q deve necessariamente ser primo, e chegaremos a uma contradição.

Se todos os fatores primos de q fossem da forma $4k+1$, então q também o seria, portanto q tem algum fator primo da forma $4k+3$, que deve estar dentre os $p_1, p_2, \ldots, p_r$ (porque presumimos que estes são todos os primos $4k+3$).

Agora, $3 \nmid q$, porque se $3 \mid q$, então $3 \mid (q-3)$, ou seja,

$$3 \mid 4(p_1 p_2 \ldots p_r),$$

o que não é possível, porque 3 foi explicitamente excluído do produto, e o que temos são $4 = 2^2$ e os outros p_i. Já temos $3 \nmid q$. Verificamos os outros primos da forma $4k+3$ (ou seja, os p_i). Seja p_j um primo da forma $4k+3$ que divide q: $p_j \neq 3$ e $p_j \mid q$. Então

$$p_j \mid 4p_1 p_2 \ldots p_n + 3$$

Mas se subtrairmos um múltiplo de p_j do lado direito, a relação continua valendo. Assim,

$$\begin{aligned}
&p_j \mid 4p_1 p_2 \ldots p_n + 3 \\
&p_j \mid 4p_1 p_2 \ldots \mathbf{p_j} \ldots p_n + 3 \\
&p_j \left| \left[4p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_n\right] \mathbf{p_j} + 3 \right. \\
&p_j \mid 3,
\end{aligned}$$

O que novamente é impossível. □

Para $4n+1$ apresentamos uma demonstração simples por redução ao absurdo, que depende do Lema 5.22, e uma família de demonstrações que depende de uma propriedade da de somas de quadrados (Lema 5.25).

Lema 5.22. *Se $n > 2$, então todo divisor ímpar de n^2+1 é da forma $4k+1$.*

A demonstração do Lema 5.22 não é dada neste momento.

Exemplo 5.23. Seja $n = 5$. Então $n^2 + 1 = 26$, e os divisores de 26 são $1, 2, 13, 26$, sendo os ímpares $4(0)+1 = 1$ e $4(3)+1 = 13$.

Para $n = 6$, temos $n^2 + 1 = 37$, com divisores $1, 37$, e $4(9)+1 = 37$.

Para $n = 9$, da mesma forma temos $9^2 + 1 = 82$, e os divisores de 82 são $1, 2, 41, 82$; Neste caso também $4(10)+1 = 41$. ◀

Teorema 5.24. *Há infinitos primos da forma $4n+1$.*

Demonstração. (usando o Lema 5.22) Suponha que o número de primos da forma $4n+1$ seja finito, e que estes sejam $p_1, p_2, \ldots, p_k$. Construa agora o número

$$r = 4p_1^2 p_2^2 \ldots p_k^2 + 1.$$

Nenhum dos p_i pode dividir r. Então os divisores primos de r não estão entre os $p_1, \ldots, p_k$ usados para construir r – devem então ser da forma $4k+3$. Mas como r é da forma x^2+1, pelo Lema 5.22, r não pode ser divisível por um ímpar da forma $4k+3$. Chegamos a uma contradição, e a demonstração está finalizada. □

A demonstração dada é por contradição, e seria interessante se houvesse outra, construtiva, de onde pudéssemos extrair um método para construir primos da forma $4k+1$.

Há uma demonstração construtiva pra o Teorema 5.24, publicada em 1992 por Neville Robbins. Esta demonstração, no entanto, depende do Lema 5.25, que apresentamos por ora sem demonstração (que será dada no Capítulo 10).

Lema 5.25. *Se n é soma de dois quadrados, $n = a^2+b^2$, com $\mathrm{mdc}(a,b) = 1$, então n não tem fatores primos da forma $4k+3$.*

No Lema 5.25, "não haver fatores primos da forma $4k+1$" significa efetivamente que não há divisores (primos ou não) da forma $4k+3$.

Embora Robbins tenha redigido a demonstração sem dividí-la em partes, neste texto apresentaremos a essência dela em um Lema, e depois a completaremos de duas formas diferentes, uma usando números de Fermat, e uma usando números de Fibonacci (as duas variantes foram originalmente apresentadas na mesma demonstração por Robbins). Nossa apresentação é ligeiramente diferente da original.

Lema 5.26. *Seja (s_n) uma sequência com as seguintes propriedades:*

i) $s_n > 1$ *quando* $n \geq 1$*;*

ii) $s_n = a_n^2 + b_n^2$*, com* $\mathrm{mdc}(a,b) = 1$*;*

iii) $\mathrm{mdc}(s_n, s_m) = 1$ *quando* $n \neq m$*;*

iv) a_n *e* b_n *tem paridades diferentes (um é par e o outro é ímpar).*

Então cada s_n tem um fator primo da forma $4k+1$, que não está na fatoração dos outros s_j.

Demonstração. A sequência s_n tem as seguintes propriedades:

i) $s_n > 1$ quando $n \geq 1$ (por definição).

ii) Para todo n, existe algum primo $p = 4k+1$ tal que $p \mid s_n$ (pelo Lema 5.25, não há divisores $4k+3$, e pela condição (iv) do enunciado, não há divisores $4k$ nem $4k+2$).

iii) Todos os s_n são co-primos entre si.

A exclusão de divisores $4k$ e $4k+2$ é relevante para excluir sequências de potências de dois. Por exemplo, a sequência $d_n = 2^n$, que contém somas de quadrados $d_i = (2^{i-2})^2 + 0^2$, satisfaria os critérios, mas seus elementos não contém primos $4k+1$. O único primo nas fatorações desses números é o 2.

Claramente, cada s_n nos dá um novo primo da forma $4k+1$, porque todos os elementos tem um divisor da forma $4k+1$, que é diferente para cada novo elemento da sequência, porque são todos co-primos. □

Repetimos agora o enunciado do Teorema 5.24, e passamos às duas demonstrações.

Ambas constróem a sequência $s_n = a_n^2 + b_n^2$, com $\text{mdc}(a,b) = 1$ e a e b tendo paridades diferentes. A demonstração usando números de Fibonacci, também usamos o Lema 5.27 (Exercício 80).

Lema 5.27. *Seja p primo. Então*

$$\text{mdc}\left(\frac{p+1}{2}, \frac{p-1}{2}\right) = 1.$$

Teorema 5.28. *Há infinitos primos da forma $4k+1$.*

Demonstração. (usando números de Fermat)
Considere a sequência (F_n), de números de Fermat (não necessariamente primos).

i) $F_n > 1$;

ii) F_n é evidentemente soma de quadrados: $F_n = 2^{2n}+1 = (2^{2n-1})^2+(1)^2$, $\text{mdc}\left(2^{2n-1}, 1\right) = 1$, e obviamente as paridades de 2^{2n-1} e 1 são opostas.

iii) Todos os F_n são co-primos entre si (Teorema 5.18).

Basta agora usar o Lema 5.26. □

Também é possível usar números de Fibonacci, embora a demonstração fique um pouco mais longa.

Demonstração. (usando números de Fibonacci)
Considere a sequência (u_n), de números de Fibonacci (não necessariamente primos). Observamos os fatos a seguir.

I) $u_{2n+1} = u_n^2 + u_{n+1}^2$ (Teorema 4.41);

II) $\mathrm{mdc}\,(u_m, u_n) = u_{\mathrm{mdc}(m,n)}$ (Teorema 4.40);

III) $2 \mid u_n$ se e somente se $3 \mid n$ (Teorema 4.42);

IV) $u_n > 1$ quando $n > 2$.

Enumere agora os primos maiores que 3: $q_1 = 5$, $q_2 = 7$, etc. Defina uma sequência (s_n), de forma que o n-ésimo termo de s_n seja o número de Fibonacci com índice q_n:

$$s_n = u_{q_n}.$$

Observamos que, por (I),

$$u_{q_n} = u^2_{\left[\frac{q_n - 1}{2}\right]} + u^2_{\left[\frac{q_n + 1}{2}\right]}. \tag{5.2}$$

Agora, embora os q_i sejam primos, precisamos garantir que os dois números elevados ao quadrado em 5.2 são co-primos.

Como pelo Lema 5.27 $\mathrm{mdc}\,((q_n\text{-}1)/2, (q_n + 1)/2)) = 1$, então por (II),

$$\mathrm{mdc}\left(u_{\left[\frac{q_n\text{-}1}{2}\right]},\ u_{\left[\frac{q_n + 1}{2}\right]}\right) = 1. \tag{5.3}$$

Como $q_n > 3$, e q_n é primo, (III) implica que $2 \nmid u_{q_n}$, portanto se considerarmos

$$u_{\left[\frac{q - 1}{2}\right]}, \qquad u_{\left[\frac{q + 1}{2}\right]}, \tag{5.4}$$

um é par e o outro, ímpar.

Finalmente, quando $m \neq n$, $q_m \neq q_n$, então $\mathrm{mdc}\,(q_m, q_n) = 1$. Por isso, a partir de (II) concluímos que $\mathrm{mdc}\,(u_{q_m}, u_{q_n}) = 1$. Temos:

i) $q_n > 1$ (de (IV));

ii) $q_{2n+1} = q^2_{\frac{n-1}{2}} + q^2_{\frac{n+1}{2}}$, com os dois elementos elevados ao quadrado sendo co-primos (Equação 5.3) e com paridade diferentes (Equação 5.4);

iii) $\mathrm{mdc}\,(u_{q_m}, u_{q_n}) = 1$, porque os q_i são co-primos, e $\mathrm{mdc}\,(u_m, u_n) = u_{\mathrm{mdc}(m,n)}$ (Teorema 4.40).

Pelo Lema 5.26, a sequência (q_n) nos dá infinitos primos da forma $4k+1$. □

Terminamos esta seção com um Teorema a respeito da série $1/p$ (soma dos recíprocos dos primos).

Teorema 5.29. *A série*

$$\sum_{p \text{ primo}} \frac{1}{p}$$

diverge.

A demonstração a seguir é de Paul Erdös.

Demonstração. Presuma que $\sum_{p \text{ primo}} \frac{1}{p} < \infty$. Nada presumimos a respeito do valor da série, mas sabemos que, como $1/p$ tende a zero (porque há infinitos primos), existe uma série começando de algum primo com valor menor que $1/2$. Ou seja, existe k inteiro tal que

$$\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}.$$

onde p_i é p i-ésimo primo.

Agora, para qualquer inteiro positivo x podemos definir o conjunto

$$M_x = \{n \leq x \ : \ \text{se } p > k, p_k \nmid n\}$$

dos números menores ou iguais a x, que *não* são divisíveis por primos maiores que p_k.

Se $n \in M_x$, então, como qualquer outro inteiro, n pode ser escrito como

$$n = m^2 r,$$

com r livre de quadrados.

Como $n \leq x$ e $= m^2 r$ há no máximo $\sqrt{x}$ possíveis valores para m, e 2^k possibilidades para r (porque há no máximo k primos diferentes que dividem n, e r é livre de quadrados). Assim,

$$|M_x| \leq 2^k \sqrt{x}.$$

Agora olhamos para os números que não incluímos em M_x – aqueles que são múltiplos de algum $p_r > p_k$

$$N_{i,x} = \{n \leq x \ : \ \exists j > k, p_j \mid n\}.$$

Então

$$\{1, 2, \ldots, x\} \setminus M_x = \bigcup_{i>k} N_{i,x},$$

e

$$|N_{i,x}| \leq \frac{x}{p_i}.$$

$$
\begin{aligned}
x - |M_x| &\leq \sum_{i>k} |N_{i,x}| < \sum_{i>k} \frac{x}{p_i} \\
x - |M_x| &< \sum_{i>k} \frac{x}{p_i} \\
x - |M_x| &< x \sum_{i>k} \frac{1}{p_i} \\
x - |M_x| &< x\frac{1}{2} && \text{(da nossa hipótese)} \\
x &< \frac{x}{2} + |M_x| \\
\frac{x}{2} &< |M_x|.
\end{aligned}
$$

Então, das duas desigualdades que obtivemos,

$$
\begin{aligned}
\frac{x}{2} &< |M_x| \leq 2^k\sqrt{x} \\
\frac{x}{2} &< 2^k\sqrt{x},
\end{aligned}
$$

mas para $x > 2^{2k+2}$,

$$x > 2^{2k+2}\frac{x}{2} > 2^{xk+1}.$$

Como chegamos a uma contradição, concluímos que a série $\sum \frac{1}{p_i}$ diverge. □

5.4 Fatoração Única em Dominios Euclideanos

Lembramos que em um anel, as *unidades* são os elementos com inversos. Em $\mathbb{Z}$, estes são ± 1; em $\mathbb{R}[x]$, são os polinômios constantes (os de grau zero), porque para outros polinômios, $1/p$ não é polinômio; nos inteiros Gaussianos ($\mathbb{Z}[i]$), as unidades são ± 1 e $\pm i$.

Definição 5.30 (elemento irredutível)**.** Um elemento x é **irredutível** se é divisível somente por unidades ou por seus próprios múltiplos por unidade (ux, onde u é unidade). ⧫

Assim, um polinômio não constante p é irredutível se os únicos outros polinômios que dividem p são constantes ou múltiplos de p. Por exemplo, o polinômio $x^2 + x$ não é irredutível, porque

$$x^2 + x = x(x + 1)$$

e portanto $x \mid x^2 + x$, e $(x + 1) \mid x^2 + x$.

Já $x^2 - 9$ é irredutível em $\mathbb{R}[x]$, no anel de polinômios com coeficientes inteiros, porque seus divisores são somente os polinômios constantes e os múltiplos deste mesmo polinômio.

A redutibilidade de um polinômio depende do anel onde trabalhamos. Podemos deixar de lado o anel dos polinômios com coeficientes reais e passar para o anel dos polinômios com coeficientes inteiros[2]. Um polinômio que é fatorável em $\mathbb{R}[x]$ pode ser irredutível em $\mathbb{Z}[x]$. Por exemplo, o polinômio $x^2 + x - 1$ tem duas raízes reais, logo é fatorável na forma $(x - r_1)(x - r_2)$:

$$x^2 + x - 1 = \left(x - \frac{\sqrt{5}-1}{2}\right)\left(x + \frac{\sqrt{5}-1}{2}\right).$$

Mas este mesmo polinômio é irredutível no anel $\mathbb{Z}[x]$, porque não é produto de outros polinômios *com coeficientes inteiros*.

Os inteiros Gaussianos irredutíveis são, da mesma forma, os divisíveis por unidades e por seus associados (múltiplos de si mesmo por unidade). Por exemplo, $1 + i$ é irredutível, porque seus divisores são somente as unidades e $(\pm 1)(1 + i)$, $(\pm i)(1 + i)$. Já $3 - i$ não é irredutível, porque

$$(1 - i)(2 + i) = 3 - i.$$

A seguir iniciamos com uma demonstração, para $\mathbb{R}[x]$, de que todos elementos podem ser escritos como produto de irredutíveis; em seguida generalizamos o enunciado para domínios Euclideanos.

Lema 5.31. *Todo polinômio diferente de zero pode ser escrito como produto de polinômios irredutíveis.*

Demonstração. Por indução no grau dos polinômios. A base se dá com $n = 1$: todo polinômio de grau um é claramente irredutível. Agora presuma que todo polinômio de grau menor que n é fatorável em irredutíveis. Considere um polinômio qualquer p de grau n. Se p é irredutível, não há mais o que mostrar. Se p não é irredutível, então $p = qr$, onde os graus de q e r são menores que n. Mas então há uma fatoração para q e uma para r, e conseguimos portanto uma fatoração para $p = qr$. □

Para inteiros Gaussianos, pode-se repetir a demonstração por indução na norma. No entanto, podemos fazer melhor: uma demonstração que valha para qualquer domínio Euclideano.

Lema 5.32. *Em um domínio Euclideano,* $\lambda(u) = 1$ *se e somente se* u *é unidade.*

O Teorema Fundamental da Aritmética vale em qualquer *domínio de fatoração única*, que não definiremos. Nos basta apenas que *todo domínio*

[2] Verifique que de fato, ambos são anéis, e que um é subanel do outro.

Euclideano é um domínio de fatoração única, e portanto vale o Teorema, que enunciamos novamente, ligeiramente modificado.

Teorema 5.33 (Fundamental da Aritmética em Domínios Euclideanos)**.** *Em um Domínio Euclideano* R*, todo elemento irredutível pode ser decomposto em um produto de irredutíveis e por uma unidade, e este produto é único.*

Demonstração. Por indução em $\lambda(x)$.

Caso base: para unidades não há o que demonstrar. Para $\lambda(x) = 2$, suponha que x seja da forma

$$x = u_1 u_2 \dots u_k(t),$$

onde u_i são unidades – e portanto $\lambda(u) = 1$. Como $\lambda(x) = 2$, e t não é unidade, vemos que t não pode ser mais fatorado (não há dois inteiros cujo produto seja dois), então t é irredutível, e é sua própria fatoração.

A hipótese é que todo elemento com norma menor que n seja fatorável em irredutíveis.

Passo: seja x com norma n. Se x é irredutível, ele é sua própria fatoração. Senão, $x = ab$, e as normas de a e b são necessariamente menores que a de x. Mas neste caso, a e b tem fatorações em irredutíveis, e a fatoração de x é a multiplicação das de a e b. □

Em qualquer domínio Euclideano há, portanto, fatoração única. A função λ usada na demonstração é, para polinômios, o grau subtraído de um[3]; para inteiros Gaussianos, a norma.

A noção de conteúdo de polinômio e o Lema de Gauss, a seguir, também valem para domínios de fatoração única; da mesma forma que fizemos com o Teorema Fundamental da Aritmética, refaremos os enunciados para Domínios Euclideanos.

Definição 5.34 (conteúdo de polinômio; polinômio primitivo)**.** O **conteúdo** de um polinômio p com coeficientes em um domínio Euclideano é o MDC de seus coeficientes, denotado $c(p)$. Se $c(p) = 1$, o polinômio é **primitivo**. ♦

Exemplo 5.35. Seja $p(x) = 6x^4 + 2x^3 + 4x$, com coeficientes em $\mathbb{Z}$ (que é domínio Euclideano). O conteúdo do polinômio é $\operatorname{mdc}(6, 2, 4) = 2$.

Os inteiros Gaussianos são, também, um domínio Euclideano. Os coeficientes do polinômio $(2 + i)x^2 - 3x$ são inteiros Gaussianos, e o polinômio é primitivo, porque seu conteúdo é $\operatorname{mdc}(2 + i, 3) = 1$. Já o polinômio $(5i-1)x^3+(4+2i)x$ tem conteúdo $\operatorname{mdc}(5i, 4 + 2i) = \{2+i, -2-i, -1+2i, 1-2i\}$ – não é, portanto, primitivo. ◄

Lema 5.36 (de Gauss)**.** *Sejam* f, g *são polinômios com coeficientes em um domínio Euclideano, nenhum deles nulo. Então* $c(fg) = c(g)\,c(f)$*. Assim, se* f *e* g *são primitivos, então* fg *também é.*

[3] Por que?

Demonstração. O Teorema afirma que a função c é multiplicativa, e depois determina que a multiplicação de primitivos; na demonstração faremos o caminho oposto, começando pela segunda parte do enunciado.

Sejam $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \ldots + b_nx^n$ dois polinômios primitivos. Seja $k = c(fg)$. Suponha que exista um primo p que divida k. Como f e g são primitivos, existe algum coeficiente a_i de f e algum b_j de g que p não divide. Mas então existe um coeficiente a_ib_j no polinômio fg, que p não pode dividir, e portanto não existe tal primo p. Assim, fg também é primitivo.

Abordamos agora a primeira parte do enunciado. Sejam dois polinômios, não necessariamente primitivos, e e h. Sejam E e H polinômios primitivos tais que

$$\begin{aligned} e &= c(e)E \\ h &= c(h)H. \end{aligned}$$

Então

$$\begin{aligned} c(eh) &= c(c(e)\,c(h)EH) \\ &= c(e)\,c(h)\,c(EH) \\ &= c(e)\,c(h), \end{aligned}$$

porque E e H são primitivos, portanto EH é primitivo e $c(EH) = 1$. □

Exercícios

Ex. 73 — Se quisermos verificar se um número n é primo por divisões sucessivas (tentamos dividí-lo por $2, 3, 5, 7, \ldots$), qual é o maior divisor que precisaremos tentar?

Ex. 74 — Determine todos os primos da forma $n^3 - 1$.

Ex. 75 — mostre que se $n^2 + 2$ é primo, então $3 \mid n$.

Ex. 76 — Prove que todo primo da forma $3n + 1$ também é da forma $6k + 1$.

Ex. 77 — Prove que se k e n são inteiros positivos e $\sqrt[k]{n}$ é racional, então $\sqrt[k]{n}$ é inteiro.

Ex. 78 — Suponha que $ab = c^n$, e que $\mathrm{mdc}\,(a, b) = 1$. Prove que existem d, e inteiros tais que

$$a = d^n, \quad b = e^n.$$

Ex. 79 — Prove que a soma de dois primos consecutivos nunca é o dobro

de um primo.

Ex. 80 — Demonstre o Lema 5.27.

Ex. 81 — Prove que todo número de Fermat F_n com $n > 1$ tem o último dígito igual a 7.

Ex. 82 — Prove que nenhum número de Fermat é quadrado perfeito.

Ex. 83 — Prove que para $n > 1$, $F_n = F_{n-1} + 2^{2^{n-1}} \cdot F_0 \cdot F_1 \cdots F_{n-2}$.

Ex. 84 — Use o Teorema 5.18 para provar que há infinitos primos.

Ex. 85 — Prove que o 3 é o único natural que é número de Fermat e também é número de Mersenne.

Ex. 86 — Mostre que todo inteiro positivo pode ser escrito como soma de números de Fibonacci.

Ex. 87 — Mostre que

$$\text{mdc}\left(n^{2^r}+1,\, n^{2^s}+1\right)$$

é sempre igual a 1 (para n par) ou 2 (para n ímpar).

Ex. 88 — Refaça a demonstração de infinitude dos primos de Euclides, mas subtraindo um ao invés de somar.

Ex. 89 — (Infinitos primos - demonstração de Stieltjes) Complete a demonstração a seguir para a infinitude dos primos: Sejam $p_1, \ldots, p_k$ todos os primos. Seja $A = p_1 p_2 \ldots p_k$, e seja $A = st$ uma fatoração de A com $s, t \geq 1$. Cada primo p_i divide s ou t, ...

Ex. 90 — (Demonstração de Euler, modernizada, para a infinitude dos primos)

i) Mostre que

$$\sum_n \frac{1}{n} = \prod_{p \text{ primo}} \frac{1}{1-\frac{1}{p}}$$

ii) Argumente que se houvesse uma quantidade finita de primos, o lado direito seria finito, e consequentemente o lado esquerdo também.

iii) Conclua que isto é impossível, observando que a série harmônica diverge.

Ex. 91 — A soma dos dígitos de um quadrado pode ser 2451?

Ex. 92 — Prove que p é primo **se e somente se** no Triângulo de Pascal, a p-ésima linha é composta de números divisíveis por p, exceto pelos dois uns nas extremidades. (A primeira linha, contendo somente o número um, tem índice zero).

$$\begin{array}{lccccccc}
 & 1 & & & & & & \\
 & 1 & 1 & & & & & \\
2^a \to & 1 & 2 & 1 & & & & \\
3^a \to & 1 & 3 & 3 & 1 & & & \\
 & 1 & 4 & 6 & 4 & 1 & & \\
5^a \to & 1 & 5 & 10 & 10 & 5 & 1 & \\
 & 1 & 6 & 15 & 20 & 15 & 6 & 1 \\
7^a \to & 1 & 7 & 21 & 35 & 35 & 21 & 7 \quad 1
\end{array}$$

(Note que a linha 2, $(1,2,1)$, contém somente o dois, que é ele mesmo divisível por dois; a linha 3 contém duas vezes o 3, divisível por 3; a linha 5, $(1,5,10,10,5,1)$, contém múltiplos de 5; a linha sete também – contém múltiplos de sete.)

Ex. 93 — Prove o Teorema de Lucas: Seja p primo, e m, n inteiros positivos, cuja representação **na base** p é

$$m = m_k m_{k-1} \cdots m_1 m_0$$
$$n = n_k n_{k-1} \cdots n_1 n_0$$

Então

$$\binom{m}{n} \equiv \prod_{j=1}^{k} \binom{m_j}{n_j} \pmod{p}.$$

Mostre como este Teorema poderia ter sido usado para resolver o Exercício 92.

Ex. 94 — A respeito do Teorema de Lucas (Exercício 93): explique detalhadamente porque, apesar de estarmos usando um sistema posicional, em que os dígitos tem significados diferentes dependendo de sua posição na representação, a ordem deles não é relevante no enunciado (simplesmente toma-se o produtório sobre todos os dígitos!)

Ex. 95 — Prove que todo inteiro positivo pode ser representado como produto de um número ímpar e uma potência de dois (mesmo que seja 2^0).

Ex. 96 — Seja $p > 5$ primo. Mostre que $p - 4 \neq n^4$, com $n \in \mathbb{Z}$.

Ex. 97 — Determine com quantos zeros termina o número 100!

Ex. 98 — Para quantos n o coeficiente binomial $\binom{100}{n}$ é ímpar?

Ex. 99 — Quantas divisões sucessivas por 1344 podemos fazer com o número 50! ?

Ex. 100 — Mostre que há infinitos primos da forma $6n + 5$.

Ex. 101 — Mostre que se p é primo em $\mathbb{Z}$, $p = 4n + 1$ e $p = a^a + b^2$, então $a + bi$ e $a = bi$ são inteiros Gaussianos irredutíveis.

Ex. 102 — Prove o Lema 5.32.

Ex. 103 — Sejam $m = p_1^{a_1} p_s^{a_2} \cdots p_k^{a_k}$ e $n = p_1^{b_1} p_s^{b_2} \cdots p_k^{b_2}$, onde $p_1, \ldots, p_k$ são primos distintos.

a) Mostre que $\text{mdc}\,(m, n) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$, onde $c_i = \min(a_i, b_i)$.

b) Calcule $\text{mdc}\left(2^3 7^9 17,\ 2^2 3^1 117^2\right)$.

Ex. 104 — Calcule a soma de todas as frações tais que o denominador e o numerador são (i) co-primos, e (ii) divisores positivos de 49000.

Ex. 105 — Qual é a probabilidade de dois inteiros serem coprimos?

Capítulo 6

Congruências

Iniciamos o estudo de congruências, que facilitam a expressão de fatos a respeito de divisibilidade.

6.1 Relações de congruênca e aritmética modular

Quando tratamos de números primos, dividimos os primos ímpares entre os da forma $4k+1$ e os da forma $4k+3$, que é o mesmo que dizer "os que deixam resto 1 quando divididos por 4 e os que deixam resto 3 quando divididos por 4". Números que deixam o mesmo resto quando divididos por um mesmo número m tem muito em comum, e os separaremos em classes de qeuivalência.

Se a e b deixam o mesmo resto quando divididos por m, então

$$\begin{aligned} a &= sm + r, \\ b &= tm + r. \end{aligned}$$

Ao subtrairmos $a - b$, teremos

$$\begin{aligned} a - b &= sm + r - tm - r \\ &= sm - tm \\ &= (s-t)m, \end{aligned}$$

portanto m divide $a - b$. Podemos, portanto, dizer que as duas afirmações são equivalentes:

i) a e b deixam o mesmo resto quando divididos por m;

ii) $m \mid a - b$.

Definição 6.1 (congruência)**.** Se $m \mid (a-b)$, ou seja, se $(a-b)/m$ é inteiro, dizemos que a é **congruente** a b módulo m, e denotamos $a \equiv b \pmod{m}$. ♦

Usualmente trataremos somente de módulos positivos, sem qualquer perda, já que $m \mid (a-b)$ e $-m \mid (a-b)$ são equivalentes.

Exemplo 6.2. $30 \equiv 16 \pmod{7}$, porque $30-16=14$, e $7 \mid 14$.
Também $12 \equiv 28 \pmod{8}$, porque $12-28=-16$, e $8 \mid -16$. ◀

Teorema 6.3. *Para todo $m > 1$, a relação de congruência módulo m é de equivalência.*

Os vários números são congruentes a k módulo m formam uma classe de equivalência. O Teorema a seguir nos possibilitará realizar operações aritméticas com as classes de congruência sem dificuldade.

Teorema 6.4. *Podemos somar e multiplicar as classes de equivalência: se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

i) $a+c \equiv b+d \pmod{m}$,

ii) $ac \equiv bd \pmod{m}$.

Demonstração. A demonstração é direta.
(i) Pela definição de congruência, $m \mid (b-a)$ e $m \mid (d-c)$, então $m \mid (b-a)+(d-c)$, logo $m \mid (b+d)-(a+c)$, e $a+c \equiv b+d \pmod{m}$.
(ii) Queremos mostrar que $m \mid (bd-ac)$. Mas $bd-ac = d(b-a)+a(d-c)$, e como m divide os dois fatores em parênteses, $(b-a)$ e $(d-c)$, m divide $d(b-a)+a(d-c)$. □

Este Teorema implica também que se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$. Também é relevante que as classes de equivalencia de inteiros módulo n formam um anel.

Teorema 6.5. *Sejam $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ as classes de equivalência módulo n. Damos o nome de $\mathbb{Z}_n$, ou $\mathbb{Z}/n\mathbb{Z}$ a este conjunto, que com as operações de soma e multiplicação descritas no Teorema 6.4, formam um anel comutativo com unidade.*

Havendo soma e multiplicação, é possível computar o valor de polinômios.

Teorema 6.6. *Se p é um polinômio com coeficientes inteiros, e $a \equiv b \pmod{m}$, então $p(a) \equiv p(b) \pmod{m}$.*

Demonstração. Seja $p(x) = k_n x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0$, e suponha $a \equiv b \pmod{m}$. Então

$$\begin{aligned} p(a) &= k_n a^n + k_{n-1} a^{n-1} + \cdots + k_1 a + k_0 \\ &\equiv k_n b^n + k_{n-1} b^{n-1} + \cdots + k_1 b + k_0 \pmod{m}, \end{aligned}$$

pelo Teorema 6.4. □

Exemplo 6.7. Sabemos que $17 \equiv 32 \equiv 2 \pmod{15}$, e escolhemos um polinômio, $p(x) = x^2 - 3x + 2$. Então

$$\begin{aligned} p(32) &= 32^2 - 3(32) + 2 = 930 \equiv 0 \pmod{15} \\ p(17) &= 17^2 - 3(17) + 2 = 240 \equiv 0 \pmod{15} \\ p(2) &= 2^2 - 3(2) + 2 = 0 \equiv 0 \pmod{15} \end{aligned}$$

Da mesma forma, temos $8 \equiv 19 \equiv 41 \pmod{11}$. Escolhemos o polinômio $q(x) = x^2 - 2x$. Então

$$\begin{aligned} q(3) &= 8^2 - 4(8) = 32 \equiv 10 \pmod{11} \\ q(19) &= 19^2 - 4(19) = 285 \equiv 10 \pmod{11} \\ q(41) &= 41^2 - 4(41) = 1517 \equiv 10 \pmod{11}. \end{aligned}$$

◀

Exemplo 6.8. Se $n \equiv 0 \pmod{2}$, então n é par; se $n \equiv 1 \pmod{2}$, é ímpar; e de maneira geral, $n \equiv 0 \pmod{k}$ é uma forma de expressar que n é divisível por k. ◀

Exemplo 6.9. Os números primos ímpares podem ser de duas formas: $p \equiv 1 \pmod{4}$ (os da forma $4k+1$), e $p \equiv 3 \pmod{4}$ (os da forma $4k+3$). ◀

Teorema 6.10. *Para todos* $a, b, c, d \in \mathbb{Z}$ *e* $1 < m \in \mathbb{Z}$,

(i) se $a \equiv b \pmod{m}$, *então* $ac \equiv bc \pmod{mc}$;

(ii) se $a \equiv b \pmod{m}$, *e* $d \mid m$, *então* $a \equiv b \pmod{d}$.

Teorema 6.11 (lei de cancelamento)**.** *Em congruências, o cancelamento de fatores se dá de acordo com a seguinte regra:*

$$ab \equiv ac \pmod{m} \text{ se e somente se } b \equiv c \left(\mod \frac{m}{\operatorname{mdc}(a,m)}\right).$$

Como caso particular,

$$\text{se } ab \equiv ac \pmod{m}. \text{ e } \operatorname{mdc}(a,m) = 1 \text{ então } b \equiv c \pmod{m}.$$

Demonstração. Mostramos primeiro que $ab \equiv ac \pmod{m}$ implica em $b \equiv c \pmod{\frac{m}{\operatorname{mdc}(a,m)}}$.

$$\begin{aligned} ab &\equiv ac \pmod{m} \\ ab - ac &= km \\ a(b-c) &= km \\ \frac{a}{\operatorname{mdc}(a,m)}(b-c) &= k\frac{m}{\operatorname{mdc}(a,m)} \\ b - c &= k\left(\frac{m}{\operatorname{mdc}(a,m)}\right) \Big/ \left(\frac{a}{\operatorname{mdc}(a,m)}\right) \end{aligned}$$

Mas $a/\operatorname{mdc}(a,m)$ e $m/\operatorname{mdc}(a,m)$ não tem fator comum (isto decorre da definição de MDC), portanto $a/\operatorname{mdc}(a,m)$ deve dividir k. Seja

$$k' = \frac{k}{a/\operatorname{mdc}(a,m)}.$$

Então

$$\begin{aligned} b - c &= k'\frac{m}{\operatorname{mdc}(a,m)} \\ b &\equiv c \pmod{\frac{m}{\operatorname{mdc}(a,m)}} \end{aligned}$$

A recíproca é verificável fazendo o caminho reverso.

O caso particular listado no enunciado acontece quando $\operatorname{mdc}(a,m) = 1$, mas pode também ser demonstrado separadamente (é um exercício bastante simples, se for usada a definição de congruência). □

Teorema 6.12. $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$ *se e somente se* $a \equiv b \pmod{\operatorname{mmc}(m_1, m_2, \ldots, m_k)}$.

Demonstração. Se $a \equiv b \pmod{m_i}$ para $i = 1, \ldots, k$. Então

$$\begin{aligned} m_1 &\mid b - a, \\ m_2 &\mid b - a, \\ &\vdots \\ m_k &\mid b - a, \end{aligned}$$

ou seja, $b - a$ é múltiplo comum de todos os m_i, e portanto o MMC deles deve dividir $b - a$:

$$\begin{aligned} &\operatorname{mmc}(m_1, m_2, \ldots, m_k) \mid b - a \\ &a \equiv b \pmod{\operatorname{mmc}(m_1, m_2, \ldots, m_k)}. \end{aligned}$$

□

Teorema 6.13. *Sejam* p *e* q *primos. Se* $a \equiv b \pmod{p}$ *e* $a \equiv b \pmod{q}$*, então* $a \equiv b \pmod{pq}$.

Demonstração. Segue diretamente do Teorema 6.12, já que $\text{mmc}(p, q) = pq$, porque p e q são primos.

□

O Lema 6.14, embora muito simples, nos permitirá trabalhar com inteiros negativos (em especial, -1) em congruências. Isto será útil em algumas demonstrações.

Lema 6.14. $m - 1 \equiv -1 \pmod{m}$.

Demonstração. Da definição de congruência,

$$\begin{aligned}(-1) - (m-1) &= -1 - m + 1 \\ &= -m\end{aligned}$$

Mas $m \mid -m$, logo Como $m \mid [(-1) - (m-1)]$, e $m - 1 \equiv -1 \pmod{m}$. □

Lema 6.15. *Se* p *é primo, então todo número* a *tem inverso único módulo* p*, ou seja, existe* $\overline{a}$ *tal que* $a\overline{a} \equiv 1 \pmod{p}$.

Demonstração. Se p é primo, $\text{mdc}(a, p) = 1$. Então, pelo Lema de Bezout, existem X, Y tais que

$$\begin{aligned} Xp + Ya &= 1 \\ Ya &= -Xp + 1 && (Ya \div p \text{ deixa resto } 1) \\ Ya &\equiv 1 \pmod{p}, \end{aligned}$$

e Y é o inverso de a módulo p.

Suponha que haja dois inversos de a, b e c ($ab \equiv 1 \pmod{p}$, e $ac \equiv 1 \pmod{p}$). Então

$$\begin{aligned} ab \equiv 1 \equiv ac &\pmod{p} \\ ab \equiv ac &\pmod{p} \\ b \equiv c &\pmod{p} && \text{(lei do cancelamento, } \text{mdc}(a, p) = 1) \end{aligned}$$

Os inversos b e c, portanto, estão na mesma classe de congruência. □

Para computar o inverso de a módulo m, podemos usar o algoritmo estendido de Euclides.

Seja $a = 4$ e $m = 35$, co-primos. Para calcular $a^{-1} \pmod{21}$, calculamos os coeficientes de Bezout para os dois números e obtemos 9 e -1.

$$9(4) - 1(35) = 1.$$

Reescrevemos de forma a isolar $1 - 9(4)$:

$$\begin{aligned} 9(4) - 1(35) &= 1 \\ -1(35) &= 1 - 9(4) \\ 35 \mid 1 &- 9(4) \\ 1 &\equiv 9(4) \pmod{35} \end{aligned}$$

e claramente 9 é inverso de 4 módulo 35, já que o produto de ambos é congruente a um.

Se a e m não são co-primos, só podemos obter coeficientes de Bezout para $aX + mY = d$, com $d > 0$. Teremos, portanto um elemento a' tal que $aa' \equiv d \pmod{m}$, mas não um inverso para a.

Por exemplo, $\text{mdc}(90, 220) = 10$. Se tentarmos obter o inverso de 90 móduilo 220, obteremos

$$\begin{aligned} 5(90) - 2(220) &= \mathbf{10} \\ 5(90) - \mathbf{10} &= 2(220) \\ 220 \mid 5(90) &- \mathbf{10} \\ 5(90) &\equiv \mathbf{10} \pmod{220}, \end{aligned}$$

e conseguimos $a' = 5$, mas $aa' = (90)(5) \equiv 10 \pmod{220}$, e não obtemos um inverso para 90 módulo 220.

Demonstraremos a seguir o Teorema de Wilson; para isso o lema 6.16 será necessário.

Lema 6.16. *Se p é primo, $a^2 \equiv 1 \pmod{p}$ se e somente se $a \equiv \pm 1 \pmod{p}$.*

Demonstração.

$$\begin{aligned} a^2 &\equiv 1 \pmod{p} \\ p \mid a^2 &- 1 \\ p \mid (a+1)&(a-1) \\ p \mid (a+1) \text{ ou } p &\mid (a-1) \qquad \text{(porque } p \text{ é primo)} \\ a \equiv -1 \pmod{p} &\text{ ou } a \equiv +1 \pmod{p}. \end{aligned}$$

□

Um exemplo simples: para $p = 11$, os quadrados são

x	x^2	$\pmod{11}$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

Somente 1 e 10 tem quadrado congruente a um módulo 11 (e $10 \equiv -1 \pmod{11}$).

Teorema 6.17 (de Wilson)**.** p *é primo se e somente se*

$$(p-1)! \equiv -1 \pmod{p}.$$

Demonstração. Suponha que n é composto; provaremos que $(n-1)! \not\equiv -1 \pmod{n}$. Se n é composto, existe algum q natural, $2 \leq q \leq n-2$, tal que $q \mid n$. Seja então $n = kq$. Suponha que $(n-1)! \equiv -1 \pmod{n}$.

$$\begin{aligned}
(n-1)! &\equiv -1 \pmod{n} \\
&= rn - 1 && \text{(para algum } r \in \mathbb{Z}\text{)} \\
&= rkq - 1 \\
&= q(rk) - 1 \\
(n-1)! &\equiv -1 \pmod{q}
\end{aligned}$$

Mas como $2 \leq q \leq n-2$, q é um dos fatores em $(n-1)!$, e $q|(n-1)!$, portanto $(n-1)! \equiv 0 \pmod{q}$ – uma contradição, e este caso não pode acontecer.

Agora passamos ao caso em que p é primo, e provaremos que $(p-1)! \equiv -1 \pmod{p}$. Pelo Lema 6.15 existe um único b tal que $ab \equiv 1 \pmod{p}$. De todos os números entre 1 e $p-1$, os únicos que são seus próprios inversos são 1 e $p-1$ (Lema 6.16). Os outros (ou seja, $2, 3, \ldots, p-2$) podem ser

agrupados em pares:

$$\begin{aligned}
\overbrace{(a_1\overline{a_1})}^{\equiv 1}\overbrace{(a_2\overline{a_2})}^{\equiv 1}\cdots\overbrace{(a_k\overline{a_k})}^{\equiv 1} &\equiv 1 \pmod{p} \\
2\cdot 3\cdot 4\cdots(p-2) &\equiv 1 \pmod{p} && (a_k \text{ são } 2\cdot 3\cdots n-2)\\
1\cdot 2\cdot 3\cdot 4\cdots(p-2) &\equiv 1 \pmod{p} && (\times 1)\\
1\cdot 2\cdot 3\cdot 4\cdots(p-2)(p-1) &\equiv p-1 \pmod{p} && (\times[p-1])\\
(p-1)! &\equiv -1 \pmod{p} && (p-1\equiv -1 \pmod{p})
\end{aligned}$$

Isto completa a demonstração. □

Para construir um exemplo, escolhemos um primo: 7. Pelo Teorema de Wilson,

$$(7-1)! = 720 \equiv -1 \pmod{7},$$

que verificamos usando a definição de congruência: $7 \mid 720-(-1)$. De fato, $721/7 = 103$.

6.2 Aplicação: critérios de divisibilidade

Uma aplicação simples de congruências é na demonstração de critérios usados para determinar se inteiros são divisíveis por 2, 3, 4, 5, 9, 10 e 11.

Teorema 6.18. *Um inteiro é par se e somente se seu último dígito (o menos significativo) é par.*

Demonstração.

$$\begin{aligned}
10 &\equiv 0 \pmod{2}\\
10^k &\equiv 0^k \equiv 0 \pmod{2}\\
x &\equiv d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n \pmod{2}\\
&\equiv d_0 \pmod{2}
\end{aligned}$$

Assim, n é par se seu último dígito for par. □

Teorema 6.19. $3 \mid n$ *se e somente se seu a soma dos dígitos de* n *é divisível por 3;* $9 \mid n$ *se e somente se seu a soma dos dígitos de* n *é divisível por 9.*

Demonstração.

$$\begin{aligned}
10 &\equiv 1 && \pmod 3\\
10^k &\equiv 1^k \equiv 1 && \pmod 3\\
x &\equiv d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n && \pmod 3\\
&\equiv d_0 + (9d_1 + d_1) + (99d_2 + d_2) + \cdots + (99\cdots 9d_n + d_n) && \pmod 3\\
&\equiv \left(d_0 + d_1 + d_2 + \cdots + d_n\right) \ + \ \left(9d_1 + 99d_2 + \cdots + 99\cdots 9d_n\right) && \pmod 3\\
&\equiv \left(d_0 + d_1 + d_2 + \cdots + d_n\right) && \pmod 3
\end{aligned}$$

Mudando o módulo para 9 obtemos o resultado para $9 \mid n$. □

Teorema 6.20. $11 \mid n$ *se e somente se a soma de seus dígitos, alternando sinal, é divisível por* 11*.*

Demonstração.

$$\begin{aligned}
10 &\equiv -1 && \pmod{11}\\
10^k &\equiv (-1)^k && \pmod{11}\\
x &\equiv d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n && \pmod{11}\\
&\equiv d_0 + (-1)d_1 + (-1)^2 d_2 + \cdots + (-1)^n d_n && \pmod{11}\\
&\equiv d_0 - d_1 + d_2 - \cdots + (-1^n)d_n && \pmod{11}
\end{aligned}$$

□

O Exercício 114 pede a demonstração de mais alguns critérios de divisibilidade.

Teorema 6.21. *Para todo inteiro positivo* n*,*

(i) $4 \mid n$ *se e somente se seus dois últimos dígitos representam um número divisível por* 4*.*

(ii) $5 \mid n$ *se e somente se seu último dígito é* 0 *ou* 5*.*

(iii) $10 \mid n$ *se e somente se seu último dígito é zero.*

Para divisores compostos por estes estudados nesta seção, basta usar simultaneamente critérios de divisibilidade: um número é divisível por 12 se e somente se é divisível por 3 e por 4, logo a soma de seus dígitos deve ser divisível por 3, *e* seus dois últimos dígitos devem representar um número divisível por 4.

Questionamos, evidentemente, sobre um critério de divisibilidade por sete. O método acima pode nos dar um critério, mas ele não é prático.

$$\begin{aligned} 10 &\equiv 3 && \pmod 7 \\ 10^k &\equiv 3^k && \pmod 7 \\ x &\equiv d_0 + 3d_1 + 3^2 d_2 + \cdots + 3^n d_n && \pmod 7 \end{aligned}$$

Assim, o que podemos dizer é que n é divisível por sete se e somente se a soma ponderada de seus dígitos, $d_0 + 3d_1 + 3^2 d_2 + \cdots + 3^n d_n$, é divisível por sete.

6.2.1 Em bases diferentes

O que fizemos para determinar critérios de divisibilidade na base dez foi buscar divisores d tais que $10 \equiv \pm 1 \pmod d$ ou $10 \equiv 0 \pmod d$. O mesmo vale para outras bases: se o divisor é d e a base é b, obteremos um critério de divisibilidade útil quando

$$b \equiv 0 \pmod d, \quad b \equiv +1 \pmod d, \quad b \equiv -1 \pmod d.$$

Exemplificamos com a base oito.

Teorema 6.22. *Na base oito,*

(i) $8 \mid n$ *se e somente se o último dígito de* n *é zero;*

(ii) $7 \mid n$ *se e somente se a soma dos dígitos de* n *é divisível por sete;*

(iii) $9 \mid n$ *se e somente se a soma alternada dos dígitos de* n *é divisível por nove.*

Demonstração.
(i)

$$\begin{aligned} 8 &\equiv 0 && \pmod 8 \\ 8^k &\equiv 0 && \pmod 8 \\ x &\equiv d_0 + 8d_1 + 8^2 d_2 + \cdots + 8^n d_n && \pmod 8 \\ &\equiv d_0 && \pmod 8 \end{aligned}$$

(ii)

$$\begin{aligned} 8 &\equiv 1 && \pmod 7 \\ 8^k &\equiv 1 && \pmod 7 \\ x &\equiv d_0 + 8d_1 + 8^2 d_2 + \cdots + 8^n d_n && \pmod 7 \\ &\equiv d_0 + d_1 + d_2 + \cdots + d_n && \pmod 7 \end{aligned}$$

(iii)

$$\begin{aligned} 8 &\equiv -1 && \pmod 9 \\ 8^k &\equiv (-1)^k && \pmod 9 \\ x &\equiv d_0 + 8d_1 + 8^2 d_2 + \cdots + 8^n d_n && \pmod 9 \\ &\equiv d_0 + (-1)d_1 + (1)d_2 + \cdots + (-1)^n d_n && \pmod 9 \\ &\equiv d_0 - d_1 + d_2 - \cdots + (-1)^n d_n && \pmod 9 \end{aligned}$$

□

6.3 Congruências Lineares e Equações Diofantinas

Equações Diofantinas são equações polinomiais onde os coeficientes são inteiros – e onde se procuram soluções inteiras. Uma equação Diofantina muito conhecida é $a^n + b^n = c^n$, que de acordo com o último Teorema de Fermat não tem soluções inteiras. Nesta seção desenvolvemos uma técnica simples para determinar soluções para o tipo mais simples de equações Diofantinas – as lineares.

Definição 6.23. Uma equação polinomial $p(x) = 0$ com coeficientes inteiros é chamada de **equação Diofantina**. Uma equação Diofantina é **linear** se o grau do polinômio p é um. ♦

Nesta seção estudamos somente as equações diofantinas lineares, da forma $ax + by = c$.

Sabemos que $ax + by = c$ (ou, equivalentemente, a congruência $ax \equiv c \pmod b$) tem solução se e somente se $\operatorname{mdc}(a, b) = d \mid c$, Para resolver a equação, primeiro a simplificamos, dividindo-a por d:

$$Ax + By = C, \quad A = \frac{a}{\operatorname{mdc}(a,b)}, B = \frac{b}{\operatorname{mdc}(a,b)}, C = \frac{c}{\operatorname{mdc}(a,b)}$$

Agora temos $\operatorname{mdc}(A, B) = 1$. Considere a equação

$$Ar + Bs = 1.$$

Podemos facilmente encontrar uma solução para ela usando o algoritmo de Euclides para o MDC: basta calcular o MDC de A e B; chegaremos a uma equação da forma $\alpha\beta + \gamma\delta = 1$.

Posteriormente, multiplicamos a equação e sua solução por C:

$$ArC + BsC = C,$$

e temos uma solução para a equação original.

Exemplo 6.24. Resolveremos a equação $15x+51y = 42$. Como $\text{mdc}\,(15, 51) = 3$ e $3 \mid 42$, as soluções que procuramos são as mesmas de

$$5x + 17y = 14.$$

Agora resolvemos $5x' + 17y' = 1$. Calculamos $\text{mdc}\,(17, 5)$ e obtemos os coeficientes de Bezout:

$$5(7) + 17(-2) = 1.$$

Temos as soluções $x' = 7, y' = -2$. Multiplicando por 14 obtemos

$$x = 98, \quad y = -28.$$

Finalmente, verificamos facilmente que $5(98) + 17(-28) = 14$.

Esta é, no entanto, somente uma das infinitas soluções para a equação. Se $ax + by = c$, então também é verdade que $a(x + kb) + b(y - ka) = c$, para todo $k \in \mathbb{Z}$:

$$\begin{aligned} a(x + kb) + b(y - ka) &= c \\ ax + kab + by - kab &= c \\ ax + by &= c \end{aligned}$$

Para determinarmos a forma geral da solução, precisamos calcular

$$\begin{aligned} a(x + bk) + b(y - ak) &= 42 \\ 15(x + 51k) + 51(y - 15k) &= 42 \\ 15(98 + 51k) + 51(-28 - 15k) &= 42. \end{aligned}$$

Na última linha, usamos $x + kb = 98 + 51k$, $y + ka = -28 - 15k$. As soluções são os pares (x, y) no conjunto

$$\{(98 + 51k, -15k - 28) \mid k \in \mathbb{Z}\}. \qquad \blacktriangleleft$$

Exemplo 6.25. A equação diofantina $6x+4y = 25$ não tem soluções, porque $\text{mdc}\,(6, 4) = 2$, e $2 \nmid 25$. $\blacktriangleleft$

Exemplo 6.26. Queremos todas as soluções para $6x + 10y = 164$, com uma restrição adicional: $x, y \geq 9$.

As soluções serão as mesmas para

$$3x + 5y = 82,$$

portanto calculamos o MDC e os coeficientes de Bezout para 3 e 5:

$$3(2) + 5(-1) = 1$$

Multiplicamos por 82, e obtemos

$$3(164) + 5(-82) = 82.$$

Esta solução ainda não é uma das que queremos, porque $y = -82 < 9$. A forma geral é, no entanto,

$$3(164 + 5k) + 5(-82 - 3k) = 82$$

e as soluções que queremos são

$$164 + 5k \geq 9 \quad \text{(i)}$$
$$-82 - 3k \geq 9 \quad \text{(ii)}$$

Resolvemos (i):

$$5k \geq 9 - 164$$
$$k \geq -\frac{155}{5} = -31$$

E agora, (ii):

$$-3k \geq 82 + 9$$
$$k \leq -\frac{91}{3} \approx -30.333$$

Assim, somente podemos usar $k = -31$. ◀

A equação diofantina $ax - my = b$ é claramente equivalente à congruência linear $a \equiv b \pmod{m}$, que tem infinitas soluções (quando há alguma). No entanto, podemos afirmar algo a respeito da quantidade de soluções incongruentes módulo m.

Teorema 6.27. *A congruência* $ax \equiv b \pmod{m}$ *tem* $d = \text{mdc}(a, m)$ *soluções incongruentes módulo* m *se e somente se* $d \mid b$. *Se* $d \nmid b$, *então não há soluções.*

Demonstração. Seja $d = \text{mdc}(a, m)$. Como a equação Diofantina $ax - my = b$ tem soluções se e somente se $d \mid b$, precisamos apenas mostrar que há d soluções incongruentes módulo m.

Se $d \mid b$, reescrevemos a equação dividindo todos por d:

$$Ax \equiv B \pmod{M}, \quad A = \frac{a}{d}, B = \frac{b}{d}, M = \frac{m}{d}.$$

Como agora A e M são co-primos, existe um único inverso para A módulo M, que denotaremos $\overline{A}$. Temos portanto $A\overline{A} \equiv 1 \pmod{M}$.

$$\begin{aligned} Ax &\equiv B \pmod{M} \\ \overline{A}Ax &\equiv \overline{A}B \pmod{M} \\ x &\equiv \overline{A}B \pmod{M} \\ M &\mid \overline{A}B - x \\ kM &= \overline{A}B - x \\ x &= \overline{A}B - kM, \end{aligned}$$

Há d valores de x incongruentes módulo m. Isso é consequência do Teorema 6.10, já que $d \mid m$. □

Exemplo 6.28. Resolveremos $396x \equiv 729 \pmod{27}$.

Como $\operatorname{mdc}(396, 27) = 9$ e $9 \mid 729$, dividimos a equação por 9:

$$44x \equiv 81 \pmod{3}.$$

Como 44 é co-primo com 3, tem inverso: $(44)(8) \equiv 1 \pmod{3}$, e

$$\begin{aligned} (44)(8)x &\equiv (8)(81) && \pmod{3} \\ x &\equiv 648 && \pmod{3} \\ 3 &\mid 648 - x \\ 3k &= 648 - x \\ x &= 3k + 648 \end{aligned}$$

Temos 9 valores de k que são incongruentes módulo 27. Estes nos darão as 9 soluções:

k	$9k + 648$	$\pmod{27}$
0	648	0
1	651	3
2	654	6
3	657	9
4	660	12
5	663	15
6	666	18
7	669	21
8	672	24
9	675	0
10	678	3
⋮	⋮	⋮

As nove primeiras linhas mostram os nove valores incongruentes. Na décima (para $k = 9$), a sequência começa a se repetir. ◀

6.4 O Teorema Chinês dos Restos

Já tratamos de como resolver congruências lineares em uma variável. Agora consideramos como resolver um sistema de congruências lineares simultâneas.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

O problema de resolver congruências simultâneas foi estudado bastante cedo na História da Matemática. No Século IV, o Chinês Sun Tsu teria proposto o problema:

> *"Há certas coisas cuja quantidade é desconhecida. Repetidamente divididas por 3, o resto é 2; por 5, o resto é 3; e por 7 o resto é 2. Qual é a quantidade?"*[1]

Também parece ter surgido no trabalho do Indiano Brahmagupta, nascido no ano 598:

> *"Uma senhora idosa vai ao mercado e um cavalo chuta seu cesto, quebrando os ovos que ela havia comprado. O cavaleiro se oferece para pagar pelo prejuízo e pergunta quantos ovos ela tinha. Ela não se lembra do número exato, mas quando os separou dois de cada vez, um havia sobrado; O mesmo aconteceu quando os separou três, quatro, cinco e seis de cada vez, mas quando os separou em grupos de sete, nenhum havia sobrado. Qual é a menor quantidade de ovos que ela poderia ter comprado?"*[2]

Enunciamos o Teorema a seguir, e damos uma demonstração construtiva.

Teorema 6.29 (Chinês dos restos)**.** *Sejam* $m_1, m_2, \ldots, m_r$ *inteiros co-primos*

[1] D. Wells, The Penguin Book of Curious and Interesting Puzzles, Penguin Books, 1992.
[2] Oystein Ore, Number Theory and Its History, Dover Publications, 1976.

entre si. Então o sistema de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

tem solução única módulo $M = m_1 m_2 \cdots m_r$*, para quaisquer* $a_1, a_2, \ldots, a_r$.

Demonstração. Para $k = 1, 2, \ldots, r$, defina

$$M_k = \frac{M}{m_k}.$$

Então $\text{mdc}\,(M_k, m_k) = 1$ para todo k, porque os m_k são co-primos, e de M_k retiramos o fator m_k.

Agora, para cada M_k, denote $\overline{M_k}$ como o inverso de M_k módulo m_k. Ou seja,

$$M_k \overline{M_k} \equiv 1 \pmod{m_k}.$$

A solução do sistema é

$$x \equiv a_1 M_1 \overline{M_1} + a_2 M_2 \overline{M_2} + \cdots + a_r M_r \overline{M_r} \pmod{M}. \tag{6.1}$$

Justificamos. Note que na soma acima,

$$\begin{aligned} a_i M_i \overline{M_i} &\equiv 0 \pmod{m_j} \\ a_i M_i \overline{M_i} &\not\equiv 0 \pmod{m_i} \end{aligned}$$

onde $i \neq j$ porque $m_j \mid M_i$, e portanto $a_i M_i \overline{M_i} \equiv (a_i)(0)(\overline{M_i}) \equiv 0 \pmod{m_j}$.

Assim, para cada m_i a soma será

$$\begin{aligned} x &\equiv a_1(0)\overline{M_1} + a_2(0)\overline{M_2} + \cdots + a_i M_i \overline{M_i} + \cdots + a_r(0)\overline{M_r} && \pmod{m_i} \\ &\equiv a_i M_i \overline{M_i} && \pmod{m_i} \\ &\equiv a_i && \pmod{m_i} \end{aligned}$$

A última linha é válida porque $M_i \overline{M_i} \equiv 1 \pmod{m_i}$.

Conseguimos então x que é congruente a cada um dos a_i módulo m_i, e que é único módulo M (porque o definimos como classe de congruência módulo M, na equação 6.1). □

Exemplo 6.30. Resolveremos o sistema

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 3 \pmod{10} \end{aligned}$$

Temos $M = (3)(7)(10) = 210$, e

$$\begin{aligned} M_1 &= (7)(10) = 70 \\ M_2 &= (3)(10) = 30 \\ M_3 &= (3)(7) = 21 \end{aligned}$$

Os inversos são

$$\begin{aligned} \overline{M_1} &= 1 \pmod 3 \\ \overline{M_2} &= 4 \pmod 7 \\ \overline{M_3} &= 1 \pmod{10} \end{aligned}$$

Assim,

$$\begin{aligned} x &\equiv 2(70)(1) + 1(30)(4) + 3(21)(1) \\ &\equiv 323 \\ &\equiv 113 \pmod{210} \end{aligned}$$

A solução do sistema é $x \equiv 113 \pmod{210}$, como podemos verificar:

$$\begin{aligned} 113 &\equiv 2 \pmod 3 \\ 113 &\equiv 1 \pmod 7 \\ 113 &\equiv 3 \pmod{10} \end{aligned}$$

Note que toda a classe de congruência 113 módulo 210 é solução para o sistema: $\{\ldots, -307, -97, 113, 323, 533, \ldots\} = \{210k + 113 \mid k \in \mathbb{Z}\}$. ◀

6.4.1 Módulos não co-primos

O Teorema Chinês dos Restos pode ser generalizado para sistemas onde os módulos não são co-primos, mas sistemas dessa forma nem sempre tem solução. Nesta seção detalhamos o critério para existência da solução, além de uma demonstração construtiva que permite obte-la, quando existir.

Nos Lemas a seguir trataremos de sistemas de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned} \tag{6.2}$$

Lema 6.31. *Se, para algum* $i \neq j$, $\mathrm{mdc}(m_i, m_j) \nmid (a_i - a_j)$, *então o sistema de congruências 6.2 não tem solução.*

Demonstração. Se $\mathrm{mdc}(m_i, m_j) \nmid (a_i - a_j)$, então

$$a_i \not\equiv a_j \pmod{\mathrm{mdc}(m_i, m_j)},$$

mas isso significa que x não pode satisfazer simultaneamente as duas equações

$$x \equiv a_i \pmod{\mathrm{mdc}(m_i)}, x \equiv a_j \pmod{\mathrm{mdc}(m_j)}$$

Lema 6.32. *Se, para todo* $i \neq j$, $\mathrm{mdc}(m_i, m_j) \mid (a_i - a_j)$, *então o sistema de congruências 6.2 tem solução.*

Demonstração. Em cada congruência $x \equiv a_i \pmod{m_i}$, denotamos a fatoração de m_i por $m_i = p_1^{i_1} p_2^{i_2} \cdots$ (ou seja, $p_1, p_2, \ldots$ são todos os primos, e $i_1, i_2, \ldots$ são os expoentes dos primos na fatoração de m_i – note que somente alguns dos primos terão expoente diferente de zero). Agora, trocamos cada uma destas congruências da forma $x \equiv a_i \pmod{m_i}$ por um conjunto de congruências, substituindo m_i em cada uma por uma das potências de primo na fatoração de m_i:

$$\begin{aligned} x &\equiv a_i \pmod{p_1^{i_1}} \\ x &\equiv a_i \pmod{p_2^{i_2}} \\ &\vdots \\ x &\equiv a_k \pmod{p_k^{i_k}}. \end{aligned}$$

O sistema resultante é equivalente ao original já que, sendo p, q primos, $x \equiv a_i \pmod{p^e}$, $x \equiv a_i \pmod{q^f}$ implica que $x \equiv a_i \pmod{p^e q^f}$.

Eliminamos os módulos compostos. No entanto, o sistema resultante pode ainda ter módulos que não são co-primos entre si, porque o mesmo primo pode estar presente na fatoração de mais de um m_i.

Suponha agora que

$$\begin{aligned} m_i &= \cdots p^N \cdots, \\ m_j &= \cdots p^n \cdots, \\ N &> n. \end{aligned}$$

Ou seja, p^N, com expoente maior, está na fatoração de m_i; p^n, com expoente menor, está na fatoração de m_j. Então $p^n \mid \text{mdc}(m_i, m_j)$.

Como $\text{mdc}(m_i, m_j) \mid (a_i - a_j)$,

$$\begin{aligned} &p^n \mid \text{mdc}(m_i, m_j) \mid (a_i - a_j) \\ &p^n \mid (a_i - a_j) \\ &a_i \equiv a_j \pmod{p^n}. \end{aligned} \tag{6.3}$$

Observamos agora que, se $N > n$,

$$\begin{aligned} x &\equiv a_i \pmod{p^N} && \\ p^N &\mid x - a_i && \text{(definição de congruência)} \\ p^n &\mid x - a_i && \text{(N>n)} \\ x &\equiv a_i \pmod{p^n} && \text{(definição de congruência)} \end{aligned}$$

e $x \equiv a_i \pmod{p^N}$ implica em $x \equiv a_i \pmod{p^n}$. Mas por 6.3, isso implica que $x \equiv a_j \pmod{p^n}$, e concluímos que

$$x \equiv a_i \pmod{p^N}$$

implica em

$$x \equiv a_j \pmod{p^n},$$

e podemos remover, dentre as congruências de módulo potência de um mesmo primo, todas exceto a da maior potência.

O resultado é um sistema de congruências equivalente ao original, mas onde cada congruência tem como módulo uma potencia de primo, sem que haja repetição dos primos. Os módulos são, portanto, co-primos, e pelo Teorema Chinês dos Restos, podemos resolver o sistema. □

O Lemma 6.33 determina que a solução do sistema, quando existe, é única módulo MMC dos módulos. Sua demonstração é pedida no Exercício 129.

Lema 6.33. *Se os módulos em um sistema de congruências como o descrito no Lema 6.32 não são co-primos e existe uma solução, ela é única módulo* $\text{mmc}(m_1, m_2, \ldots, m_k)$.

Os lemas anteriores tem como consequência a validade do Teorema a seguir.

Teorema 6.34. *Sejam* $m_1, m_2, \ldots, m_k \in \mathbb{N}$ *e* $d = \text{mdc}\,(m_1, m_2, \ldots, m_k)$. *Então um sistema de congruências*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

tem solução se e somente se $d \mid (a_i - a_j)$ *para todos* $i \neq j$*, e a solução é única módulo* $\text{mmc}(m_1, m_2, \ldots, m_k)$.

Exemplo 6.35. Considere o sistema de congruências

$$\begin{aligned} x &\equiv 31 \pmod{72} \\ x &\equiv 15 \pmod{20} \\ x &\equiv 13 \pmod{42} \end{aligned}$$

Verificamos que $\text{mdc}\,(m_i, m_j) \mid (a_i - a_j)$:

$$\begin{aligned} \text{mdc}\,(72, 20) &= 4 \mid 16 = 31 - 15 \\ \text{mdc}\,(72, 42) &= 6 \mid 18 = 31 - 13 \\ \text{mdc}\,(20, 42) &= 2 \mid 2 = 15 - 13 \end{aligned}$$

Substituímos as congruências por outras, com módulos potencia de primo.

$$\begin{aligned} 72 &= 2^3 \cdot 3^2 \\ 20 &= 2^2 \cdot 5 \\ 42 &= 2^2 \cdot 3 \cdot 7 \end{aligned}$$

portanto o primeiro sistema equivalente é

$$\begin{aligned} x &\equiv 31 \pmod{2^3} \\ x &\equiv 31 \pmod{3^2} \\ x &\equiv 15 \pmod{2^2} \\ x &\equiv 15 \pmod{5} \\ x &\equiv 13 \pmod{2} \\ x &\equiv 13 \pmod{3} \\ x &\equiv 13 \pmod{7} \end{aligned}$$

Eliminamos $x \equiv 15 \pmod{2^2}$, $x \equiv 13 \pmod{2}$ e $x \equiv 13 \pmod{3}$, e obtemos

$$\begin{aligned} x &\equiv 31 \pmod{2^3} \\ x &\equiv 31 \pmod{3^2} \\ x &\equiv 15 \pmod{5} \\ x &\equiv 13 \pmod{7}. \end{aligned}$$

Agora os módulos são co-primos, e podemo usar o Teorema Chinês dos restos. Obtemos $x = 895$, que será único módulo $\text{mmc}(72, 20, 42) = 2520$. É trivial verificar o resultado:

$$\begin{aligned} 895 &\equiv 31 \pmod{72} \\ 895 &\equiv 15 \pmod{20} \\ 895 &\equiv 13 \pmod{42}. \end{aligned}$$ ◀

6.5 O Teorema Chinês dos Restos, novamente

Apresentamos novamente o Teorema Chinês dos Restos, mas desta vez usando isomorfismo entre anéis.

Seja $n = ab$, com $\text{mdc}(a, b) = 1$, e considere os anéis

$$\begin{aligned} \mathbb{Z}_n &= \{0, 1, 2, \ldots, n-1\} \\ \mathbb{Z}_a &= \{0, 1, 2, \ldots, a-1\} \\ \mathbb{Z}_b &= \{0, 1, 2, \ldots, b-1\} \end{aligned}$$

E observe que o produto cartesiano

$$\begin{aligned} \mathbb{Z}_a \times \mathbb{Z}_b &= \{(x, y) \mid x \in \mathbb{Z}_a, y \in \mathbb{Z}_b\} \\ &= \{(0,0), (0,1), \ldots, (a-1, b-1)\} \end{aligned}$$

também é anel. Evidentemente,

$$|\mathbb{Z}_n| = |\mathbb{Z}_a|\,|\mathbb{Z}_b|.$$

Definimos agora uma função $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$, tal que

$$f(x) = \Big(x \pmod{a},\ x \pmod{b}\Big). \tag{6.4}$$

É comum autores apresentarem esta função sem explicitar os módulos, "$f(x) = (x, x)$". Para evitar a confusão visual da notação de módulo e também evitar a ambiguidade, denotaremos por $[x]_z$ a classe de equivalência x

$(\text{mod } z)$, e portanto

$$f(x) = ([x]_a,\ [x]_b)\,.$$

Enunciamos uma nova versão do Teorema Chinês dos Restos. Este enunciado, em um primeiro exame, não parece ter relação com o Teorema Chinês dos Restos enunciado anteriormente (Teorema 6.29) – mas a relação ficará clara adiante.

Teorema 6.36 (Chinês dos Restos)**.** *A função* f*, definida na equação 6.4, é bijetora.*

Demonstração. Como o domínio e contra-domínio são finitos e tem a mesma cardinalidade, se f for injetora, ela será também bijetora, necessariamente. Verificamos portanto que f é injetora.

Suponha, por absurdo, que f não é injetora:

$$\begin{aligned} [x_1]_n &\neq [x_2]_n, \\ f([x_1]_n) &= ([x]_a, [x]_b), \qquad (6.5) \\ f([x_2]_n) &= ([x]_a, [x]_b). \qquad (6.6) \end{aligned}$$

Mas destas equações, olhando apenas para a primeira parte dos pares ordenados, vemos que

$$\begin{aligned} &\text{de 6.5,}\ \ x_1 \equiv x \pmod a \\ &\text{de 6.6,}\ \ x_2 \equiv x \pmod a \end{aligned}$$

Disso temos que

$$x_1 \equiv x_2 \pmod a.$$

Da mesma forma, se olharmos o lado direito dos pares ordenados, teremos

$$x_1 \equiv x_2 \pmod b.$$

Mas se x_1 e x_2 são congruentes nos dois módulos, então serão congruentes módulo $ab = n$. Chegamos à contradição que havíamos previsto, e terminamos a demonstração. □

Um exemplo simples ilustra claramente o que diz o Teorema 6.36.

Sejam $a = 3, b = 4$, e $n = ab = 12$. A tabela a seguir mostra a função

$f(x)$, que é claramente bijetora.

x	(x,x)	x	(x,x)
0	$(0,0)$	6	$(0,2)$
1	$(1,1)$	7	$(1,3)$
2	$(2,2)$	8	$(2,0)$
3	$(0,3)$	9	$(0,1)$
4	$(1,0)$	10	$(1,2)$
5	$(2,1)$	11	$(2,3)$

A conexão deste Teorema com o Teorema Chinês onde apresentamos um sistema de congruências fica clara com o seguinte exemplo.

Exemplo 6.37. Sejam $a = 10$ e $b = 17$, com $n = ab = 170$. Como f é bijeção, existe algum x tal que $f(x) = (5, 12)$; queremos determiná-lo. Mas isto é o mesmo que buscar a solução para

$$\begin{aligned} x &\equiv 5 \pmod{10} \\ x &\equiv 12 \pmod{17} \end{aligned}$$

Considere a equação

$$17s + 10t = 1.$$

Obtemos os coeficientes de Bezout, $s = 3, t = -5$:

$$3(17) - 5(10) = 1.$$

Agora multiplicamos, e chegamos a

$$51 - 50 = 1.$$

Observamos que

$$\begin{aligned} 51 &\equiv 1 \pmod{10} \\ 51 &\equiv 0 \pmod{17} \\ -50 &\equiv 0 \pmod{10} \\ -50 &\equiv 1 \pmod{17} \end{aligned}$$

Temos dois números que são congruentes a zero e um nos dois módulos, de forma que podemos escrever

$$\begin{aligned} [1]_{10}(5) + [0]_{10}(12) &\equiv 5 \pmod{10} \\ [0]_{17}(5) + [1]_{17}(12) &\equiv 12 \pmod{17} \end{aligned}$$

Ou seja,

$$(51)(5) + (-50)(12) \equiv 5 \pmod{10}$$
$$(51)(5) + (-50)(12) \equiv 12 \pmod{17}$$

Não é coincidência os lados esquerdos das congruências serem idênticos: nos os construímos assim. Agora, uma vez que

$$51(5) + (-50)12 = -345,$$

percebemos que

$$-345 \equiv 5 \pmod{10}$$
$$-345 \equiv 12 \pmod{17}$$

que é o que procurávamos. ◀

Nesta Seção *usamos* isomorfismos entre anéis para obter um resultado equivalente ao Teorema Chinês dos Restos, mas ainda o aplicamos somente em $\mathbb{Z}_n$. O Teorema pode ser também generalizado para que seja *aplicado em* anéis arbitrários – tópico fora do escopo deste texto.

Já tratamos de como resolver um sistema com duas congruências. Não é difícil adaptar o segundo enunciado do Teorema Chinês dos Restos (Teorema 6.36) para um número arbitrário de congruências.

6.6 Congruências lineares em n variáveis

Tratamos anteriormente de congruências lineares em uma única variável. Queremos também poder resolver congruências lineares em várias variáveis,

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}.$$

Da mesma forma que para congruências lineares em uma variável, é necessário que $\text{mdc}(a_1, a_2, \ldots, a_n, m) \mid b$ para que haja solução.

Primeiro observamos que esta congruência é equivalente à equação Diofantina

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n - b = km$$

onde as incógnitas são os a_i e k.

Para maior clareza, iniciamos com um exemplo em três variáveis,

$$a_1x_1 + a_2x_2 + a_3x_3 = s \tag{6.7}$$

Sabemos que, fixados $a_1, a_2 \in \mathbb{Z}$ os valores possíveis para $a_1x + a_2y$ são

múltiplos de $\operatorname{mdc}(a_1, a_2)$. Assim, a equação 6.7 pode ser reescrita

$$\operatorname{mdc}(a_1, a_2)\, r + a_3 x_3 = s,$$

com duas incógnitas (r e x_3). Agora podemos resolvê-la obtendo os coeficientes de Bezout.

É possível adaptar este método para qualquer número de variáveis, eliminando uma de cada vez, desde que $\operatorname{mdc}(a_1, a_2, \ldots, a_n) \mid s$. O Exercício 131 pede o desenvolvimento deste algoritmo.

É possível também determinar o número de soluções da congruência; é disso que trata o Teorema 6.38. O Exercício 132 pede a demonstração deste Teorema.

Teorema 6.38. *Sejam $a_1, a_2, \ldots, a_n, m$ inteiros positivos, e seja também $d = \operatorname{mdc}(a_1, a_2, \ldots, a_n, m)$. Então a congruência*

$$a_1 x_1 + \cdots + a_n x_n \equiv b \pmod{m}$$

tem $d m^{n-1}$ soluções incongruentes módulo m, quando $d \mid b$. Se $d \nmid b$, não há soluções.

6.7 Congruências polinomiais de qualquer grau

É natural que tentemos obter também soluções para congruências não lineares. Nesta seção tratamos das congruências polinomiais em uma variável.

Definição 6.39 (congruência polinomial)**.** Uma congruência da forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x_1 + a_0 \equiv 0 \pmod{m},$$

com $a_i \in \mathbb{Z}$, com pelo menos um $a_i \not\equiv 0 \pmod{m}$, é uma **congruência polinomial**. O **grau** da congruência é o maior j tal que $a_j \not\equiv 0 \pmod{m}$. ♦

É importante observar que o grau de uma congruência não é necessariamente igual ao do polinômio usado para descrevê-la. Por exemplo, o grau do polinômio $10x^2+3x-2$ é dois; mas o grau da congruência $10x^2+3x-2 \equiv 0 \pmod 5$ é um, e não dois, porque $10 \equiv 0 \pmod 5$. Esta congruência na verdade é equivalente a $0x^2 + 3x - 2 \equiv 0 \pmod 5$, ou seja, $3x - 2 \equiv 0 \pmod 5$, já que $10x^2$ sempre será congruente a zero módulo 5, e pode ser ignorado.

Teorema 6.40. *Se a é solução para uma congruência $f(x) \equiv 0 \pmod m$ e $d \mid m$, então a também é solução para $f(x) \equiv 0 \pmod d$.*

Demonstração. Segue imediatamente do Teorema 6.10 (parte ii). □

O fato de toda solução módulo d ser também solução módulo m, múltiplo de d, não implica que não haja *mais* soluções módulo m. O Teorema 6.41

mostra que pode, realmente, haver mais soluções. Na demonstração dada usamos o Teorema Chinês dos Restos, na segunda forma, para contagem, ao invés de para obtenção das soluções.

Teorema 6.41. *Seja* $f(x)$ *um polinômio com coeficientes inteiros, e* m *um inteiro positivo. Denote por* $N(m)$ *a quantidade de soluções da congruência* $f(x) \equiv 0 \pmod{m}$. *Então, se* $m = m_1 m_2$, *com* m_1 *e* m_2 *co-primos,* $N(m) = N(m_1)N(m_2)$.

Demonstração. Se x é solução para $f(x) \equiv 0 \pmod{m}$, pelo Teorema 6.40 x também é solução para $f(x) \equiv 0 \pmod{m_1}$ e para $f(x) \equiv 0 \pmod{m_2}$. Pelo Teorema Chinês dos restos, como $\text{mdc}(m_1, m_2) = 1$, então $g(x) = (x, x)$ é bijeção entre $\mathbb{Z}_m$ e $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Assim, para cada solução módulo m temos um par (x_1, x_2), com $x_1 \in \mathbb{Z}_{m_1}$ e $x_2 \in \mathbb{Z}_{m_2}$. O fato de g ser bijeção nos garante que o número de soluções módulo m é $N(m_1)N(m_2)$. □

Claramente, pode-se obter as soluções de uma congruência polinomial módulo m fatorando m e obtendo as soluções módulo p^k, para cada potência de primo na fatoração[3].

Voltamos a atenção portanto para congruências polinomiais da forma $f(x) \equiv 0 \pmod{p^a}$, com p primo.

Será interessante se pudermos reduzir o problema de obter solução para uma congruência módulo p^a a outra, módulo p^b, com $b < a$.

Procuramos as soluções de uma congruência módulo p^a. Para qualquer $b < a$, como $p^b \mid p^a$, o Teorema 6.40 nos garante que as soluções módulo p^b também são soluções módulo p^a. Obteremos agora um método para, a partir de soluções módulo p^b, chegar a soluções módulo p^a.

Lema 6.42 (de Hensel)**.** *Seja* $f(x)$ *um polinômio com coeficientes inteiros. Se* $x \in \mathbb{Z}$, $f(x) \equiv 0 \pmod{p^b}$ *e* $f'(x) \not\equiv 0 \pmod{p}$, *então existe um único* t *inteiro positivo tal que* $f(x + tp^b) \equiv 0 \pmod{p^{b+1}}$.

Quando $f'(x) \equiv 0 \pmod{p}$, a solução é *singular*; de outra forma, é *não singular*.

O Lema de Hensel é semelhante ao método de Newton – o que ficará claro em sua demonstração.

Demonstração. Suponha que $f(x_j) \equiv 0 \pmod{p^j}$. Escrevemos a expansão de Taylor de $f(x + tp^j)$:

$$f(x + tp^j) = f(x) + tp^j f'(x) + \frac{(tp^j)^2 f''(x)}{2!} + \cdots + \frac{(tp^b)^n f^{(n)}(x)}{n!}.$$

[3] O que não significa que seja um método prático. Para m grande, não são conhecidos algoritmos eficientes para fatoração.

Aogra, cada termo $a_j x^j$ no polinômio $f(x)$ contribui em cada $f^{(k)}(x)/k!$ com o termo

$$\frac{j(j-1)\cdots(j-k+1)}{k!}c_j x^{j-k} = \binom{j}{k} c_j x^{j-k}.$$

Isto significa que todos os $f^{(k)}(x)/k!$ são inteiros. Logo,

$$f(x + tp^j) \equiv f(x) + tp^j f'(x) \pmod{p^{j+1}}$$

e podemos determinar t tal que

$$f(x) + tp^j f'(x) \equiv 0 \pmod{p^{j+1}}.$$

Mas $p^j \mid f(x)$, então temos

$$tf'(x) \equiv -\frac{f(x)}{p^j} \pmod{p}.$$

Se $\operatorname{mdc}(f'(x), p) = 1$, multiplicamos a congruência pelo inverso de $f'(x)$, obtendo

$$t \equiv -\left[f'(x)\right]^{-1} \frac{f(x)}{p^b} \pmod{p}.$$

Assim, se a_j é solução para $f(x) \equiv 0 \pmod{p^j}$, então uma solução módulo p^{j+1} é

$$\begin{aligned} a_{j+1} &= a_j + tp^j \\ &= a_j + \left(-\left[f'(a_j)\right]^{-1} \frac{f(a_j)}{p^j}\right) p^j \\ &= a_j - \left[f'(a_j)\right]^{-1} f(a_j). \end{aligned}$$

□

O exercício 133 pede a contagem do número de soluções (o enunciado do Corolário 6.43).

Corolário 6.43. *O número de soluções será zero se* $p \mid f'(x)$ *mas* $p \nmid \frac{f(x)}{p^b}$*; um se* $p \nmid f'(x)$*, e* p *se* p *divide tanto* $f'(x)$ *como* $\frac{f(x)}{p^b}$*.*

Exemplo 6.44. Tentaremos identificar as soluções da congruência

$$x^3 + 2x - x - 2 \equiv 0 \pmod{27}.$$

Temos os polinômios

$$\begin{aligned} f(x) &= x^3 + 2x - x - 2 \\ f'(x) &= 3x^2 + 4x - 1. \end{aligned}$$

Como $27 = 3^3$, tentaremos inicialmente encontrar soluções para

$$f(x) \pmod 3$$

Uma vez que temos um primo suficientemente pequeno, podemos tentar as únicas possibilidades de solução, $0, 1, 2$.

$$\begin{aligned} f(0) = -2 &\equiv 1 \pmod 3 \\ f(1) = 0 &\equiv 0 \pmod 3 \\ f(2) = 12 &\equiv 0 \pmod 3 \end{aligned}$$

As soluções módulo três são 1 e 2. Verificamos as derivadas de f nesses valores.

$$\begin{aligned} f'(1) = 6 &\equiv 0 \pmod 3 \\ f'(2) = 19 &\equiv 1 \pmod 3 \end{aligned}$$

O Lema de Hensel não nos permite usar a solução 1, porque $f'(1) \equiv 0 \pmod 3$. Usaremos $x_1 = 2$. O inverso de $f'(2)$ é

$$\begin{aligned} \left[f'(2)\right]^{-1} &\equiv (1)^{-1} \pmod 3 \\ &\equiv 1 \pmod 3. \end{aligned}$$

A solução módulo 3^2 é

$$\begin{aligned} x_2 &= x_1 - \left[f'(2)\right]^{-1} f(2) \\ &= 2 - (1)(12) \\ &= -10 \\ &\equiv 8 \pmod 9 \end{aligned}$$

Verificamos:

$$f(8) = 630 \equiv 0 \pmod 9.$$

A solução módulo 3^3 é

$$\begin{aligned} x_3 &= x_2 - \left[f'(2)\right]^{-1} f(8) \\ &= 8 - (1)(630) \\ &= -622 \\ &\equiv 26 \pmod{27} \end{aligned}$$

Finalmente,

$$f(26) = 18900 \equiv 0 \pmod{27}.$$

Note que $p \nmid f'(x)$ – ou seja, $3 \nmid 19$, e pelo Corolário 6.43, há uma só solução. ◀

O Lema de Hensel trata apenas de soluções não-singulares. É possível, em algumas situações, elevar uma solução singular módulo p^j para j^{j+1}, conforme o enunciado do Teorema 6.45. A demonstração (na verdade muito simples) é pedida no exercício 134.

Teorema 6.45. *Seja* x_j *uma solução para* $f(x) \equiv 0 \pmod{p^j}$. *Se* $f(x_j) \equiv 0 \pmod{p^{j+1}}$ *então* $f(a + kp^j) \equiv 0 \pmod{p^{j+1}}$, para todo inteiro k.

Exemplo 6.46. Tentaremos identificar as soluções da congruência

$$x^3 - 100x \equiv 0 \pmod{25}.$$

Temos os polinômios

$$f(x) = x^3 - 100x$$
$$f'(x) = 3x^2 - 100.$$

Como $25 = 5^2$, tentaremos inicialmente encontrar soluções para

$$x^3 - 100x^2 \pmod{5}$$

Uma vez que temos um primo suficientemente pequeno, podemos tentar as únicas possibilidades de solução, $0, 1, 2, 3, 4$.

$$\begin{aligned} f(0) = \quad & 0 \equiv 0 \pmod{5} \\ f(1) = \quad & -99 \equiv 1 \pmod{5} \\ f(2) = & -192 \equiv 3 \pmod{5} \\ f(3) = & -273 \equiv 2 \pmod{5} \\ f(4) = & -336 \equiv 4 \pmod{5} \end{aligned}$$

A única solução módulo cinco é $x_1 = 0$. Verificamos as derivadas de f em zero.

$$f'(0) = -100 \equiv 0 \pmod{5}$$

O Lema de Hensel não nos permite usar a solução zero, porque $f'(0) \equiv 0 \pmod{5}$.

Agora, mesmo x_1 sendo singular, temos $f(x_1) \equiv 0 \pmod{5^2}$. Logo, pelo Teorema 6.45,

$$f(x_1 + 5k) \equiv 0 \pmod{5^2},$$

e temos as soluções $0, 5, 10, 15, 20$:

$$\begin{aligned} f(0) &= 0 && \equiv 0 \pmod{25} \\ f(5) &= -375 && \equiv 0 \pmod{25} \\ f(10) &= 0 && \equiv 0 \pmod{25} \\ f(15) &= 1875 && \equiv 0 \pmod{25} \\ f(20) &= 6000 && \equiv 0 \pmod{25} \end{aligned}$$

São cinco soluções módulo 25, como queríamos. ◀

O Teorema 6.47, de Lagrange, é o semelhante em aritmética modular ao Teorema Fundamental da Álgebra.

Teorema 6.47. *Seja $f(x)$ um polinômio de grau n com coeficientes integrais, e p um primo que* não *divide o coeficiente líder de $f(x)$. Então a congruência $f(x) \equiv 0 \pmod{p}$ tem no máximo n soluções incongruentes módulo p.*

Demonstração. Procedemos por indução no grau do polinômio $f(x)$. A base de indução é com graus zero e um.

Quando $f(x)$ tem grau zero, a congruência é $a_0 \equiv 0 \pmod{p}$, e há zero soluções.

Quando $f(x)$ tem grau um, a congruência é $a_1 x + a_0 \equiv 0 \pmod{p}$. Como sempre há inversos módulo primo, a_1 tem inverso, e a congruência tem exatamente uma solução $x \equiv -a_0(a_1)^{-1} \pmod{p}$.

Presumimos que o enunciado vale para polinômios de grau menor que k, com $k \geq 2$. Suponha que uma congruência $f(x) \equiv 0 \pmod{p}$ de grau k tenha mais que k soluções. Seja $a_k x^k$ o primeiro termo de $f(x)$, e $y_1, y_2, \ldots, y_{k+1}$ soluções, *todas incongruentes módulo* p, desta congruência. Seja

$$g(x) = f(x) - a_k(x - y_1)(x - y_2)\cdots(x - y_n).$$

Como os y_i são soluções, $(x - y_1)\cdots(x - y_n)$ será congruente a $f(x)$ módulo p.. Mas $f(x) \equiv 0 \pmod{p}$, e

$$\begin{aligned} g(y_i) &\equiv f(y_i) - a_k(y_i - y_1)(y_i - y_2)\cdots(y_i - y_i)\cdots(y_i - y_k) \\ &\equiv 0 \pmod{p}, \end{aligned}$$

para todo y_i. Mas $g(x)$ tem grau menor que k (o termo líder de $f(x)$ é cancelado por $a_k x^k$ em $g(x)$). Isto significa que temos uma congruência de grau menor que k, com mais que k soluções. Como p não divide o termo líder de $f(x)$, o grau de $f(x)$ é n. Pela hipótese de indução, só nos resta supor que, para todo x inteiro,

$$g(x) \equiv 0 \pmod{p}.$$

Ou seja, $g(x)$ é identicamente zero.

Tomamos então y_{k+1}.

$$\begin{aligned} g(y_{k+1}) &\equiv f(y_{k+1}) - a_0(y_{k+1} - y_1)(y_{k+1} - y_2)\cdots(y_{k+1} - y_i)\cdots(y_{k+1} - y_k) \\ &\equiv -a_0(y_{k+1} - y_1)(y_{k+1} - y_2)\cdots(y_{k+1} - y_i)\cdots(y_{k+1} - y_k) \\ &\equiv 0 \pmod{p} \end{aligned}$$

Mas Isto não é possível, porque $p \nmid a_0$, e p também não divide nenhum dos fatores no lado esquerdo da congruência, porque são diferenças entre números incongruentes módulo p. Chegamos a uma contradição, e a demonstração está pronta. □

Corolário 6.48. *Se* $a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$ *tem mais que* n *soluções, então para todo coeficiente* a_i, $p \mid a_i$.

Exercícios

Ex. 106 — Prove que para todo $a > 0$ e todo $m > 1$, $a \equiv a \pmod{m}$.

Ex. 107 — Prove que para todo x ímpar e todo inteiro positivo n,

$$x^{2^n} \equiv 1 \pmod{2^{n+2}}$$

Ex. 108 — Prove que se p é primo, $n < p < 2n$, então

$$\binom{2n}{n} \equiv 0 \pmod{p}$$

Ex. 109 — Seja p primo. Qual é o menor inteiro positivo congruente a $(p-2)!$ módulo p?

Ex. 110 — Prove que se p é primo, $ab \equiv ac \pmod{p}$, e $p \nmid a$, então $b \equiv c \pmod{p}$.

Ex. 111 — Prove que se $0 \leq |a| < m/2$, $0 \leq |b| < m/2$ e $a \equiv b \pmod{m}$, então $a = b$.

Ex. 112 — Prove que $a^x \equiv b^x \pmod{m}$ e $a^y \equiv b^y \pmod{m}$, então

$$a^{\mathrm{mdc}(x,y)} \equiv b^{\mathrm{mdc}(x,y)} \pmod{m}.$$

Ex. 113 — Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, é verdade que $x^a \equiv x^b \pmod{m}$, para $x > 1$? E é verdade que $a^b \equiv c^d \pmod{m}$?

Ex. 114 — Demonstre o Teorema 6.21.

Ex. 115 — Resolva as equações ou explique porque não é possível fazê-lo.

(a) $4x - y = 9$

(b) $15x + 21y = 18$

(c) $23x + 15y = 5$

(d) $21x + 15y = 3$

(e) $121x - 88y = 572$

Ex. 116 — Determine para quais valores de K as equações a seguir tem solução.

(a) $15Kx - 8y = 14$

(b) $2Kx + 110y = 63$

Ex. 117 — Calcule os inversos

(a) $5^{-1} \pmod{31}$

(b) $8^{-1} \pmod{21}$

(c) $13^{-1} \pmod{42}$

Ex. 118 — Mostre uma solução inteira positiva para $30x + 18y = 132$, ou prove que não existe.

Ex. 119 — No Exemplo 6.26, se trocarmos a restrição "$x, y \geq 9$" por "$x > y$", quais valores de k podemos usar?

Ex. 120 — Há soluções para a equação diofantina $4x + 8y = 36$, se exigirmos que tanto x como y não possam ser escritos como soma de quadrados? Caso haja, quais são? Caso não haja, qual o motivo? E se exigirmos isso somente de x?

Ex. 121 — Mostre que a equação diofantina $4x + 8y = 36$ (a mesma do Exercício 120) tem infinitas soluções em que x é soma de quadrados.

Ex. 122 — Seja p um primo ímpar. Determine quais inteiros n existem tais que $p \mid n2^n + 1$.

Ex. 123 — Sejam a, b co-primos, e considere a sequência a, $a + b$, $a + 2b, \ldots, a + kb, \ldots$ Prove que há uma quantidade infinita de números nesta sequencia que tem os mesmos divisores primos (ou seja, cuja fatoração difere somente nos expoentes).

Ex. 124 — Extenda a noção de congruência para o anel $\mathbb{Z}[i]$ dos inteiros Gaussianos, e prove que para todo $\alpha = a + bi$, se $\alpha \equiv \beta \pmod{1+i}$, então β é -1, 0 ou $+1$.

Ex. 125 — Da forma como apresentamos, o Teorema Chinês dos restos nos dá solução para sistemas onde cada equação é da forma $x \equiv a_i \pmod{m_i}$. Mostre como resolver sistemas da forma $b_i x \equiv a_i \pmod{m_i}$.

Ex. 126 — Resolva os sistemas de congruências.

(i)

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod{28} \\ x &\equiv 10 \pmod{13} \end{aligned}$$

(ii)

$$\begin{aligned} x &\equiv 1 \pmod{36} \\ x &\equiv 10 \pmod{12} \\ x &\equiv 15 \pmod{470} \end{aligned}$$

(iii)

$$\begin{aligned} x &\equiv 4 \pmod{10} \\ 4x &\equiv 5 \pmod{21} \\ 10x &\equiv 2 \pmod{11} \end{aligned}$$

(iv)

$$\begin{aligned} x &\equiv 3 \pmod{20} \\ 3x &\equiv 2 \pmod{35} \\ 2x &\equiv 1 \pmod{12} \end{aligned}$$

Ex. 127 — Em dúzias, sobra um; em dezenas, sobram três; em setes, sobram seis. Qual é o número?

Ex. 128 — Há um método geral para resolver sistemas de congruências sem usar os dois enunciados do Teorema Chinês dos Restos: encontre uma solução geral para a primeira congruência, substitua na segunda, e assim por diante. Formalize este método e use-o para resolver um dos sistemas do Exercício 126.

Ex. 129 — Demonstre o Lema 129.

Ex. 130 — Desenvolva um algoritmo que, dada uma lista de números naturais $m_1, m_2, \ldots, m_k$ e um número inteiro a_1 , gere aleatoriamente (não necessariamente de maneira equiprovável) um sistema de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

de forma que o sistema tenha solução.

Ex. 131 — Desenvolva o método para resolução de congruências lineares em várias variáveis, mencionado na seção 6.6.

Ex. 132 — Demonstre o Teorema 6.38.

Ex. 133 — Demonstre o Corolário 6.43.

Ex. 134 — Demonstre o Teorema 6.45.

Ex. 135 — Resolva

(a) $x^4 - x^3 - x^2 + x \equiv 0 \pmod{25}$

(b) $x^2 - 6x^2 + 8x \equiv 0 \pmod{81}$

(c) $x^3 - 8x + 20x - 16 \equiv 0 \pmod{49}$

Ex. 136 — Seja $M(x) : \mathbb{Z}_p \to \mathbb{Z}_p$ uma função que mapeia classes de resíduos. Mostre que para todo primo p existe um polinômio $f(x)$, de grau estritamente menor que p e com coeficientes integrais, tal que $f(x) \equiv M(x) \pmod{p}$ para todo $x \in \mathbb{Z}$.

Capítulo 7

Funções Aritméticas

Propriedades importantes dos números inteiros podem ser estudadas através de funções, que tem domínio igual aos inteiros positivos.

Definição 7.1 (função aritmética)**.** Uma **função aritmética** é uma função que tem os inteiros positivos como domínio, e complexos como contradomínio. ♦

Não usaremos funções aritméticas com contradomínio complexo neste texto – será suficiente restringir a atenção a funções com contradomínio real.

Exemplo 7.2. De maneira geral, qualquer sequência é uma função aritmética.

Funções simples tendo inteiros positivos como domínio, como $f(n) = 2n$ são funções aritméticas. Também

$$f(n) = \begin{cases} 1 & \text{se o } n\text{-ésimo dígito de } \pi \text{ é par} \\ -1 & \text{se o } n\text{-ésimo dígito de } \pi \text{ é ímpar} \end{cases}$$

é função aritmética. ◄

7.1 Funções Multiplicativas

As três funções a seguir foram definidas e estudadas por Euler.

Definição 7.3 (funções d, σ, ϕ)**.** Para todo n positivo,
A função $d(n)$ dá o número de divisores positivos de n;
A função $\sigma(n)$ dá a soma dos divisores positivos de n;
A função $\phi(n)$ dá o número de inteiros positivos k menores ou iguais a n, tais que $\text{mdc}\,(k, n) = 1$. ♦

Exemplo 7.4. Os divisores de 12 são

$$1, 2, 3, 4, 6, 12,$$

portanto

$$\begin{aligned} d(12) &= 6, \\ \sigma(12) &= 28. \end{aligned}$$

Os números k menores que 12 tais que $\operatorname{mdc}(k, 12) = 1$ são

$$1, 5, 7, 11,$$

portanto $\phi(12) = 4$. ◀

O Teorema a seguir relaciona $d(n)$ com a fatoração de n.

Teorema 7.5. *Seja n um número natural com fatoração $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.*

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

Exemplo 7.6. Temos $72 = 2^3 \cdot 3^2$, e os divisores de 72 são

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72,$$

portanto $d(72) = 12$. Pelo Teorema 7.5, obtemos o mesmo valor:

$$\begin{aligned} d(72) &= (3 + 1)(2 + 1) \\ &= 4 \cdot 3 \\ &= 12. \end{aligned}$$ ◀

Demonstração. Começamos observando que[1]

$$d(1) = \prod_{\emptyset} = 1$$

Agora demonstramos o Teorema por indução na quantidade de fatores primos distintos de n (cada um elevado a uma potência).

Provamos a base, com um único fator (ou seja, n é uma potência de primo p^j):

$$d(p^j) = j + 1,$$

porque $p^0, p^1, \ldots, p^j$ dividem p^j.

[1] Assim como o somatório de nenhum elemento é o neutro aditivo, $(\sum) = \sum_{\emptyset} = 0$, o produtório de nenhum elemento é o neutro multiplicativo, $(\prod) = \prod_{\emptyset} = 1$.

A hipótese de indução é que se n tem r fatores primos distintos, então

$$d(n) = \prod_{i=1}^{r}(\alpha_i + 1).$$

Agora seja $N = np^\beta$, sendo p ausente da fatoração de n ($p \nmid n$). Então, como

$$d(n) = \prod_{i=1}^{r}(\alpha_i + 1),$$

os divisores de N são compostos pelos $\beta+1$ divisores de β e os $d(n)$ divisores de N:

$$\begin{aligned} c \mid N \quad &\Leftrightarrow \quad c = ab, \\ a \mid n, \quad & \quad b \mid p^\beta, \end{aligned}$$

e como $b \mid p^\beta$, b é da forma p^k, havendo $\beta + 1$ possibilidades para k (de 0 a β). A quantidade de divisores será, portanto, multiplicada por $\beta + 1$, e

$$\begin{aligned} d(N) &= (\beta + 1)\prod_{i=1}^{r}(\alpha_i + 1) \\ &= (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)(\beta + 1). \end{aligned}$$ □

Lema 7.7. *Se p é primo, então*

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

Demonstração. Os divisores de p^k são $p^0, p^1, \ldots, p^k$. Como demonstrado no Exemplo 2.4,

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1},$$

o que imediatamente nos dá o resultado, tomando $n = k + 1$. □

Teorema 7.8. *Seja n um número natural com fatoração $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Então*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}.$$

Exemplo 7.9. Seja $n = 2 \cdot 3^2 = 18$. Os divisores de 18 são

$$1, 2, 3, 6, 9, 18,$$

cuja soma é 39. Usando a fórmula dada no Teorema 7.8,

$$\begin{aligned}\sigma(18) &= \sigma(2 \cdot 3^2) \\ &= \left(\frac{2^{1+1}-1}{1}\right)\left(\frac{3^{2+1}-1}{2}\right) \\ &= \left(\frac{3}{1}\right)\left(\frac{26}{2}\right) \\ &= 39.\end{aligned}$$

◀

Demonstração. A demonstração é por indução em quantidade de fatores primos distintos, da mesma maneira que a do Teorema 7.5, para $d(n)$. Usa-se aqui o Lema 7.7. Os detalhes são pedidos no Exercício 141. □

O Teorema 7.10 identifica uma forma fechada para ϕ; sua demonstração é o Exercício 146.

Teorema 7.10. *Se a fatoração de* n *é* $p_1 p_2 \cdots p^k$*, então*

$$\phi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$$

Exemplo 7.11. Calculamos $\phi(150)$. Sabemos que $150 = 2 \cdot 3 \cdot 5^2$, portanto

$$\begin{aligned}\phi(150) &= \phi(2 \cdot 3 \cdot 5^2) \\ &= \phi(2)\phi(3)\phi(5^2) \\ &= 1 \cdot 2 \cdot 20 \\ &= 40.\end{aligned}$$

Usando o Teorema 7.10, obtemos

$$\begin{aligned}\phi(150) &= 150\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 150\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \\ &= 150 \cdot \frac{4}{15} \\ &= 40.\end{aligned}$$

◀

Teorema 7.12. *Para todo* n *positivo em* $\mathbb{Z}$*,*

$$\sum_{d|n} \phi(d) = n.$$

Exemplo 7.13. Os divisores de 12 são

$$1, 2, 3, 4, 6, 12,$$

e então

$$\begin{aligned}\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) &= 1+1+2+2+2+4\\ &= 12.\end{aligned}$$ ◀

Demonstração. (Combinatória) Considere as n frações

$$\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}.$$

Simplifique-as, deixando todas na forma reduzida.

Em todas as frações simplificadas, o demoninador será um divisor de n (se a fração era a/n e foi simplificada para b/m, evidentemente $m \mid n$). Por exemplo, quando simplificamos

$$\frac{15}{40} \longrightarrow \frac{3}{8},$$

o denominador (8) é divisor de 40.

As frações onde n ainda é o denominador são aquelas nas quais o numerador era co-primo com n. Há $\phi(n)$ destas frações.

Para cada divisor d de n haverá exatamente $\phi(d)$ frações onde o denominador é igual a d. Se somarmos todos estes $\phi(d)$ teremos o número total de frações, n. □

A demonstração acima poderá ficar mais clara com uma ilustração. Escolhemos $n = 18$ e listamos as frações. A primeira linha tem as frações antes da simplificação; a segunda as tem já simplificadas.

$$\begin{array}{cccccccccccccccccc}
\frac{1}{18} & \frac{2}{18} & \frac{3}{18} & \frac{4}{18} & \frac{5}{18} & \frac{6}{18} & \frac{7}{18} & \frac{8}{18} & \frac{9}{18} & \frac{10}{18} & \frac{11}{18} & \frac{12}{18} & \frac{13}{18} & \frac{14}{18} & \frac{15}{18} & \frac{16}{18} & \frac{17}{18} & \frac{18}{18}\\
\downarrow & & & \downarrow & & & & \downarrow & & & \downarrow & & & & \downarrow & & & \downarrow\\
\frac{1}{18} & \frac{1}{9} & \frac{1}{6} & \frac{2}{9} & \frac{5}{18} & \frac{1}{3} & \frac{7}{18} & \frac{4}{9} & \frac{1}{2} & \frac{5}{9} & \frac{11}{18} & \frac{2}{3} & \frac{13}{18} & \frac{7}{9} & \frac{5}{6} & \frac{8}{9} & \frac{17}{18} & \frac{1}{1}
\end{array}$$

Os divisores de 18 são $1, 2, 3, 6, 9$, e o número de frações com cada um deles

no denominador é

$$\begin{aligned}\phi(1) &= 1\\ \phi(2) &= 1\\ \phi(3) &= 2\\ \phi(6) &= 2\\ \phi(9) &= 6\\ \phi(18) &= 6\end{aligned}$$

A soma deles é 18.

Definição 7.14 (função multiplicativa)**.** Seja f uma função aritmética. Se, para todos inteiros a, b com $\operatorname{mdc}(a,b) = 1$, $f(ab) = f(a)f(b)$, dizemos que a função f é **multiplicativa**. ♦

Exemplo 7.15. A função $f(n) = n^2$ é multiplicativa, porque

$$f(nm) = (nm)^2 = n^2m^2 = f(n)f(m). \qquad \blacktriangleleft$$

Teorema 7.16. *Se f é uma função multiplicativa, então $f(1) = 1$.*

Demonstração. Seja n tal que $f(n) \neq 0$. Então $f(n) = f(n \cdot 1) = f(n)f(1)$, o que implica que $f(1) = 1$. □

Teorema 7.17. *As funções ϕ, σ, d são multiplicativas.*

Exemplo 7.18. $\operatorname{mdc}(6,5) = 1$, e os valores de ϕ, σ e d para os dois números são

$$\begin{aligned}\phi(6) &= 2, \qquad & \phi(5) &= 4,\\ d(6) &= 4, \qquad & d(5) &= 2,\\ \sigma(6) &= 12, \qquad & \sigma(5) &= 6.\end{aligned}$$

Como as funções são multiplicativas, temos

$$\begin{aligned}\phi(30) &= \phi(6 \cdot 5)\\ &= \phi(6)\phi(5)\\ &= 2 \cdot 4\\ &= 8.\end{aligned}$$

E de fato, há 8 números cujo MDC com 30 é um:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Verificamos os divisores.

$$\begin{aligned} d(30) &= d(6 \cdot 5) \\ &= d(6)d(5) \\ &= 4 \cdot 2 \\ &= 8. \end{aligned}$$

E são oito os divisores de 30:

$$1, 2, 3, 5, 6, 10, 15, 30.$$

Quanto à função σ,

$$\begin{aligned} \sigma(30) &= \sigma(6 \cdot 5) \\ &= \sigma(6)\sigma(5) \\ &= 12 \cdot 6 \\ &= 72, \end{aligned}$$

que é a soma dos divisores de 30. ◀

Demonstração. Sejam $a, b \in \mathbb{Z}$, com $\operatorname{mdc}(a, b) = 1$. Suponha que as fatorações de a e b sejam

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \\ b &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}, \end{aligned}$$

onde não há $p_i = q_j$. Qualquer divisor de ab será representado de maneira única como produto de divisores de ab:

$$d \mid ab \quad \Rightarrow \quad d = \prod_{\substack{i \le r \\ j \le s}} p^{\gamma_i} q^{\delta_j}.$$

Claramente, se há A divisores de a e B divisores de b, e a interseção dos dois conjuntos de divisores é vazia (porque a e b não tem primos em comum), então a quantidade $d(ab)$ é igual ao produto das quantidades $d(a)$ e $d(b)$,

$$d(ab) = d(a)d(b).$$

Para σ, temos

$$\begin{aligned} \sigma(ab) = \sum_{d \mid ab} d &= \left(\sum_{s \mid a} s \right) \left(\sum_{t \mid b} t \right) \\ &= \sigma(a)\sigma(b). \end{aligned}$$

Para ϕ, observe os anéis $\mathbb{Z}_a$, $\mathbb{Z}_b$ e $\mathbb{Z}_{ab}$. Pelo Teorema Chinês dos Restos, a função $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$,

$$f(x) = (x, x),$$

é bijetora.

(x, x) é unidade se e somente se x é unidade em $\mathbb{Z}_a$ e em $\mathbb{Z}_b$, o que significa que $x \pmod{ab}$ é unidade se e somente se $x \pmod{a}$ e $x \pmod{b}$ são unidades.

Mas a quantidade de unidades em $\mathbb{Z}_n$ é igual a $\phi(n)$, logo, a quantidade de unidades em $\mathbb{Z}_{ab}$ é igual ao produto das quantidades de unidades em $\mathbb{Z}_a$ e $\mathbb{Z}_b$.

$$\phi(ab) = \phi(a)\phi(b). \qquad \square$$

Usando a multiplicidade de ϕ, podemos construir uma demonstração diferente para o Teorema 7.12.

Demonstração. (do Teorema 7.12, usando multiplicidade de ϕ) Temos duas funções multiplicativas,

$$f(n) = \sum_{d|n} \phi(n)$$
$$g(n) = n$$

A multiplicidade de f é simples de verificar, usando a multiplicidade de ϕ.

Dessa forma, se mostrarmos que $f(p^a) = p^a$, pela multiplicidade de f e g, teremos o resultado desejado.

Usaremos um fato simples (a demonstração é pedida no Exercício 137):

$$\phi(p^a) = p^a - p^{a-1}.$$

Agora temos

$$\begin{aligned} f(p^a) = \sum_{d|p^a} \phi(p^a) = \sum_{i=0}^{a} \phi(p^i) & \\ &= 1 + \sum_{i=1}^{a} \phi(p^i) \\ &= 1 + \sum_{i=1}^{a} p^i - p^{i-1} \\ &= p^a, \end{aligned}$$

como queríamos demonstrar. $\square$

7.1.1 Função μ de Moebius

A função μ de Moebius é definida de forma a caracterizar quando um número é livre de quadrados. Sua importância está também em outros fatos. Por exemplo, suponha que para duas funções aritméticas quaisquer, f e g, sempre seja verdade que

$$f(n) = \sum_{d|n} g(d).$$

A fórmula da inversão de Moebius dá uma forma fechada para a expressão de g em função de f.

Definição 7.19 (função μ, de Moebius)**.** Seja $n \in \mathbb{Z}$. A **função μ de Moebius** é a função multiplicativa tal que

$$\begin{aligned} \mu(1) &= +1, \\ \mu(p) &= -1, \\ \mu(p^2) &= 0. \end{aligned}$$ ♦

Tratamos 1 separadamente na definição porque não é primo.

Como exigimos na Definição 7.19 que μ seja multiplicativa, observamos que que pode ser interessante usar a Definição 7.20 para μ. Note que a primeir adefinição implica trivialmente nas propriedades descritas na segunda, por exigir que μ seja multiplicativa – mas a que a segunda definição implica na multiplicatividade não é trivial, e o demonstramos adiante (Teorema 7.22).

Definição 7.20 (função μ, de Moebius - segunda definição)**.** Seja $n \in \mathbb{Z}$. A **função μ de Moebius** é

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } p^2 \mid n \ \ (p \text{ primo}), \\ (-1)^k & \text{se } n = p_1 p_2 \dots p_k \ \ (p_i \neq p_j). \end{cases}$$ ♦

Exemplo 7.21.

$$\begin{aligned} \mu(7) &= (-1)^1 &&= -1 \\ \mu(21) = \mu(3 \cdot 7) &= (-1)^2 &&= +1 \\ \mu(30) = \mu(2 \cdot 3 \cdot 5) &= (-1)^3 &&= -1 \\ \mu(60) &= \mu(2^2 \cdot 3 \cdot 5) &&= \ \ 0 \end{aligned}$$

◄

Teorema 7.22. *A Definição 7.20, embora não o explicite, implica na propriedade da multiplicatividade de μ, sendo portanto equivalente à Defini-*

ção 7.19.

Demonstração. Sejam

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$
$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$$

Presumimos que não há fator comum, já que a definição de função multiplicativa só trata de casos em que $\mathrm{mdc}\,(a, b) = 1$.

Suponha que todos os α_i e β_j são iguais a um (a e b são ambos livres de quadrado). Então

$$\mu(a) = (-1)^s$$
$$\mu(b) = (-1)^t,$$

e como não a e b não tem primos em comum em sua fatoração, ab será também livre de quadrado, e

$$\mu(ab) = (-1)^{s+t} = \mu(a)\mu(b).$$

Agora, sem perda de generalidade, suponha que a não é livre de quadrado: um dos α_i é maior que um. Então $\mu(a) = 0$. Mas se a tem um fator primo elevado a potência maior que um, ab também tem. Assim,

$$\mu(ab) = 0 = \mu(a)\mu(b).$$

Finalmente, se $a = 1$, então

$$\begin{aligned}\mu(ab) &= \mu(1 \cdot b)\\ &= \mu(b)\\ &= 1 \cdot \mu(b)\\ &= \mu(a)\mu(b).\end{aligned}$$

e terminamos de verificar todos os casos. □

Teorema 7.23. *Para todo inteiro positivo* n*,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1,\\ 0 & \text{se } n > 1.\end{cases}$$

Exemplo 7.24. Os divisores de 6 são $1, 2, 3, 6$, portanto

$$\begin{aligned}\mu(1) &= +1\\ \mu(2) &= (-1)^1 = -1\\ \mu(3) &= (-1)^1 = -1\\ \mu(6) &= \mu(2\cdot 3) = (-1)^2 = +1\end{aligned}$$

Temos então

$$\begin{aligned}\sum_{d|6}\mu(d) &= \mu(1)+\mu(2)+\mu(3)+\mu(6)\\ &= (+1)+(-1)+(-1)+(+1)\\ &= 0.\end{aligned}$$

◀

Demonstração. Esta demonstração é realizada em dois casos. Um caso para n decomposto em um único primo (ou seja, n é potência de primo) e outro para n tendo vários primos diferentes na fatoração. Embora a divisão em casos seja parecida com a que faríamos em uma demonstração por indução, a demonstração é direta, porque uma hipótese de indução não é usada na prova do segundo.

Verificamos inicialmente que a fórmula está correta para um único primo p, de forma que $n = p^a$. Como os divisores de p^a são $p^0, p^1, \ldots, p^a$, então

$$\begin{aligned}\sum_{d|p^a}\mu(p^a) &= \mu(1)+\mu(p)+\mu(p^2)+\mu(p^3)+\cdots+\mu(p^a)\\ &= 1-1+0+0+\cdots+0\\ &= 0.\end{aligned}$$

Agora tratamos do segundo caso, em que $n = mp^a$, onde m tem k divisores primos, e que p é primo (simplesmente separamos um dos primos p da

fatoração de n).

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \overbrace{\sum_{d|m} \mu(d)}^{d|mp^0} + \overbrace{\sum_{d|m} \mu(pd)}^{d|mp^1} + \overbrace{\sum_{d|m} \mu(p^2 d)}^{d|mp^2} + \cdots + \overbrace{\sum_{d|m} \mu(p^a d)}^{d|mp^a} \\
&= \sum_{d|m} \mu(d) + \sum_{d|m} \mu(p)\mu(d) + 0 + 0 + \cdots + 0 \\
&= \sum_{d|m} \mu(d) + \sum_{d|m} (-1)\mu(d) + 0 + 0 + \cdots + 0 \\
&= \sum_{d|m} \mu(d) - \sum_{d|m} \mu(d) + 0 + 0 + \cdots + 0 \\
&= 0.
\end{aligned}$$

□

Teorema 7.25 (fórmula da inversão de Moebius)**.** *Sejam* f, g *funções aritméticas, não necessariamente multiplicativas. Então, as duas afirmações a seguir são equivalentes.*

$$\forall n \in \mathbb{Z}, \quad f(n) = \sum_{d|n} g(d) \tag{7.1}$$

$$\forall n \in \mathbb{Z}, \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) \tag{7.2}$$

Dizemos que as funções f *e* g *são um* par de Moebius*.*

Uma maneira alternativa de escrever a Equação 7.2 é

$$\forall n \in \mathbb{Z}, \quad g(n) = \sum_{ab=n} \mu(a) f(b).$$

Exemplo 7.26. Já sabemos, pelo Teorema 7.12, que

$$n = \sum_{d|n} \phi(n).$$

Isto é o mesmo que determinar $f(n) = n$, e escrever

$$f(n) = \sum_{d|n} \phi(n).$$

A fórmula de inversão de Moebius determina, portanto, que

$$\begin{aligned}\phi(n) &= \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d)\left(\frac{n}{d}\right) \\ &= n \sum_{d|n} \frac{\mu(d)}{d}.\end{aligned}$$

Para exemplificar, calculamos $\phi(540)$ de duas maneiras. Primeiro, usamos a definição de $\phi(n)$.

$$\begin{aligned}\phi(540) &= \phi(2^2 \cdot 3^3 \cdot 5) \\ &= \phi(2^2) \cdot \phi(3^3) \cdot \phi(5) \\ &= 2 \cdot 18 \cdot 4 \\ &= 144.\end{aligned}$$

Agora usamos a fórmula que obtivemos usando a inversão de Moebius (apenas como ilustração do conceito, porque neste caso nos será mais trabalhoso do que calcular $\phi(n)$ usando a definição como fizemos):

$$\phi(540) = 540 \sum_{d|540} \frac{\mu(d)}{d}.$$

Observamos que $540 = 2^2 \cdot 3^3 \cdot 5$, mas $\mu(2^2) = \mu(3^2) = \mu(3^3) = 0$, porque todos tem fatores primos repetidos. Não precisamos, assim, considerar os termos em que estes aparecem.

$$\phi(540) = 540\Big(\cdots + \underbrace{\frac{\mu(2^2)}{2^2}}_{\substack{=0/2^2 \\ =0}} + \cdots \Big)$$

Podemos então usar apenas os divisores 1, 2, 3, $2 \cdot 3$, $2 \cdot 5$, $3 \cdot 5$ e $2 \cdot 3 \cdot 5$.

Calculamos:

$$\begin{aligned}
\phi(540) &= 540 \sum_{D|540} \frac{\mu(D)}{D} && \text{(D livre de quadrados)} \\
&= 540 \left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(5)}{5} + \right. \\
&\qquad \left. \frac{\mu(2\cdot 3)}{2\cdot 3} + \frac{\mu(2\cdot 5)}{2\cdot 5} + \frac{\mu(3\cdot 5)}{3\cdot 5} + \frac{\mu(2\cdot 3\cdot 5)}{2\cdot 3\cdot 5} \right) \\
&= 540 \left[+1 - 1\left(\frac{1}{2}\right) - 1\left(\frac{1}{3}\right) - 1\left(\frac{1}{5}\right) \right. \\
&\qquad \left. +1\left(\frac{1}{2\cdot 3}\right) + 1\left(\frac{1}{2\cdot 5}\right) + 1\left(\frac{1}{3\cdot 5}\right) - 1\left(\frac{1}{2\cdot 3\cdot 5}\right) \right] \\
&= 540 - 270 - 180 - 108 + 90 + 54 + 36 - 18 \\
&= 144. \qquad \blacktriangleleft
\end{aligned}$$

Demonstração. Tratamos das duas implicações separadamente. Começamos com (7.1 $\Rightarrow$ 7.2).

Sejam então f e g duas funções aritméticas, e presuma que 7.1 vale.

$$\begin{aligned}
\sum_{ab=n} \mu(a) f(b) &= \sum_{ab=n} \left[\mu(a) \sum_{d|b} g(d) \right] && \text{(por 7.1)} \\
&= \sum_{ad|n} \mu(a) g(d) \\
&= \sum_{d|n} g(d) \sum_{a|\frac{n}{d}} \mu(a)
\end{aligned}$$

Mas pelo Teorema 7.23,

$$\sum_{d|\frac{n}{d}} \mu(d) = \begin{cases} 1 & \text{se } n/d > 1, n > d \\ 0 & \text{se } n/d = 1, n = d. \end{cases}$$

e na última equação,

$$\sum_{a|n} \mu(a) g\left(\frac{n}{d}\right) = \sum_{a|n} g(a) \sum_{d|\frac{n}{d}} \mu(a),$$

temos $\sum_{a|\frac{n}{d}} \mu(d)$ igual a zero quando $n/d > 1$,

e igual a um quanto $n = d$, portanto

$$\begin{aligned}\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{n|n} g(n) \\ &= g(n),\end{aligned}$$

e, partindo de 7.1, $f(n) = \sum_{d|n} g(d)$, determinamos que

$$g(n) = \sum_{ab=n} \mu(a) f(b).$$

Como presumimos (7.1) neste desenvolvimento, ele só estabelece que (7.1) implica em (7.2). Precisamos estabelecer o outro sentido da implicação.

Passamos agora a demonstrar (7.2 $\Rightarrow$ 7.1). Novamente, presuma que f e g são funções aritméticas, e presuma que 7.2 vale.

$$\begin{aligned}\sum_{a|n} g(a) &= \sum_{a|n} \mu(a) \sum_{d|a} f\left(\frac{a}{d}\right) && \text{(por (7.2))} \\ &= \sum_{a|n} \sum_{d|a} \mu(a) f\left(\frac{a}{d}\right) \\ &= \sum_{a|n} \sum_{d|a} f(a) \mu\left(\frac{a}{d}\right) \\ &= \sum_{a|n} f(a) \left(\sum_{d|a} \mu\left(\frac{a}{d}\right) \right)\end{aligned}$$

Novamente, $\sum_{d|a} \mu\left(\frac{a}{d}\right)$ é zero quando $a/d > 1$ e um quando $a = d$:

$$\begin{aligned}\sum_{a|n} f(a) \left(\sum_{d|a} \mu\left(\frac{a}{d}\right) \right) &= f(n)(1) + \sum_{\substack{d|a \\ d<a}} f(n)(0) \\ &= f(n).\end{aligned}$$

Estabelecemos, portanto, que $f(n) = \sum_{a|n} g(a)$ (7.1), usando (7.2). □

Exemplo 7.27. Alguns exemplos de pares de Moebius são

$$(n, \phi(n)) : \; n = \sum_{d|n} \phi(d)$$
$$(d(n), 1) : \; d(n) = \sum_{d|n} 1$$
$$(\sigma(n), id) : \; \sigma(n) = \sum_{d|n} d$$

◀

Teorema 7.28. *Se* f, g *é um par de Moebius, e uma delas é multiplicativa, então a outra também é.*

Demonstração. Suponha que f e g sejam um par de Moebius,

$$\forall n \in \mathbb{Z}, \;\; f(n) = \sum_{d|n} g(d)$$
$$\forall n \in \mathbb{Z}, \;\; g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right)$$

e que $\text{mdc}\,(a, b) = 1$. Então, se g é multiplicativa,

$$\begin{aligned}
f(ab) &= \sum_{d|ab} g(d) \\
&= \sum_{c|a} \sum_{e|b} g(ce) && (\text{mdc}\,(a, b) = 1) \\
&= \sum_{c|a} \sum_{e|b} g(c) g(e) && (g \text{ é multiplicativa}) \\
&= \sum_{c|a} g(c) \sum_{e|b} g(e) \\
&= f(a) f(b).
\end{aligned}$$

Se f é multiplicativa,

$$\begin{aligned} g(ab) &= \sum_{d|ab} \mu(d) f\left(\frac{ab}{d}\right) \\ &= \sum_{c|a} \sum_{e|b} \mu(ce) f\left(\frac{ab}{ce}\right) && (\text{mdc}\,(a,b)=1) \\ &= \sum_{c|a} \sum_{e|b} \mu(c)\mu(e) f\left(\frac{a}{c}\right) f\left(\frac{b}{e}\right) && (f, \mu \text{ multiplicativas}) \\ &= \sum_{c|a} \mu(c) f\left(\frac{a}{c}\right) \sum_{e|b} \mu(e) f\left(\frac{b}{e}\right) \\ &= g(a)g(b). && \square \end{aligned}$$

7.2 Maior Inteiro (chão), $\lfloor x \rfloor$

A noção natural de "número inteiro menor que ou igual a x" é de uso suficiente amplo para que tenham sido definidas para ela nome e notação.

Definição 7.29 (menor inteiro maior ou igual a x (chão de x))**.** Se $x \in \mathbb{R}$, o **maior inteiro menor ou igual a** x, ou **chão de** x, é denotado por $\lfloor x \rfloor$ ou $[x]$. O conceito simétrico é o de **menor inteiro maior ou igual a** x, ou **teto de** x, denotado $\lceil x \rceil$. ♦

Exemplo 7.30.

$$\begin{aligned} \lfloor 1/2 \rfloor &= 0 & \lfloor e \rfloor &= 2 \\ \lfloor 3/2 \rfloor &= 1 & \lfloor \varphi \rfloor &= 1 \\ \lfloor -1/2 \rfloor &= -1 & \left\lfloor \sqrt{2} \right\rfloor &= 1 \\ \lfloor -3/2 \rfloor &= -2 & \left\lfloor -\sqrt{2} \right\rfloor &= -2 \\ \lfloor 3 \rfloor &= 3 & \lfloor \pi \rfloor &= 3 \quad \blacktriangleleft \end{aligned}$$

Exemplo 7.31. O número de dígitos necessário para representar um número n em base dez é

$$\lfloor \log_{10}(n) \rfloor + 1.$$

De maneira geral, o número de dígitos necessário para representar um número n em base b é

$$\lfloor \log_b(n) \rfloor + 1. \quad \blacktriangleleft$$

Por ser simétrico a $\lfloor x \rfloor$, não trataremos de $\lceil x \rceil$. O Teorema 7.32 lista algumas propriedades de $\lfloor x \rfloor$, que são de simples verificação.

Teorema 7.32. *Para todos* $x, y \in \mathbb{R}$, $n \in \mathbb{Z}$,

(a) $x = \lfloor x \rfloor + f$, *onde* $f \in [0, 1)$ *é a* parte fracionária *de* x.

(b) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

(c) $\lfloor x \rfloor + \lfloor -x \rfloor$ *é zero se* $x \in \mathbb{Z}$, *senão é* -1.

(d) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.

(e) $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$, *se* $n > 0$.

(f) $0 \leq \lfloor x \rfloor - 2 \lfloor x/2 \rfloor \leq 1$.

(g) $| \mathbb{Z} \cap (x, y] | \; = \; \lfloor y \rfloor - \lfloor x \rfloor$.

(h) $| \{kn : k \in \mathbb{Z}^+, kn \leq x\} | = \lfloor x/n \rfloor$

(i) *O menor inteiro congruente a* $n \mod m$ *é o* $k \in \mathbb{Z}$ *tal que* $n = m \lfloor a/m \rfloor + k$.

No Teorema 7.33, que traz a fórmula de de Polignac-Legendre [2], afirmamos que há uma forma fechada simples para a ordem do expoente de um primo na fatoração de $n!$ – ou seja, podemos facilmente saber qual a maior potência de um primo p que divide $n!$.

Teorema 7.33 (fórmula de de-Polignac e Legendre)**.** *Sejam* p *primo e* n *inteiro positivo. Então*

$$\operatorname{ord}_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Exemplo 7.34. Por exemplo, se $p = 7$ e $n = 20$, temos

$$\begin{aligned} \operatorname{ord}_7(20!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{20}{7^i} \right\rfloor \\ &= \left\lfloor \frac{20}{7} \right\rfloor + \left\lfloor \frac{20}{7^2} \right\rfloor + \cdots \\ &= \lfloor 2.857 \cdots \rfloor + \lfloor 0.408 \cdots \rfloor + \cdots \\ &= 2 + 0 + \cdots \\ &= 2, \end{aligned}$$

porque os termos mais adiante são todos zero. E a ordem de 7 em 20! é, de fato, dois:

$$20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19. \qquad \blacktriangleleft$$

[2] O primeiro nome é "Alfonse de Polignac", daí o duplo "de".

Demonstração. A soma sempre é finita, porque quando $p^i > n$, $\lfloor n/p^i \rfloor = 0$.

Claramente, os únicos primos que dividem $n!$ são menores ou iguais que n. O último deles é $\lfloor n/p \rfloor$.

Se visualizarmos $n!$ como produto de inteiros, cada um com sua fatoração única, teremos

$$n! = 1 \cdot 2 \cdot \cdots (p_1 p_2 \ldots p_k) \cdots (n-1)n,$$

Cada fator em $n!$ contribui com algum p^j. Se dividirmos n por p, estaremos contando o número de vezes que p aparece com expoente ≥ 1 em $n!$. Ao dividirmos por p^2, o número de vezes que aparece com expoente ≥ 2, e assim por diante.

Assim, a soma

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

contabiliza exatamente a soma dos expoentes de p em $n!$. □

O Exemplo 7.35 é uma interessante aplicação do Teorema 7.33.

Exemplo 7.35. Provaremos que o número

$$\frac{100!}{(10!)^{10} 11!}$$

é inteiro.

Precisamos mostrar que, para cada potência de primo p^r na fatoração do denominador, existe um fator p^s no numerador, com $s \geq b$.

No denominador temos

$$\begin{aligned} 10! &= 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} \\ 11! &= 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4} \cdot 11^{b_5} \end{aligned}$$

A ordem de cada um dos expoentes é, usando o Teorema 7.33, para $10!$:

$$\begin{aligned} \operatorname{ord}_2(10!) &= \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{2^2} \right\rfloor + \left\lfloor \frac{10}{2^3} \right\rfloor = 5 + 2 + 1 = 8 \\ \operatorname{ord}_3(10!) &= \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{3^2} \right\rfloor = 3 + 1 = 4 \\ \operatorname{ord}_5(10!) &= \left\lfloor \frac{10}{5} \right\rfloor = 2 \\ \operatorname{ord}_7(10!) &= \left\lfloor \frac{10}{7} \right\rfloor = 1. \end{aligned}$$

Agora, para 11!:

$$\begin{aligned}
\operatorname{ord}_2(11!) &= \left\lfloor \frac{11}{2} \right\rfloor + \left\lfloor \frac{10}{2^2} \right\rfloor + \left\lfloor \frac{10}{2^3} \right\rfloor = 5+2+1 = 8 \\
\operatorname{ord}_3(11!) &= \left\lfloor \frac{11}{3} \right\rfloor + \left\lfloor \frac{10}{3^2} \right\rfloor = 3+1 = 4 \\
\operatorname{ord}_5(11!) &= \left\lfloor \frac{11}{5} \right\rfloor = 2 \\
\operatorname{ord}_7(11!) &= \left\lfloor \frac{11}{7} \right\rfloor = 1 \\
\operatorname{ord}_{11}(11!) &= \left\lfloor \frac{11}{11} \right\rfloor = 1
\end{aligned}$$

Como temos 10! elevado à décima potência, multiplicamos os expoentes de 10! por dez. Assim, temos

$$\begin{aligned}
\operatorname{ord}_2(10!^{10}) &= 80 \\
\operatorname{ord}_3(10!^{10}) &= 40 \\
\operatorname{ord}_5(10!^{10}) &= 20 \\
\operatorname{ord}_7(10!^{10}) &= 10
\end{aligned}$$

Os expoentes no denominador $D = (10!)^{10}11!$ são

$$\begin{aligned}
\operatorname{ord}_2(D) &= 80+8 = 88 \\
\operatorname{ord}_3(D) &= 40+4 = 44 \\
\operatorname{ord}_5(D) &= 20+2 = 22 \\
\operatorname{ord}_7(D) &= 10+1 = 11 \\
\operatorname{ord}_{11}(D) &= 1
\end{aligned}$$

Verificamos se temos o necessário no numerador, $N = 100!$:

$$\begin{aligned}
\operatorname{ord}_2(100!) &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \left\lfloor \frac{100}{2^3} \right\rfloor + \left\lfloor \frac{100}{2^4} \right\rfloor + \left\lfloor \frac{100}{2^5} \right\rfloor + \left\lfloor \frac{100}{2^6} \right\rfloor \\
&= 50 + 25 + 12 + 6 + 3 + 1 \\
&= 97 \\
&> \mathbf{88}. \\
\operatorname{ord}_3(100!) &= \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{3^2} \right\rfloor + \left\lfloor \frac{100}{3^3} \right\rfloor + \left\lfloor \frac{100}{3^4} \right\rfloor \\
&= 33 + 11 + 3 + 1 \\
&= 48 \\
&> \mathbf{44}. \\
\operatorname{ord}_5(100!) &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor \\
&= 20 + 4 \\
&= 24 \\
&> \mathbf{22}. \\
\operatorname{ord}_7(100!) &= \left\lfloor \frac{100}{7} \right\rfloor + \left\lfloor \frac{100}{7^2} \right\rfloor \\
&= 14 + 2 \\
&= 16 \\
&> \mathbf{11}. \\
\operatorname{ord}_{11}(100!) &= \left\lfloor \frac{100}{11} \right\rfloor \\
&= 9 \\
&> \mathbf{1}.
\end{aligned}$$

E o número N/D é inteiro[3]. ◀

7.3 $\pi(n)$

A função $\pi(n)$ dá o número de primos menores ou iguais a n. Por exemplo,

$$\begin{array}{ll}
\pi(2) = 1 & \pi(7) = 4 \\
\pi(3) = 2 & \pi(8) = 4 \\
\pi(4) = 2 & \pi(9) = 4 \\
\pi(5) = 3 & \pi(10) = 4 \\
\pi(6) = 3 & \pi(11) = 5
\end{array}$$

[3] $N/D = 5904968808604507115824213572133292476575768202778243210230806239411719226124080755200$.

O Teorema 7.36 explicita uma relação entre $\pi(n)$ e $\phi(n)$,

Teorema 7.36. *Para quaisquer* k, n *inteiros positivos,*

$$\pi(n) \leq \left\lceil \frac{n}{k} \right\rceil \phi(k) + 2k$$

Demonstração. Se $k \geq n$, então o resultado segue trivialmente:

$$\pi(n) < n < s < 2k.$$

Suponha, portanto, que $n > k$ Sejam s o quociente e r o resto da divisão de n por k,

$$n = ks + r.$$

Visualizamos esta divisão como o agrupamento de s sequências de k números, seguidas de uma sequência de r números.

Na primeira sequência, $1, \ldots, k$, há no máximo k primos.

Agora, cada número m tal que $\text{mdc}\,(m, k) > 1$ tem um fator primo p em comum com k, tal que $p < k$. Pelo menos um múltiplo de p estará dentre $k+1, \ldots, 2k$, portanto cada divisor de k que encontrarmos nos permite contar um múltiplo de primo no intervalo $k+1, \ldots, 2k$. Assim, haverá *no máximo* $\phi(k)$ primos em $k+1, \ldots 2k$. O mesmo vale para as outras sequências, $tk+1, \ldots (t+1)k$. Assim, contabilizamos (i) k primos na primeira sequência; (ii) $r < k$ primos na última sequência; e (iii) $(s-1)\phi(k)$ primos nas demais.

$$\begin{aligned}
\pi(n) &\leq k + r + (s-1)\phi(k) \\
\pi(n) &\leq 2k + (s-1)\phi(k) \\
\pi(n) &\leq 2k + s\phi(k) \\
\pi(n) &\leq 2k + \left\lceil \frac{x}{k} \right\rceil \phi(k)
\end{aligned}$$

□

7.4 Crescimento de $\pi(n)$

Nesta seção identificaremos limitantes superior e inferior para $\pi(n)$. O Teorema dos Números Primos, demonstrado em 1896 por Hadamard e Poussin, enuncia que

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Não demonstraremos este Teorema. Ao invés disso, trabalharemos na demonstração (muito mais fácil) do Teorema de Chebychev. A demonstração usualmente dada usa, além do Teorema de Polignac-Legendre (Teorema 7.33), somente conceitos elementares de Matemática. A demonstra-

ção do Teorema de Chebytchev incluída aqui depende de um Teorema conjecturado por Bertrand em 1845, e demonstrado por Chebychev em 1852.

Para cada inteiro n e primo p, definimos como r_p o expoente tal que $p^{r_p} \leq 2n$ e $p^{r_p+1} > 2n$.

O Lema 7.37 estabelece o fundamento para nossa demonstração do Teorema de Chebychev a respeito do crescimento de $\pi(n)$.

Lema 7.37. *Seja n inteiro positivo. Então*

$$\prod_{n<p<2n} p \;\Bigg|\; \binom{2n}{n} \;\Bigg|\; \prod_{p<2n} p^{r_p},$$

onde os números p no produtório são os primos entre n e $2n$.

Demonstração. Para o lado esquerdo, vemos que como

$$\binom{2n}{n} = \frac{(2n)!}{n!n!},$$

então p está na fatoração de $2n!$, porque é menor que $2n$, mas não está na fatoração de $n!n!$, porque é maior que n.

Já para o lado direito, $\binom{2n}{n} \mid \prod_{p<2n} p^{r_p}$,

$$\begin{aligned}
\operatorname{ord}_p(2n!) &= \sum_{i=1}^{r_p} \left\lfloor \frac{2n}{p^i} \right\rfloor \\
\operatorname{ord}_p(n!n!) &= 2\operatorname{ord}_p(n!) = 2\sum_{j=1}^{r_p} \left\lfloor \frac{n}{p^j} \right\rfloor
\end{aligned}$$

Tendo a ordem de p no numerador e no denominador, podemos calcular a ordem de p em $\binom{2n}{n}$.

$$\begin{aligned}
\operatorname{ord}_p \binom{2n}{n} &= \sum_{i=1}^{r_p} \left(\left\lfloor \frac{2n}{p_i} - 2\left\lfloor \frac{n}{p_i} \right\rfloor \right\rfloor \right) \\
&\leq \sum_{i=1}^{r_p} 1 \\
&= r_p.
\end{aligned}$$

Assim, como $\operatorname{ord}_p \binom{2n}{n} \leq r_p$, temos o resultado que queríamos:

$$\binom{2n}{n} \;\Bigg|\; \prod_{p<2n} p^{r_p}. \qquad \square$$

Com estes resultados já é possível demonstrar o Teorema de Chebychev.

Teorema 7.38 (de Chebychev)**.** *Existem constantes positivas* A *e* B *tais que, para todo* $x > 2$*,*

$$A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x}.$$

Demonstração. A demonstração de divisibilidade no Lema 7.37 tem o único propósito de nos ajudar a demonstrar uma desigualdade, já que para $a, b \in \mathbb{Z}$, $a \mid b \Rightarrow a \leq b$. Pelo Lema,

$$\prod_{n<p<2n} p \;\leq\; \binom{2n}{n} \;\leq\; \prod_{p<2n} p^{r_p}.$$

Agora, compare número $n^{\pi(2n)-\pi(n)}$ com $\prod_{n<p<2n} p$

$$n^{\pi(2n)-\pi(n)} = n \cdot n \cdot n \cdots n$$
$$\prod_{n<p<2n} p = p_1 \cdot p_2 \cdots p_k$$

Há $\pi(2n) - \pi(n)$ fatores em ambos os casos, mas cada um dos p_i é maior que n, logo

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p<2n} p$$

Da mesma forma, comparamos $(2n)^{\pi(2n)}$ com $\prod_{p<2n} p^{r_p}$.

$$(2n)^{\pi(2n)} = (2n) \cdot (2n) \cdots (2n)$$
$$\prod_{p<2n} p^{r_p} = p_1^{r_{1p}} \cdot p_2^{r_{2p}} \cdots p_k^{r_{kp}}$$

Há $\pi(2n)$ fatores nas duas expressões, e cada $p_i^{r_{p_i}}$ é menor que $2n$, portanto

$$\prod_{p<2n} p^{r_p} \leq (2n)^{\pi(2n)}.$$

Disso concluimos que

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p<2n} p \;\leq\; \binom{2n}{n} \;\leq\; \prod_{p<2n} p^{r_p} \leq (2n)^{\pi(2n)}$$

Tomando o logaritmo da desigualdade,

$$[\pi(2n) - \pi(n)]\log(n) \;\leq\; \log\binom{2n}{n} \;\leq\; \pi(2n)\log(2n) \tag{7.3}$$

Observamos que

$$\binom{2n}{n} \geq 2^n$$
$$\log\binom{2n}{n} \geq n\log(2) \qquad \text{(log)}$$

Do lado direito da desigualdade 7.3, obtemos o limitante inferior para $\pi(n)$:

$$\pi(2n)\log(n) \geq \log\binom{2n}{n}$$
$$\pi(2n)\log(n) \geq n\log(2)$$
$$\pi(2n) \geq \log(2)\left(\frac{n}{\log n}\right)$$

A desigualdade que obtivemos é para $2n$, e não para n; no entanto,

$$\begin{aligned}\pi(m) &\geq \pi\left(2\left\lfloor\frac{m}{2}\right\rfloor\right)\\ &\geq C\,\frac{\left\lfloor\frac{m}{2}\right\rfloor}{\log\left(\left\lfloor\frac{m}{2}\right\rfloor\right)} && \text{(para algum } C>0\text{)}\\ &\geq B\frac{m}{\log m}, && \text{(para algum } B>0\text{)}\end{aligned}$$

e demonstramos que $\pi(n) \geq B\, n/\log(n)$.

Passamos ao limitamte superior. Destacamos inicialmente que

$$\binom{2n}{n} \leq 2^{2n}$$
$$\log\binom{2n}{n} \leq 2n\log(2). \qquad \text{(log)}$$

Escrevemos novamente o lado esquerdo da desigualdade 7.3.

$$\left[\pi(2n)-\pi(n)\right]\log(n) \leq \log\binom{2n}{n}$$
$$\left[\pi(2n)-\pi(n)\right]\log(n) \leq 2n\log(2)$$
$$\pi(2n)-\pi(n) \leq 2\log(2)\frac{n}{\log(n)}$$

É simples verificar, por indução, e usando os resultado já obtido até agora, que

$$\pi(2^k) \leq 3\frac{2^k}{k}. \qquad (7.4)$$

Como $n/\log(n)$ é monotonicamente crescente para $n \geq e$, suponha que

$2^k < n \leq 2^{k+1}$ para algum k. Então

$$\begin{aligned}
\pi(n) &\leq \pi(2^{k+1}) && (n \leq 2^{2^k+1}) \\
&\leq 6\frac{2^k}{k+1} && \text{(por (7.4))} \\
&= 6\frac{\log(2)2^k}{\log(2)(k+1)} \\
&= 6\log(2)\frac{2^k}{\log(2)k+\log(2)} \\
&= B\frac{2^k}{\log(2)k}\log(2)k+\log(2) && (B = 6\log 2) \\
&< B\frac{2^k}{\log(2)k} \\
&= B\frac{2^k}{\log(2^k)} \\
&\leq B\frac{n}{\log n}. && (2^k < n)
\end{aligned}$$

Mostramos, portanto, que $\pi(n) < B\frac{n}{\log(n)}$, e a demonstração termina aqui. □

Exercícios

Ex. 137 — Mostre que se p é primo, $\phi(p^n) = p^n - p^{n-1}$.

Ex. 138 — Mostre que se $n > 2$ então $\phi(n)$ é par.

Ex. 139 — Mostre que para todos $n, k \in \mathbb{N}$,

$$\phi(n^k) = n^{k-1}\phi(n).$$

Ex. 140 — Resolva:

a) $\phi(n) = 12$

b) $\phi(n) = n/2$

c) $\phi(\phi(n)) = 2^{20}3^8$

Ex. 141 — Mostre os detalhes da demonstração do Teorema 7.8.

Ex. 142 — Prove que $\phi(2k)$ é $2\phi(k)$ se k é par, ou $\phi(k)$ se k é ímpar.

Ex. 143 — Prove que para todo n inteiro positivo,

$$\sum_{i=1}^{n} M\left(\left\lfloor \frac{n}{i} \right\rfloor\right) = 1.$$

Ex. 144 — Prove que para todo n inteiro positivo,

$$n = \phi(n) \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}.$$

Ex. 145 — Sejam $f : \mathbb{N} \to \mathbb{R}$ e $g : \mathbb{N} \to \mathbb{R}$, com

$$g(n) = \sum_{d|n} f(d).$$

Prove que

$$f(n) = \sum_{\substack{d|n \\ n \text{ livre de quadrados}}} (-1)^{p(n/d)} g(d),$$

onde $p(n/s)$ é a quantidade de primos distintos na fatoração de n/d

Ex. 146 — Demonstre o Teorema 7.10.

Ex. 147 — Prove que se $f(n)$ é uma função aritmética multiplicativa, então

$$f(\text{mdc}\,(a,b)) \cdot f(\text{mmc}(a,b)) = f(a)f(b).$$

Ex. 148 — Seja n um inteiro positivo. O *radical* de um n é o produto dos primos *distintos* na fatoração (ou seja, é a fatoração de n, mas modificada para que todo primo tenha expoente um). Denotamos o radical de n por $\text{rad}(n)$. Por exemplo, $600 = (2^3)(3)(5^2)$, então $\text{rad}(600) = (2)(3)(5) = 30$. Prove que

$$\frac{\phi(n)}{n} = \frac{\phi(\text{rad}(n))}{\text{rad}(n)}.$$

Ex. 149 — Prove que para todo inteiro positivo n,

$$\sigma(n) = \prod_{d|n} \left(\frac{p^{a+1} - 1}{p - 1}\right).$$

Ex. 150 — Prove que

$$\mu(n) = \sum_{\substack{1 \le k \le n \\ \mathrm{mdc}(k,n)=1}} e^{2\pi i k/n}$$

Ex. 151 — Calcule

$$\int_0^\infty \lfloor x \rfloor \, e^{-x} dx$$
$$\int_0^{k\pi} \lfloor x \rfloor \, \mathrm{sen}(x) dx$$

Ex. 152 — Prove que p é primo se e somente se

$$\sum_{j-1}^{\infty} \left(\left\lfloor \frac{n}{j} \right\rfloor - \left\lfloor \frac{n-1}{j} \right\rfloor \right) = 2.$$

Ex. 153 — Modifique o argumento da demonstraçõa de Erdös para a infinitude dos primos (Teorema 5.19 – enunciado na página 71, prova na página 72), para obter uma cota inferior para $\pi(n)$.

Ex. 154 — Prove que para $x \in \mathbb{R}$ não inteiro,

$$\lfloor x \rfloor = x - \frac{1}{2} + \frac{1}{\pi} \sum_{j=1}^{\infty} \frac{\mathrm{sen}(2\pi x j)}{j}$$

Ex. 155 — Seja $f : [1,45] \to \mathbb{Z}$ (o domínio de f é o intervalo $[1,45]$),

$$f(x) = \left\lfloor \frac{x}{7} \right\rfloor \left\lfloor \frac{37}{x} \right\rfloor.$$

Qual é a cardinalidade da imagem de $f(x)$?

Ex. 156 — Encontre n tal que $\phi(\sigma(2^n)) = 2^n$.

Ex. 157 — Encontre expressões fechadas para

a) $\sum_{d|n} \mu(d)\sigma(d)$

b) $\sum_{d|n} \frac{\mu(d)}{d}$

c) $\sum_{d|n} \mu(d)\phi(d)$

d) $\sum_{d|n} \mu^2(d)\phi^2(d)$

e) $\sum_{d|n} \frac{\mu(d)}{\phi(d)}$

Ex. 158 — Resolva:

a) $\phi(3^a 5^b) = 360$

b) $\phi(n) = 16$

Ex. 159 — Prove que

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = \sum_{d|n} \frac{\mu(d)}{d}.$$

Ex. 160 — Prove que a definição dada a seguir é equivalente à Definição 7.19.

Definição 7.39. A **função** μ **de Moebius** é a <u>única</u> função aritmética tal que

$$\begin{aligned} \mu(1) &= 1 \\ \sum_{d|n} \mu(d) &= 0, \quad \forall n \in \mathbb{N},\ n > 1. \end{aligned}$$ ♦

Ex. 161 — Determine a quantidade de funções $f : \mathbb{Z}_n \to n$ multiplicativas e crescentes, com $f(2) = 4$. Determine também para quantos valores estas funções são iguais (para quantos n vale $f_i(k) = f_j(k)$).

Ex. 162 — Prove que a soma dos números k menores que n, tais que $\text{mdc}\,(k, n) = 1$, é

$$\frac{n\phi(n)}{2}.$$

Ex. 163 — Prove que se $n = n_1 + n_2 + \cdots + n_k$ então

$$\frac{n!}{n1! \cdot n2! \cdots n_k!} \quad \in \mathbb{Z}.$$

Ex. 164 — Prove que a seguinte fórmula de inversão (similar à inversão de Moebius) vale.

Sejam duas funções f e g. Então,

$$g(x) = \sum_{j=1}^{\lfloor x \rfloor} f\left(\frac{x}{j}\right)$$

se e somente se

$$f(x) = \sum_{j=1}^{\lfloor x \rfloor} \mu(j) g\left(\frac{x}{j}\right).$$

Ex. 165 — Com quantos zeros termina $100!/40!$?

Ex. 166 — Qual é a maior potência de 40 que divide $40!$?

Ex. 167 — Na demonstração do Teorema de Chebychev (Teorema 7.38), mencionamos que é possível provar, por indução, que

$$\pi(2^k) \leq 3\frac{2^k}{k}.$$

Mostre os detalhes.

Ex. 168 — Prove que

$$\pi(n) = \sum_{j=2}^{n} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor$$

Ex. 169 — Prove que (* Legendre) se a fatoração de n é $p_1 p_2 \dots p_n$, então

$$\pi(n) = \pi\left(\sqrt{n}\right) - 1 + \lfloor n \rfloor - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \cdots$$

Ex. 170 — Definmos a *função de Merten* e *matriz de Redheffer*
Definição 7.40 (função de Merten)**.** A **função de Merten**, $M(n)$ dá a soma de $\mu(k)$ para todo $k \leq n$:

$$M(n) = \sum_{1 \leq k \leq n} \mu(k). \qquad \blacklozenge$$

Por exemplo,

$$\begin{aligned} M(4) &= \mu(1) + \mu(2) + \mu(3) + \mu(4) \\ &= 1 + (-1) + (-1) + 0 = -1. \end{aligned}$$

Merten conjecturou que $|M(x)|$ seria sempre estritamente menor do que x, mas a conjectura foi provada falsa por Odlyzko e Riele em 1985.
Definição 7.41 (matriz de Redheffer)**.** A **matriz de Redheffer de ordem** n, denotada $R_{n\times n}$ é uma matriz quadrada de ordem n, com elementos $r_{ij} = 1$ se $j = 1$ ou $i \mid j$; caso contrário, $r_{ij} = 0$. $\blacklozenge$

Por exemplo,

$$R_{6\times 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Prove que para todo inteiro positivo n,

$$M(n) = \det R_{n\times n}.$$

Ex. 171 — A função de Merten é multiplicativa?

Ex. 172 — A funções aritméticas multiplicativas formam um grupo, se usarmos como operação a convolução de Dirichlet?

Capítulo 8

Sistemas de Resíduos

Sistemas de resíduos são conjuntos finitos de inteiros com certas características em comum, relacionadas a divisibilidade.

8.1 Sistemas completos e reduzidos de resíduos

Se $a \equiv b \pmod{m}$, dizemos que a e b representam o mesmo **resíduo** módulo m. Por exemplo, como $25 \equiv 4 \pmod{7}$, então 4 e 25 são o mesmo resíduo módulo 7. A palavra *resíduo* significa "resto de divisão" – veja que 4 é o resto de $25 \div 7$, e também é o resto de $4 \div 7$.

Definição 8.1 (sistema completo de resíduos)**.** Um conjunto X de inteiros é um **sistema completo de resíduos** módulo m se para cada $n \in \mathbb{Z}$, existe exeatmente um elemento em X que é congruente a n módulo m. ⧫

Ou seja, um sistema completo de resíduos módulo m identifica os possíveis restos da divisão de inteiros por m, devendo haver exatamente um elemento no sistema para cada possível resto.

O conjunto $\{0, 1, 2, \ldots, n-1\}$ é um sistema completo de resíduos módulo n, assim como $\{3, 4, 5, \ldots, n+2\}$. Mais concretamente, o conjunto $\{0, 5, 10, 15\}$ é um sistema completo de resíduos módulo quatro:

$$\begin{aligned} 0 &\equiv 0 \pmod{4} \\ 5 &\equiv 1 \pmod{4} \\ 10 &\equiv 2 \pmod{4} \\ 15 &\equiv 3 \pmod{4}. \end{aligned}$$

Todo inteiro é congruente a $0, 1, 2$ ou 3 módulo quatro – e há exatamente um representante de cada uma destas classes de congruência no conjunto $\{0, 5, 10, 15\}$.

Definição 8.2 (sistema reduzido de resíduos)**.** Um **sistema reduzido de resíduos** módulo m é um conjunto de inteiros co-primos com m, não congruentes entre si. Todo k inteiro co-primo com m deve ser congruente módulo m a algum elemento do conjunto. ♦

O conjunto $\{1, 3\}$ é um sistema reduzido de resíduos módulo quatro:

$$\begin{aligned} 1 &\equiv 1 \pmod 4 \\ 3 &\equiv 3 \pmod 4. \end{aligned}$$

Um inteiro pode ser congruente a $0, 1, 2$ ou 3 módulo quatro. No entanto, 0 e 2 não são co-primos com 4, e portanto um inteiro co-primo com m será necessariamente congruente a 1 ou 3 módulo 4.

Os elementos em um sistema reduzido de resíduos são aqueles que tem inverso (porque todos são co-primos com o módulo) – ou seja, são as *unidades* módulo m. Quando o módulo é um primo p, todos os números de 0 a $p - 1$ compõem o sistema reduzido de resíduos, e todos são unidades.

O Lema 8.3 garante que se um elemento a é parte de um sistema reduzido de resíduos, toda a sua classe de equivalência também é, porque toda ela será co-prima com o módulo.

Lema 8.3. *Se* $a \equiv b \pmod m$ *e* $\operatorname{mdc}(a, m) = 1$*, então* $\operatorname{mdc}(b, m) = 1$.

Demonstração. Se $a \equiv b \pmod m$ então

$$\begin{aligned} m \mid (a - b) & \\ km &= a - b \\ a &= km + b \\ \operatorname{mdc}(a, m) &= \operatorname{mdc}(km + b, m) \\ 1 &= \operatorname{mdc}(km + b, m) \\ 1 &= \operatorname{mdc}(b, m). \end{aligned}$$

□

Para o módulo 14, o sistema reduzido de resíduos é $\{1, 3, 5, 9, 11, 13\}$. O Lema 8.3 determina que quaisquer inteiros congruentes a estes são também co-primos com 14. Podemos veriricar, como breve ilustração, que

$$\begin{aligned} 23 &\equiv 9 \pmod{14}, \\ 25 &\equiv 11 \pmod{14}, \end{aligned}$$

e tanto 23 como 23 são co-primos com 14.

Teorema 8.4. *Todo sistema reduzido de resíduos módulo* m *tem exatamente* $\phi(m)$ *elementos.*

Demonstração. Demonstramos em partes: (i) mostramos que os inteiros entre 1 e $m - 1$ que são co-primos com m são todos incongruentes entre si,

e portanto são um sistema reduzido de resíduos módulo m de tamaho $\phi(m)$; (ii) mostramos que um sistema reduzido de resíduos não pode ser maior que este; e (iii) mostramos que o conjunto também não pode ser menor.

(i) Suponha que $0 < a, b < m$ são co-primos com m. Como tanto a como b estão entre 1 e $m-1$, a divisão $a \div m$ deixa resto a, e a divisão $b \div m$ deixa resto b, e portanto $a \not\equiv b \pmod{m}$.

(ii) Suponha que haja um sistema reduzido de resíduos módulo m com $r > \phi(m)$ elementos $s_1, s_2, \ldots, s_r$. Cada um destes elementos é congruente módulo m a algum inteiro entre 0 e $m-1$. Sabemos que só há $\phi(m)$ inteiros a_i nesse intervalo que são co-primos com m, e também sabemos, pelo Lema 8.3, que se $s_i \equiv a_i$, e s_i é co-primo com m, então a_i deveria ser também. Mas isso significa que haveria $r > \phi(m)$ inteiros entre 0 e $m-1$ co-primos com m – uma contradição.

(iii) Um conjunto com menos de $\phi(m)$ elementos não pode ser um sistema reduzido de resíduos módulo m, porque todo inteiro co-primo com m deve ter representante de sua classe de congruência no sistema, e há pelo menos $\phi(m)$ deles, como já demonstrado na parte (i). □

É relevante que o Lema 8.3 nos permite trocar um elemento a do conjunto por qualquer inteiro b congruente a a módulo m: como são congruentes, continua havendo um representante daquela classe de congruência. Como $\text{mdc}(a, n) = 1$, o Lema garante que $\text{mdc}(b, m) = 1$.

Teorema 8.5. *Se* $\{r_1, r_2, \ldots, r_n\}$ *é sistema completo (ou reduzido) de resíduos módulo* m*, então para qualquer* k *co-primo com* m*, o conjunto* $\{kr_1, kr_2, \ldots, kr_n\}$ *também é.*

Demonstração. Primeiro (i), verificamos que ao multiplicar os elementos por k eles continuam incongruentes entre si; e depois (ii), mostramos que se $\text{mdc}(r_i, m) = 1$ então $\text{mdc}(ar_i, m) = 1$.

(i) se $r_i \not\equiv r_j \pmod{m}$ então $m \nmid (r_j - r_j)$, e também $m \nmid a(r_i - r_j)$, porque pelo enunciado $\text{mdc}(a, m) = 1$, e m não divide a nem $(r_i - r_j)$.

Agora, se $\text{mdc}(r_i, m) = 1$, então $\text{mdc}(ar_i, m) = 1$ também. Suponha que $\text{mdc}(ka, m) = d > 1$. Isto significa que

$$d \mid ar_i$$
$$d \mid m$$

Mas como $\text{mdc}(r_i, m) = 1$, d não poderia dividir tanto m como r_i, logo d deve dividir a e m – mas $\text{mdc}(k, m) = 1$, e d não pode ser diferente de um. □

O sistema reduzido de resíduos módulo 14 que usamos anteriormente é $\{1, 3, 5, 9, 11, 13\}$. Multiplicamos todos por 15 (porque $\text{mdc}(14, 15) = 1$), e temos

$$\{15, 45, 75, 135, 165, 195\},$$

que também é sistema reduzido de resíduos módulo 14.

A seguir apresentamos o Teorema de Euler e o pequeno Teorema de Fermat. O segundo, na verdade, é caso particular do primeiro, portanto apresentaremos concretamente uma só demonstração.

Teorema 8.6 (de Euler)**.** *Se* $\operatorname{mdc}(a, m) = 1$ *então*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Seja $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ um sistema reduzido de resíduos módulo m. Pelo Teorema 8.5, $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ também é um sistema de resíduos módulo m. Agora, como cada $ar_i \equiv r_i \pmod{m}$, então pelo Teorema 6.4 também vale $ar_i ar_j \equiv r_i r_j \pmod{m}$. Multiplique então todos os números ar_i:

$$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

Mas como $\operatorname{mdc}(r_i, m) = 1$ para todos os r_i, podemos usar a lei do cancelamento, eliminando os r_i, e reescrevemos

$$a^{\phi(m)} \equiv 1 \pmod{m}. \qquad \square$$

Como $\phi(14) = 6$, o Teorema de Euler garante que a sexta potência de qualquer inteiro co-primo com 14 será congruente a um módulo 14. Por exemplo,

$$9^6 = 531441 \equiv 1 \pmod{14}.$$

Teorema 8.7 (pequeno Teorema de Fermat)**.** *Se* p *é primo e* $p \nmid a$ *então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat enunciou este Teorema sem demonstração em 1640, ainda sem usar a linguagem de congruências (o que afirmou é que se p é primo e a não é divisível por p, então $a^{p-1} - 1$ é divisível por p). A demonstração foi dada por Euler em 1736; a generalização de Euler foi publicada em 1763.

O pequeno Teorema de Fermat pode ser visto como consequência direta do Teorema de Euler, já que para todo primo p, $\phi(p) = p - 1$. Há outras demonstrações possíveis – pode-se usar argumentos combinatórios, por exemplo. Há também uma demonstração usando teoria de Grupos, que abordaremos mais adiante neste Capítulo.

8.2 Raízes primitivas

Considere o sistema completo de resíduos $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$. Se tomarmos o número 3, e o multiplicarmos iteradamente, vemos que

$$\begin{aligned}
3^1 &= 3 && \equiv 3 \pmod{10} \\
3^2 &= 9 && \equiv 9 \pmod{10} \\
3^3 &= 27 && \equiv 7 \pmod{10} \\
3^4 &= 81 && \equiv 1 \pmod{10} \\
3^5 &= 243 && \equiv 3 \pmod{10} \\
3^6 &= 729 && \equiv 9 \pmod{10} \\
3^7 &= 2187 && \equiv 7 \pmod{10} \\
&\vdots
\end{aligned}$$

Observamos que há um padrão a sequência gerada $(3, 9, 7, 1)$ se repete, e vemos que com potências de 3 conseguimos escrever $1, 3, 9, 7$ módulo 10. Mas com 3 não geramos todos os números módulo dez. Naturalmente nos perguntamos se não há algum outro que o faça.

Mais ainda, notamos que com o número 3, geramos o neutro multiplicativo, 1. Isto significa que todos os elementos no conjunto gerado, $\{1, 3, 7, 9\}$, tem inverso módulo dez! Isto acontece porque, dado 3^k neste conjunto, sempre podemos multiplicá-lo por 3^j, tal que $k + j$ sejam o expoente da próxima potência na classe de congruência do um: Temos $3^2 = 9$. Para calcular o inverso de 9, calculamos $3^9 3^x \equiv 1 \pmod{10}$. Com $x = 2$, conseguimos $3^2 3^2 = 81 \equiv 1 \pmod{10}$.

Veremos adiante que 3 é chamado de "raiz primitiva" módulo dez.

Agora, com 2 não conseguimos gerar neutro:

$$\begin{aligned}
2^1 &= 2 && \equiv 2 \pmod{10} \\
2^2 &= 4 && \equiv 4 \pmod{10} \\
2^3 &= 8 && \equiv 6 \pmod{10} \\
2^4 &= 16 && \equiv 8 \pmod{10} \\
2^5 &= 32 && \equiv 2 \pmod{10} \\
2^6 &= 64 && \equiv 4 \pmod{10} \\
&\vdots
\end{aligned}$$

Por isso, não conseguimos inversos neste conjunto.

O que observamos com as potências de 3 (mas não com as de 2) é que $3^4 \equiv 1 \pmod{10}$, e que 4 e o menor expoente inteiro positivo para o qual

uma potência de 3 é congruente a 1 módulo 10. Isto nos leva à definição de ordem de um elemento em um sistema de resíduos.

Definição 8.8 (ordem de elemento em sistema de resíduos)**.** Se h é o menor inteiro positivo tal que $a^h \equiv 1 \pmod{m}$, dizemos que a **ordem**[1] de a em m é h. ♦

A ordem de 5 módulo 124 é, por exemplo, 3, porque $5^3 = 125$, logo $5^3 \equiv 1 \pmod{124}$.

As primeiras perguntas que fazemos são – sempre há algum elemento a tal que $a^k \equiv 1 \pmod{m}$, para algum k? E se nem sempre existe tal elemento, conseguimos determinar algum critério de existência? O Teorema 8.9 responde com exatidão estas perguntas.

Teorema 8.9. *Existe* h *tal que* $a^h \equiv 1 \pmod{m}$ *se e somente se* $\operatorname{mdc}(a, m) = 1$.

Demonstração. Primeiro, suponha que $\operatorname{mdc}(a, m) = 1$. Devemos ter, pelo Teorema de Euler, $a^{\phi(m)} \equiv 1 \pmod{m}$, portanto podemos usar $h = \phi(m)$.

Agora, suponha que $a^h \equiv 1 \pmod{m}$. Como $\operatorname{mdc}(1, m) = 1$, pelo Teorema 8.3, $\operatorname{mdc}\left(a^h, m\right) = 1$, e $\operatorname{mdc}(a, m) = 1$. □

Damos agora nome a estas potências – o conceito de raiz primitiva é importante porque as raízes primitivas podem ser usadas para descrever completamente sistemas reduzidos de resíduos (todos os elementos no sistema são potências delas).

Definição 8.10 (raiz primitiva)**.** Se g tem ordem $\phi(m)$ módulo m, dizemos que g é uma **raiz primitiva** módulo m. ♦

Para $m = 14$ temos a raiz primitiva 3, porque

$$\begin{aligned}
3^1 &= 3 && \equiv 3 && \pmod{14}\\
3^2 &= 9 && \equiv 9 && \pmod{14}\\
3^3 &= 27 && \equiv 13 && \pmod{14}\\
3^4 &= 81 && \equiv 11 && \pmod{14}\\
3^5 &= 243 && \equiv 5 && \pmod{14}\\
3^6 &= 729 && \equiv 1 && \pmod{14}\\
3^7 &= 2187 && \equiv 3 && \pmod{14}
\end{aligned}$$

O menor expoente para o qual 3^i é congruente a 1 módulo 14 é seis – que também é $\phi(14)$.

Como notamos anteriormente, as classes de congruência de $3^1, 3^2, \ldots$ – e de forma geral, de $g^1, g^2, \ldots$ quando g é raiz primitiva – formam uma

[1] Em terminologia mais antiga, "a pertence ao expoente h módulo m".

sequência que se repete. Temos adiante uma ilustração: na primeira linha, os g^i, onde g é raiz primitiva para algum módulo m; na segunda linha, $a_j < m$ representa a classe de congruencia de g^i.

$$\begin{array}{rc|cccccccccc} g^i = & & g^1 & g^2 & g^3 & \cdots & g^s & g^{s+1} & g^{s+2} & \cdots & g^{2s} & \cdots \\ \equiv & & a_1 & a_2 & a_3 & \cdots & 1 & a_1 & a_2 & \cdots & 1 & \cdots \end{array}$$

Repetimos o exemplo da raiz primitiva 3 módulo 14:

$$\begin{array}{rc|cccccccccccc} 3^i = & & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 & 3^6 & 3^7 & 3^8 & 3^9 & 3^{10} & g^{11} & g^{12} & \cdots \\ \equiv & & 3 & 9 & 13 & 11 & 5 & 1 & 3 & 9 & 13 & 11 & 5 & 1 & \cdots \end{array}$$

Fica claro, então, que se $g^i \equiv 1 \pmod{m}$, então $g^k i$ também será congruente a 1 módulo m. No entanto, não provamos que de fato este comportamento sempre acontece. O Teorema 8.11 trata disso, capturando portanto a característica de repetição da sequência de potências módulo m.

Teorema 8.11. *Se a ordem de a módulo m é h, e $a^k \equiv 1 \pmod{m}$, então $h \mid k$.*

Demonstração. Dividimos k por h:

$$k = qh + r, \quad 0 \leq |r| < h.$$

Agora, do enunciado temos

$$\begin{aligned} 1 &\equiv a^k && \pmod{m} \\ &\equiv a^{qh+r} && \pmod{m} \\ &\equiv (a^h)^q a^r && \pmod{m} \\ &\equiv (1)^q a^r && \pmod{m} \\ &\equiv a^r && \pmod{m} \end{aligned}$$

Mas se $a^r \equiv 1$, e $0 \leq |r| < h$, então $r = 0$, e $h \mid k$. □

A ordem de 9 módulo 14 é 3, porque

$$\begin{aligned} 9^1 = 9 &\equiv 9 && \pmod{14} \\ 9^2 = 18 &\equiv 4 && \pmod{14} \\ 9^3 = 729 &\equiv 1 && \pmod{14}. \end{aligned}$$

Mas sabemos, pelo Teorema de Euler, que $9^6 \equiv 1 \pmod{14}$. E como determina o Teorema 8.11, $3 \mid 6$.

Uma raiz primitiva gera um conjunto de números. O próximo Teorema identifica este conjunto – é um sistema reduzido de resíduos módulo m.

Teorema 8.12. *Se g é raiz primitiva módulo m, então $g, g^2, \ldots, g^{\phi(m)}$ são um sistema reduzido de resíduos módulo m.*

Demonstração. Demonstramos que os g^i são (i) incongruentes entre si, e (ii) co-primos com m.

Começamos com a incongruência dos g^i. Suponha que existam dois elementos $g^s \equiv g^t \pmod{m}$, com $1 \leq s < t \leq \phi(m)$. Então

$$\begin{aligned} m &\mid (g^t - g^s) \\ m &\mid (g^{t-s+s} - g^s) \\ m &\mid (g^{t-s} g^s - g^s) \\ m &\mid g^s(g^{t-s} - 1). \end{aligned}$$

Mas como g é raíz primitiva módulo m, o Teorema 8.9 garante que $\operatorname{mdc}(g, m) = 1$, e $\operatorname{mdc}(g^s, m) = 1$. Concluímos que $m \nmid g^s$, e por isso

$$\begin{aligned} m &\mid (g^{t-s} - 1) \\ g^{t-s} &\equiv 1 \pmod{m} \end{aligned}$$

Então $t - s < \phi(m)$, e $g^{t-s} \equiv 1 \pmod{m}$. Mas como g é raiz primitiva, $\phi(m)$ deveria ser o menor expoente de g congruente a 1 módulo m – e chegamos a uma contradição.

Assim, todos os g^i do enunciado são incongruentes módulo m.

Passamos a outra parte da demonstração, os g^i são co-primos com m. Novamente pelo Teorema 8.9, $\operatorname{mdc}(g, m) = 1$, e evidentemente $\operatorname{mdc}\left(g^k, m\right) = 1$ também, o conjunto é um sistema reduzido de resíduos. □

Uma raiz primitiva módulo 10 é 3, porque $\phi(10) = 4$ e $3^4 \equiv 1 \pmod{10}$. Então os números 3^i, com $1 \leq i \leq 4$ são um sistema reduzido de resíduos:

$$\begin{aligned} 3^1 &\equiv 3 && \pmod{10} \\ 3^2 &\equiv 9 && \pmod{10} \\ 3^3 &\equiv 7 && \pmod{10} \\ 3^4 &\equiv 1 && \pmod{10} \end{aligned}$$

$1, 3, 7, 9$ são os quatro números menores que e co-primos com 10.

Se a tem ordem h, podemos perguntar qual é a ordem de a^k. O Teorema 8.13 e o Corolário 8.14 tratam disso, e serão úteis mais adiante para determinar a quantidade de raízes primitivas para cada m.

Teorema 8.13. *Se a ordem de a é h módulo m, e $\operatorname{mdc}(j, h) = d$, então a ordem de a^j módulo m é h/d.*

Cabe neste ponto um comentário, antes da demonstração. É evidente que, se a ordem de a é h módulo m, então para todo múltiplo de h (por

exemplo, jh),

$$\begin{aligned} a^{jh} &\equiv (a^j)^r \\ &\equiv 1^r \\ &\equiv q \pmod{m}. \end{aligned}$$

O Teorema 8.13 aborda outros casos, onde o expoente não é múltiplo de h, e determina também a ordem de a^j: não basta que $(a^j)s \equiv 1 \pmod{m}$, queremos o *menor* s para o qual isto ocorre.

Demonstração. Se a^j tem ordem k módulo m, então

$$(a^j)^k = a^{jk} \equiv 1 \pmod{m}.$$

Pelo Teorema 8.11, como a ordem de a é h, então

$$h \mid kj$$

Dividimos os dois lados da relação por $\operatorname{mdc}(j,h)$:

$$\underbrace{\left(\frac{h}{\operatorname{mdc}(j,h)}\right)}_{(i)} \;\Big|\; \underbrace{\left(\frac{j}{\operatorname{mdc}(j,h)}\right)}_{(ii)} k$$

Mas como agora (i) é co-primo com (ii), então a relação vale se e somente se $(i) \mid k$:

$$\frac{h}{\operatorname{mdc}(j,h)} \;\Big|\; k.$$

Assim, o menor posistivo n tal que $(a^j)^n \equiv 1 \pmod{m}$ é $h/\operatorname{mdc}(j,h)$. □

Por exemplo, a ordem de 5 módulo 26 é 4:

$$\begin{aligned} 5^1 &\equiv 5 && \pmod{26} \\ 5^2 &\equiv 25 && \pmod{26} \\ 5^3 &\equiv 21 && \pmod{26} \\ 5^4 &\equiv 1 && \pmod{26} \end{aligned}$$

Se perguntarmos qual deve ser a ordem de 5^6 módulo 26, usamos o Teorema 8.13 com $a = 5$, $h = 4$ e $j = 6$. Como $d = \operatorname{mdc}(4,6) = 2$, a ordem de 5^6 é $h/d = 2$:

$$\begin{aligned} (5^6)^1 &\equiv 25 && \pmod{26} \\ (5^6)^2 &\equiv 1 && \pmod{26} \end{aligned}$$

Corolário 8.14. *Se g é raiz primitiva módulo m, então g^k também é raiz primitiva módulo m se e somente se* $\text{mdc}\,(k, \phi(m)) = 1$.

Demonstração. A ordem de g módulo m é $\phi(m)$, por definição (g é raiz primitiva). Se $\text{mdc}\,(k, \phi(m)) = 1$, então pelo Teorema 8.13, a ordem de g^k é

$$\frac{\phi(m)}{\text{mdc}\,(k, \phi(m))},$$

que só pode ser igual a $\phi(m)$ se $\text{mdc}\,(k, \phi(m)) = 1$. □

Como exemplo, escolhemos $m = 18$. Uma raiz primitiva módulo 18 é 5, que podemos encontrar por sucessivas tentativas (2, 3, 4 falham, e 5 gera todos os 18 elementos). Quem são as outras raízes primitivas? Certamente podem ser escritas como 5^k, porque *todo* elemento em $\mathbb{Z}_{18}$ pode. Agora, 5^k pode ser raiz primitiva módulo dezoito se e somente se k for co-primo com $\phi(18) = 6$ – ou seja, se k for 1 ou 5.

$$5^1 \equiv 5 \pmod{18}$$
$$5^5 \equiv 11 \pmod{18}$$

As raízes primitivas módulo 18 são, portanto, 5 e 11.

Agora passa a ser simples contar as raízes primitivas módulo m.

Teorema 8.15. *Há exatamente zero ou $\phi(\phi(m))$ raízes primitivas modulo m.*

Demonstração. Suponha que haja raízes primitivas, e que g seja uma delas. Há $\phi(m)$ elementos no sistema reduzido de resíduos $g, g^2, \ldots, g^{\phi(m)}$. O Corolário 8.14 determina que g^k é raiz primitiva módulo m se e somente se k é co-primo com $\phi(m)$. Existem $\phi(\phi(m))$ elementos assim. □

Finalmente, enunciamos sem demonstração o Teorema das Raízes Primitivas, que permite determinar exatamente para quais números m existem raízes primitivas.

Teorema 8.16 (das Raízes Primitivas)**.** *Existem raízes primitivas módulo m se e somente se $m = 1$, $m = 2$, $m = 4$, $m = p^k$, ou $m = 2p^k$, onde p é primo ímpar.*

Por exemplo, 15 é produto de dois primos ímpares, e não é da forma prescrita no Teorema. Não há, portanto, raízes primitivas módulo 15.

Já $50 = (2)5^2$ é o dobro da potência de um único primo ímpar, e há $\phi(\phi(50)) = 8$ raízes primitivas módulo 50, que são $3, 13, 17, 23, 27, 37$ e 47.

8.3 Raízes primitivas com módulo primo

Apesar de não termos demonstrado o Teorema 8.16 (das raízes primitivas), podemos facilmente provar que sempre há raízes primitivas módulo p quando p é primo. De fato, já o fizemos!

Teorema 8.17. *Sempre há raízes primitivas quando o módulo é primo.*

Demonstração. Segue imediatamente do Teorema 8.9. □

Podemos também tirar algumas conclusões a respeito de raízes primitivas módulo p, que nos serão úteis mais tarde.

Teorema 8.18. *Se g é raiz primitiva módulo $p \in \mathbb{Z}$ e p é primo, então*

$$g^{p-1} \equiv +1 \pmod{p}$$
$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Demonstração. A primeira parte é o pequeno Teorema de Fermat.

Para a segunda parte, veja que

$$\left(g^{\frac{p-1}{2}}\right)\left(g^{\frac{p-1}{2}}\right) = g^{p-1} \equiv 1 \pmod{p}$$

Como o número entre parênteses multiplicado por ele mesmo é congruente a um, ele deve ser congruente a $+1$ ou -1. Mas não pode ser $+1$, porque se fosse, teríamos

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

o que não pode ocorrer, porque g é raiz primitiva, e sua ordem (o *menor* expoente k tal que g^k é congruente a um) é $p-1$. Portanto, $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Observe que nesta demonstração usamos o fato da equação $x^2 \equiv 1 \pmod{p}$ ter somente duas soluções módulo p ($+1$ e -1), e também o fato de haver ordem neste anel – foi crucial observar que $(p-1)/2 < (p-1)$.

Exemplificamos:

$$2^6 = 64 \equiv 16 \equiv -1 \pmod{13}$$
$$2^{12} = 4096 \equiv +1 \pmod{13}$$

8.4 Grupos

Um grupo é uma estrutura algébrica com uma única operação. Os sistemas de resíduos de que tratamos são exemplos de grupos – e demonstraremos nesta seção o Teorema de Euler usando alguns fatos básicos sobre grupos.

Definição 8.19 (grupo)**.** Um **grupo** é um conjunto onde está definida uma operação binária, que por ora denotaremos $\odot$, tal que

(i) $\odot$ é associativa;

(ii) há um neutro e no conjunto: $a \odot e = e \odot a = a$;

(iii) todo elemento a tem inverso $\overline{a}$, tal que $a \odot \overline{a} = e$.

Se a operação $\odot$ é comutativa, dizemos que o grupo é comutativo, ou "abeliano".

A quantidade de elementos em um grupo finito é chamada de *ordem* do grupo. ⧫

Listamos agora alguns exemplos de grupos.

Exemplo 8.20.

- Os inteiros, com a operação de soma: a operação é associativa; existe o neutro zero; e todo inteiro n tem inverso aditivo $-n$. O grupo é comutativo.
- Os reais sem o zero, com a operação de multiplicação: a operação é associativa; existe o neutro um; todo real $x \neq 0$ tem inverso multiplicativo $1/x$. O grupo é comutativo.
- Em um espaço vetorial, os vetores formam um grupo com a operação de soma: a operação é associativa; existe o vetor neutro zero; todo vetor v tem um inverso $-v$. Este grupo é comutativo, porque $v + w = w + v$
- O conjunto das matrizes com entradas reais e a mesma quantidade de linhas e colunas, usanado a operação usual de soma: a soma de matrizes é associativa, existe como neutro a matriz zero, e toda matriz A tem uma inversa aditiva $-A$. Além disso, o grupo é comutativo, porque $A + B = B + A$.
- O conjunto das matrizes quadradas não singulares de ordem n, com a operação de multiplicação. A multiplicação de duas matrizes não singulares resulta em outra matriz não singular[2]; a operação de mutiplicação de matrizes é asosciativa, $A(BC) = (AB)C$; existe o neutro multiplicativo I (a matriz identidade); e toda matriz não-singular A tem inversa A^{-1}. O grupo *não* é comutativo porque, em geral, $AB \neq BA$.
- Seja $(R, +, \cdot)$ um anel. Se considerarmos somente a operação de adição em R, temos um grupo (isto segue diretamente da definição de anel).

[2]Nos outros exemplos era evidente que a operação é fechada, mas aqui faz sentido mencionar que a multiplicação não gerará uma matriz fora do conjunto que especificamos.

- Seja A um conjunto. Então o conjunto $S(A)$ de todas as bijeções $\sigma : A \to A$, de A nele mesmo (ou seja, $S(A)$ é o conjunto das permutações de A), é um grupo com a função identidade como elemento neutro; composição como operação de grupo; e função inversa como inverso de cada bijeção.

- Finalmente, o conjunto unitário $\{x\}$ com uma operação $x \cdot x = x$ é um grupo. A operação é evidentemente associativa (por vacuidade); o único elemento, x, é o neutro, e o inverso do único elemento é ele mesmo. Além disso o grupo é, por vacuidade, comutativo. ◀

O Teorema 8.21 nos permitirá trabalhar com expoentes da maneira usual em grupos. Sua demonstração é pedida no Exercício 184.

Teorema 8.21. *Seja* G *um grupo, onde denotamos a operação por* $\cdot$ *(da mesma forma que a multiplicação usual), e onde também denotamos por* x^a *a aplicação da operação* $a-1$ *vezes em* x*,*

$$x^a = \underbrace{x \cdot x \cdot x \cdot \cdots x}_{a-1 \text{ operações}}.$$

Em G *valem as leis usuais para expoentes:*

$$(x^a)^b = x^{ab},$$
$$x^{a+b} = x^a x^b.$$

O Teorema vale independente da comutatividade da operação, porque trata apenas de um único elemento (x).

Tanto adição como multiplicação em inteiros (e reais) são operações que podem ser usadas na definição de um grupo, e em diferentes situações pode-se usar uma ou outra notação. Nesta situação, as leis de cancelamento são

$$(a(b(x)) = (ab)x,$$
$$(a + b)x = ax + bx.$$

No exemplo a seguir é possível não apenas perceber que as leis de expoentes valem, mas também observar o funcionamento da estrutura de grupo.

Exemplo 8.22. Seja $(G, \odot)$ um grupo, com

$$G = \{e, a, b, c\}$$

e $\odot$ dada pela tabela a seguir.

$\odot$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Verificamos que $c^5 = c^2 \odot c^3$. No desenvolvimento, os trechos sublinhados correspondem àqueles onde a operaçõa será aplicada.

$$\begin{aligned} c^5 &= \underline{c \odot c} \odot c \odot c \odot c \\ &= \underline{a \odot c} \odot c \odot c \\ &= \underline{d \odot c} \odot c \\ &= \underline{b \odot c} \\ &= e. \end{aligned}$$

Da mesma forma,

$$\begin{aligned} c^2 &= \underline{c \odot c} \\ &= a, \\ c^3 &= \underline{c \odot c} \odot c \\ &= \underline{a \odot c} \\ &= d, \end{aligned}$$

portanto $c^2 \odot c^3 = a \odot d = e$.

Observamos também que o grupo é comutativo, porque a tabela é simétrica. ◀

Teorema 8.23. *Todo sistema reduzido de resíduos módulo n é um grupo comutativo com a operação de multiplicação módulo n, com neutro igual a um. A ordem do grupo é $\phi(n)$.*

Demonstração. Se a, b pertencem a um sistema reduzido de resíduos módulo m, então $\operatorname{mdc}(a, m) = \operatorname{mdc}(b, m) = 1$. Isto significa que $\operatorname{mdc}(ab, m)$ também é um, e ab tem representante de sua classe de congruência no sistema. Assim, a operação é fechada no conjunto.

A multiplicação é associativa; existe o elemento neutro 1, ou algum $x \equiv 1 \pmod{m}$ no sistema; falta somente verificar que todo elemento tem inverso. O inverso de um elemento a é $\overline{a}$, tal que $a\overline{a} \equiv 1 \pmod{m}$. Esta equação tem solução se e somente se $\operatorname{mdc}(a, m) = 1$ – o que é verdadeiro. □

O Teorema 8.11 pode ser visto como caso particular do Teorema 8.24,

para grupos.

Teorema 8.24. *Seja x um elemento de ordem n em um grupo, e suponha que $x^k = 1$, com k inteiro positivo. Então $n \mid k$.*

Demonstração. Expresse a divisão de k por n como $k = nq + r$, com q, r inteiros positivos e $0 \leq r < n$. Então

$$\begin{aligned} 1 &= x^k \\ &= x^{nq+r} \\ &= (x^n)^q x^r \\ &= x^r, \end{aligned}$$

então $r = 0$ e $n \mid k$. □

Em nossa discussão sobre raízes primitivas verificamos que as potências $g^1, g^2, \ldots$ formam um padrão que se repete ciclicamente. Isto acontece porque para algum n, $g^n = g$. Dizemos que grupos como este são *cíclicos*.

Definição 8.25 (grupo cíclico)**.** Um grupo é **cíclico** se todos seus elementos podem ser esritos como potência de algum elemento: $x = ggg\ldots g = g^n$, para algum n. Um elemento g usado desta forma para descrever todos os outros é um gerador do grupo. ⧫

Evidentemente as raízes primitivas em sistemas reduzidos de resíduos são geradores, o que significa que estes sistemas são grupos cíclicos.

Teorema 8.26. *Um sistema reduzido de resíduos é um grupo cíclico.*

Demonstração. Uma raiz primitiva módulo m gera o sistema reduzido de resíduos. □

É natural a definição de subgrupo – um grupo dentro de outro grupo.

Definição 8.27 (subgrupo)**.** Seja G um grupo. Um subconjunto H de G é **subgrupo** de G se também ele é grupo, com a mesma operação. ⧫

As matrizes triangulares inferiores formam um grupo com a operação de adição, portanto são um subgrupo do grupo de todas as matrizes.

Os inteiros pares com a operação de soma formam um subgrupo de $\mathbb{N}$.

As matrizes quadradas (com ordem n fixa) com determinante ± 1 formam um grupo com a operação de multiplicação – um subgrupo do grupo das matrizes não singulares.

Teorema 8.28 (de Lagrange)**.** *A ordem de um subgrupo divide a ordem do grupo.*

O Teorema de Lagrange é um dos resultados mais elementares em Teoria de Grupos – mas com ele já podemos elaborar uma demonstração mais interessante do Teorema de Euler.

Demonstração do Teorema de Euler. Seja $a < n$, co-primo com n. Então as potências de a módulo n – $a, a^2, \ldots, a^t \pmod n$ – formam um subgrupo, onde $a^t \equiv a^0 \equiv 1 \pmod n$. De acordo com o Teorema de Lagrange, $t \mid \phi(n)$ (ou seja, $kt = \phi(n)$). Então

$$\begin{aligned} a^{\phi(n)} &\equiv a^{kt} \\ &\equiv (a^t)^k \\ &\equiv 1^k \\ &\equiv 1 \pmod n. \end{aligned}$$ □

É também interessante comparar o Teorema de Lagrange com o Teorema 8.11.

8.4.1 O grupo de unidades

Se n não é primo, nem todo elemento em $\mathbb{Z}_n$ tem inverso (ou seja, nem todos são unidades). Quando escolhemos apenas as unidades em $\mathbb{Z}_n$, obtemos um sistema reduzido de resíduos onde todos os elementos tem inverso – este é o *grupo de unidades módulo* n.

Definição 8.29 (grupo de unidades módulo n)**.** Para todo inteiro positivo n, definimos o **grupo de unidades módulo** n como o subconjunto de $\mathbb{Z}_n$ onde todos os elementos são unidades módulo n; a operação de grupo é a multiplicação módulo n. Denotamos este grupo por U_n. ♦

Exemplo 8.30. As unidades módulo 10 são $1, 3, 7, 9$, portanto estes são os elementos do grupo U_{10}, onde a operação de grupo é a multiplicação módulo 10. ◀

Teorema 8.31. *O grupo U_n é cíclico.*

A demonstração do Teorema 8.32 é pedida no Exercício 199.

Teorema 8.32. *Seja n um inteiro positivo. Então $\mathbb{Z}_{\phi n}$ é grupo com a operação de multiplicação; além disso, U_n é isomorfo a $\mathbb{Z}_{\phi n}$.*

Exercícios

Ex. 173 — Prove que em uma lista de $k + 1$ números $a_1, a_2, \ldots, a_{k+1}$ há pelo menos dois números, a_i e a_j, tais que $(a_i - a_j) \mid k$.

Ex. 174 — Encontre todas as raízes primitivas módulo 5, 7, 9, e 11.

Ex. 175 — Mostre um sistema completo de resíduos módulo 13 contendo somente inteiros ímpares.

Ex. 176 — Suponha que $a^{n-1} \equiv 1 \pmod{n}$ mas que, para todo d divisor próprio de $n-1$, $a^d \not\equiv 1 \pmod{n}$. Prove que n é primo.

Ex. 177 — Fixe $n > 1$ inteiro e defina $\omega = e^{\frac{2\pi i}{n}}$ ($\omega \in \mathbb{C}$), e

$$\Omega_n = \{0, \omega, \omega^2, \ldots, \omega^{n-1}\}.$$

Prove que para qualquer conjunto $\{k_0, k_1, \ldots, k_{n-1}\} \subseteq \mathbb{Z}$,

$$\Omega_n = \{\omega^{k_0}, \omega^{k_1}, \ldots, \omega^{k_{n-1}}\}$$

se e somente se $k_0, k_1, \ldots, k_{n-1}$ é sistema completo de resíduos módulo n

Ex. 178 — Prove que se $\{a_1, a_2, \ldots, a_k\}$ é um sistema reduzido de resíduos módulo p, então $\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_k}\}$, onde $\overline{a_i}$ é o inverso de a_i módulo p, também é.

Ex. 179 — Seja $\{a_1, a_2, \ldots, a_k\}$ um sistema reduzido de resíduos módulo m (e portanto $k = \phi(m)$). Prove que $\{a_1^r, a_2^r, \ldots, a_k^r\}$ também é sistema reduzido de resíduos se e somente se $\text{mdc}\,(r, \phi(m))$.

Ex. 180 — Seja p primo. Prove que 1 e $p-1$ são os únicos números no conjunto $\{0, 1, \ldots, p-1\}$ cujos quadrados são congruentes a um módulo p.

Ex. 181 — Sejam a, b raízes primitivas módulo p, um primo ímpar. Prove que ab não pode ser raiz primitiva módulo p.

Ex. 182 — Prove que se p é um primo ímpar e a tem ordem $2k$ módulo p, então $a^k \equiv -1 \pmod{p}$.

Ex. 183 — Prove que o conjunto dos inteiros módulo m, para todo $m \geq 0$, é um grupo comutativo com a operação de soma módulo m.

Ex. 184 — Demonstre o Teorema 8.21.

Ex. 185 — O conjunto $G = \{a, b, c, d, e\}$, com a operação a seguir é um grupo? Se for, é comutativo?

$\odot$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Ex. 186 — Seja $m > 2$. Os números $1^2, 2^2, 3^2, \ldots, m^2$ formam um sistema completo de resíduos módulo m?

Ex. 187 — Seja p um primo ímpar, e sejam $\{s_1, s_2, \ldots, s_{p-1}\}$ e $\{t_1, t_2, \ldots, t_{p-1}\}$ dois sistemas completos de resíduos módulo p. Prove que $\{s_1t_1, s_2t_2, \ldots, s_kt_k\}$ não pode ser sistema completo de resíduos módulo p.

Ex. 188 — Se p é um primo ímpar e g é raiz primitiva módulo p^k, quando g também seria raiz primitiva módulo $2p^k$?

Ex. 189 — (Olimpíada Matemática de São Petersburgo) Prove que $m \mid \phi(a^m - 1)$ para todos os inteiros a e m.

Ex. 190 — Seja $n \in \mathbb{Z}$ tal que $3 \nmid n$ ou tal que $9 \mid n$. Prove que $n^7 \equiv n \pmod{63}$.

Ex. 191 — Sejam a, b co-primos. Prove que $\{0, a, 2a, 3a, \ldots, (b-a)a\}$ é um sistema completo de resíduos módulo b.

Ex. 192 — Mostre que se $a_1, a_2, \ldots, a_k$ é um sistema reduzido de resíduos módulo m, onde $m > 2$, então $\sum_i a_i \equiv 0 \pmod{m}$.

Ex. 193 — Prove que para todo inteiro positivo n maior que um, $n \mid \phi(2^n - 1)$.

Ex. 194 — Seja p primo e $\{a_1, a_2, \ldots, a_k\}$ um sistema completo de resíduos módulo p. Prove que para todo inteiro n existe r tal que

$$n = \sum_{i=0}^{r} x_i p^i \pmod{p^{r+1}},$$

onde x_i é algum dos a_i.

Ex. 195 — Suponha que $p > 3$ seja primo. Prove que o produto das raízes primitivas entre 1 e $p-1$ módulo p é congruente a 1 módulo p.

Ex. 196 — Prove que se $\text{mdc}(a, b) = 1$ e a ordem de a módulo b é rs, então a ordem de b^s em a é t.

Ex. 197 — Dois grupos $(G, \odot)$ e $(H, \boxdot)$ são isomorfos se existe uma bijeção entre eles que preserva estrutura – ou seja, se existe $f : G \to H$ bijetora tal que $\forall a, b \in G$, $f(a \odot b) = f(a) \boxdot f(b)$.

(a) Prove que os grupos aditivos definidos por dois sistemas completos de resíduos com o mesmo módulo são isomorfos, e que por isso podemos tratá-los como se fossem um só: "*o* sistema completo de resíduos módulo m".

(b) Faça o mesmo com grupos multiplicativos definidos por sistemas reduzidos de resíduos.

Ex. 198 — Suponha que g seja raiz primitiva módulo p^k. Prove que g também é raiz primitiva módulo p.

Ex. 199 — Demonstre o Teorema 8.32.

Ex. 200 — Prove que em qualquer grupo, todo elemento tem um único inverso.

Ex. 201 — Seja $C \subset \mathbb{R}^2$ o conjunto de pontos da circunferência unitária,

$$C = \{(x, y) \mid x^2 + y^2 = 1\}.$$

Este conjunto pode ser um grupo, onde

- $e = (1, 0)$ é o elemento neutro;
- o inverso de cara ponto (x, y) é $\overline{(x, y)} = (x, -y)$.

a) Determine uma operação de grupo.

b) Verifique que o mesmo vale se trocarmos $\mathbb{R}$ por qualquer corpo.

Capítulo 9

Resíduos Quadráticos

Limitamo-nos até o momento ao estudo de congruências lineares – mais especificamente, as da forma $ax \equiv b \pmod{m}$. Este Capítulo trata de congruências envolvendo quadrados.

O problema de resolver equações quadráticas na forma geral pode ser reduzido ao de resolver equações da forma $x^2 = a \pmod{p}$, de que tratamos a partir de agora. Ao final deo Capítulo mostramos como resolver a equação geral de segundo grau tendo método apenas para a equação mais simples $x^2 \equiv a \pmod{p}$.

9.1 Resíduos Quadráticos

Inicialmente, damos um nome aos quadrados módulo m.

Definição 9.1 (resíduo quadrático)**.** Dizemos que a é um **resíduo quadrático** módulo m se a equação $x^2 \equiv a \pmod{m}$ tem solução.

Denotamos por Q_n o conjunto (ou ainda, o grupo) dos resíduos quadráticos módulo n. ♦

O critério de Euler permite determinar quando um elemento é quadrado módulo p, se p for primo.

Teorema 9.2 (critério de Euler)**.** *Se p é primo, então a é resíduo quadrático módulo p se e somente se*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Demonstração. Se a é resíduo quadrático módulo p, então

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (x^2)^{\frac{p-1}{2}} && \pmod p \\ &\equiv x^{p-1} && \pmod p \\ &\equiv 1 && \pmod p. \qquad \text{(pelo Teorema de Euler)} \end{aligned}$$

Agora suponha que $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Como p é primo, deve haver alguma raiz primitiva g módulo p, e existe algum k tal que $g^k \equiv a \pmod p$. Agora reescrevemos a congruência do enunciado,

$$(g^k)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p$$

Mas a ordem de g é $p-1$, porque é raiz primitiva, e portanto $k(p-1)/2$ deve ser múltiplo de $p-1$. Então $k/2$ é inteiro, e k é par. Como $g^k \equiv g^{2j} \equiv a \pmod p$, a é resíduo quadrático. □

Um exemplo com módulo 13: elevamos 7 ao quadrado; 49 é resíduo quadrático módulo 13; mas como $49 \equiv 10 \pmod{13}$, então 10 é resíduo quadrático módulo 13. Observamos que que $10^6 \equiv 1 \pmod{13}$, porque $10^3 10^3 = 130^6$ e $10^6 = 76923(13) + 1$. Usamos o Teorema de Euler e confirmamos que 10 é resíduo quadrático módulo 13:

$$10^{12} \equiv 1 \pmod{13}.$$

Corolário 9.3. *A quantidade de resíduos quadráticos módulo p é exatamente igual à de resíduos não quadráticos.*

Demonstração. Seja g um gerador de $\mathbb{Z}_p$. Podemos descrever $\mathbb{Z}_p$, portanto como

$$\mathbb{Z}_p = \left\{ g^0, g^1, g^2, \ldots, g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, g^{\frac{p-1}{2}+1}, \ldots, g^{p-2} \right\}.$$

Então os quadrados módulo $\mathbb{Z}_p$ são

$$\begin{aligned} \mathbb{Z}_p &= \left\{ g^0, g^2, g^4, \ldots, g^{p-1-2}, g^{p-1}, g^{p-1+2}, g^{\frac{p-1}{+}4}, \ldots, g^{2p-4} \right\}. \\ &= \left\{ g^0, g^2, g^4, \ldots, g^{p-3}, 1, g^{p-1}g^2, g^{p-1}g^4 \ldots, g^{p-1}g^{p-3} \right\}. \\ &= \left\{ g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^2, g^4 \ldots, g^{p-3} \right\}. \end{aligned}$$

Notamos que a sequência se repete duas vezes. Temos somente que mostrar que estes são todos incongruentes modulo p Suponha que r^2 e s^2 sejam congruentes módulo p. Mas se $r^2 \equiv s^2 \pmod p$, então e $r^2 - s^2 \equiv 0 \pmod p$, ou seja, $(r+s)(r-s) \equiv 0 \pmod p$, e $r \equiv \pm s \pmod p$. □

Por exemplo, para $p = 11$ há cinco resíduos quadráticos $(1, 3, 4, 5, 9)$, e cinco não quadráticos $(2, 6, 7, 8, 10)$.

Lema 9.4. *Seja s o número de primos diferentes entre si que dividem um inteiro positivo n. Se $a \in U_n$ é resíduo quadrático, a quantidade R de elementos x de U_n tais que $x^2 = a$ é*

$$R = \begin{cases} 2^{s+1} & n = 8k \\ 2^{s-1} & n = 4k+2 \\ 2^s & \textit{em outros casos} \end{cases}$$

Demonstração. Se a está em Q_n, então existe algum x em U_n tal que $x^2 = a$. Qualquer unidade $y \in U_n$ é da forma $y = rx$ para algum r em U_n (r é o inverso de x). Então, $s^2 = a$ se e somente se $(rx)^2 = a$ e, consequentemente, $r^2 = 1$. Assim, a quantidade R é igual à quantidade de soluções de $x^2 = 1$ em U_n. □

O Exercício 214 pede a demonstração do Teorema 9.5.

Teorema 9.5. *O conjunto Q_n dos resíduos quadráticos módulo n é subgrupo de U_n.*

Há duas funções que facilitam cálculos a respeito de resíduos quadráticos – estas são chamadas de *"símbolo de Legendre"* e *"símbolo de Jacobi"*.

Definição 9.6 (símbolos de Legendre e Jacobi)**.** Se p é primo ímpar, então o **símbolo de Legendre** para a e p é

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \not\equiv 0 \pmod p \text{ e } a \text{ é resíduo quadrático módulo } p \\ 0 & \text{se } p \mid a \\ -1 & \text{em outros casos.} \end{cases}$$

Se m não é primo, e $m = p_1 p_2 \cdots p_k$, definimos o **símbolo de Jacobi**

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

Os símbolos de Legendre e Jacobi podem também ser denotados por (a/p), (a/m). ♦

Como já mencionamos que as classes de congruência de resíduos quadráticos módulo 11 são $1, 3, 4, 5, 9$, então

$$\left(\frac{5}{11}\right) = +1, \quad \left(\frac{6}{11}\right) = -1, \quad \left(\frac{22}{11}\right) = 0,$$

O critério de Euler pode ser reescrito, portanto como "$(a/p) = +1$ se e somente se $a^{(p-1)/2} \equiv 1 \pmod p$".

Teorema 9.7. *Se* p *é primo e* $a \equiv b \pmod{p}$*, então*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \tag{i}$$

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \tag{ii}$$

Demonstração. (i) segue naturalmente da definição do símbolo de Legendre:

- se $(a/p) = 0$, então $p \mid a$; mas se $a \equiv b \pmod{p}$, então $p \mid b$, e $(b/p) = 0$;
- se $(a/p) = 1$, então a é quadrado módulo p; mas se $b \equiv a \pmod{p}$, então $b \equiv a \equiv x^2 \pmod{p}$, e $(b/p) = 1$;
- se $(a/p) = -1$, então a não se enquadra nos casos já discutidos, e se $b \equiv a \pmod{p}$, b também não pode se enquadrar neles. Assim, $(b/p) = -1$.

(ii) é verdadeira porque

- se $(a/p) = 0$, então $p \mid a$, e $p \mid ab$, logo $(ab/p) = 0$;
- se $(a/p) = +1$, então $a \equiv b \equiv x^2 \pmod{p}$, e $ab \equiv x^2x^2 \pmod{p}$, logo $(ab/p) = 1$;
- se $(a/p) = -1$, então como $a \equiv b \pmod{p}$, temos $ab \equiv aa \pmod{p}$, e $(ab/p) = 1$. □

Teorema 9.8. *Se* p *é primo, então*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Demonstração. Se $p \mid a$, então $p \mid a^{\frac{p-1}{2}}$, e $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$, logo

$$\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Pelo critério de Euler, se a é resíduo quadrático módulo p, então

$$\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Se $a \not\equiv 0 \pmod{p}$ não é resíduo quadrático, então

$$\begin{aligned} a^{\frac{p-1}{2}} &= (g^{2k+1})^{\frac{p-1}{2}} && \pmod{p} \\ &\equiv g^{\frac{(2k+1)(p-1)}{2}} && \pmod{p} \\ &\equiv g^{k(p-1)} g^{\frac{p-1}{2}} && \pmod{p} \\ &\equiv (1)(-1) && \pmod{p} \\ &\equiv -1 && \pmod{p} \end{aligned}$$

Assim, nos três casos (quando $(a/p) = -1, 0 + 1$), o enunciado vale. □

9.2 Reciprocidade Quadrática

A Lei da Reciprocidade Quadrática, que enunciamos a seguir, foi chamada por Gauss de "Teorema de Ouro". Gauss apresentou pelo menos oito demonstrações desse Teorema; depois dele, surgiram mais de uma centena (incluindo pequenas variações, mas ainda assim um número notável).

Teorema 9.9 (Lei da Reciprocidade Quadrática)**.** *Sejam* $p \neq q$ *dois primos ímpares, e considere as equações*

$$\begin{aligned} x^2 &\equiv q \pmod{p} \\ x^2 &\equiv p \pmod{q} \end{aligned}$$

Se os dois primos forem da forma $4k + 3$*, então uma delas tem solução e a outra não.*

Se pelo menos um dos primos for da forma $4k + 1$*, então ou as duas equações tem solução, ou nenhuma tem.*

Reformulamos agora o Teorema, de maneira a facilitar sua demonstração – usaremos o símbolo de Lagrange. Afirmamos que

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

exceto quando p e q são da forma $4k+3$, quando vale a negação da igualdade acima.

Considere a expressão

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

analisando as possibilidades para os expoentes:

p, q	$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$		paridade	valor
$4k+1, 4j+1$	$\frac{(4k)(4j)}{4}$	$= 4kj$	par	$+1$
$4k+3, 4j+3$	$\frac{(4k+2)(4j+2)}{4}$	$= 4kj + 2j + 2k + 1$	ímpar	-1
$4k+3, 4j+1$	$\frac{(4k+2)(4j)}{4}$	$= 16kj + 8j$	par	$+1$

Isto nos permite reformular a Lei da Reciprocidade quadrática sem mencionar explicitamente os tipos de primo ($4k+1$, $4k+3$).

Teorema 9.10 (Lei da Reciprocidade Quadrática)**.** *Se* $p \neq q$ *são primos ímpares, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Apresentamos duas das demonstrações mais simples deste Teorema: a de Eisenstein, através da contagem de pontos em um reticulado, e a de Rousseau, que depende apenas de resultados básicos da Teoria de Números.

9.2.1 Demonstração Geométrica de Eisenstein

Nesta seção detalharemos a demonstração geométrica dada por Eisenstein, que é provavelmente uma das mais simples. Para esta demonstração, Eisenstein formulou um Lema, não muito diferente de outro, proposto por Gauss.

Definição 9.11. $LR_m(x)$ é o menor representante da classe de equivalência de x módulo m:

$$LR_m(x) = \text{menor } a \text{ em } [0, m) \text{ tal que } a \equiv x \pmod{m}. \qquad \blacklozenge$$

Exemplo 9.12. Temos por exemplo $3 \equiv 12 \equiv -6 \pmod 9$, mas $LR_9(3) = LR_9(12) = LR_9(-6) = 3$. ◀

O Lema de Eisenstein estabelece uma relação importante entre dois primos p e q e o símbolo de Legendre (q/p).

Lema 9.13 (de Eisenstein)**.** *Seja* p *um primo ímpar e* q *um ímpar positivo. Então*

$$\left(\frac{q}{p}\right) = (-1)^{\sum \left\lfloor \frac{qu}{p} \right\rfloor},$$
$$\textit{com } u = 2, 4, 6, \ldots, p-1$$

Exemplo 9.14.

$$\begin{aligned}\left(\frac{5}{11}\right) &= (-1)^{\lfloor\frac{2\cdot5}{11}\rfloor+\lfloor\frac{4\cdot5}{11}\rfloor+\lfloor\frac{6\cdot5}{11}\rfloor+\lfloor\frac{8\cdot5}{11}\rfloor+\lfloor\frac{10\cdot5}{11}\rfloor}\\ &= (-1)^{\lfloor\frac{10}{11}\rfloor+\lfloor\frac{20}{11}\rfloor+\lfloor\frac{30}{11}\rfloor+\lfloor\frac{40}{11}\rfloor+\lfloor\frac{50}{11}\rfloor}\\ &= (-1)^{0+1+2+3+4}\\ &= +1.\end{aligned}$$

De fato, 5 é resíduo quadrático módulo 11, já que $4^2 = 16 \equiv 5 \pmod{11}$. ◀

Exemplo 9.15. Escolhemos desta vez 7 módulo 13:

$$\begin{aligned}\left(\frac{7}{13}\right) &= (-1)^{\lfloor\frac{2\cdot7}{13}\rfloor+\lfloor\frac{4\cdot7}{13}\rfloor+\lfloor\frac{6\cdot7}{13}\rfloor+\lfloor\frac{8\cdot7}{13}\rfloor+\lfloor\frac{10\cdot7}{13}\rfloor+\lfloor\frac{12\cdot7}{13}\rfloor}\\ &= (-1)^{\lfloor\frac{14}{13}\rfloor+\lfloor\frac{28}{13}\rfloor+\lfloor\frac{42}{13}\rfloor+\lfloor\frac{56}{13}\rfloor+\lfloor\frac{70}{13}\rfloor+\lfloor\frac{84}{13}\rfloor}\\ &= (-1)^{1+2+3+4+5+6}\\ &= (-1)^{21}\\ &= -1.\end{aligned}$$

E 7 *não* é resíduo quadrático módulo 13. ◀

A demonstração dada aqui é a mesma de Eisenstein, com a simplificação de notação sugerida por Gauss, que observou que o menor inteiro positivo representando $qu \pmod p$ é $\left\lfloor \frac{qu}{p} \right\rfloor$.

Demonstração. Observando o somatório $\sum \left\lfloor \frac{qu}{p} \right\rfloor$, vemos que será útil definir

$$r(u) = \mathrm{LR}_p(qu),$$

a classe de equivalência módulo p no numerador.

Primeiro, notamos que

$$r(u)$$

é par, porque $u = 2k$ (ou seja, u é par), logo $r(u) \equiv (2k)q \pmod p$.

Além disso,

$$(-1)^{r(u)}r(u) \pmod p$$

é também par.

Agora observamos também que os $(-1)^{r(u)}r(u)$ são todos distintos módulo p. Suponha que existam u e t, tais que $(-1)^{r(u)}r(u) \equiv (-1)^{r(t)}r(t)$

$(\mathrm{mod}\ p)$. Então teríamos

$$\begin{aligned}(-1)^{r(u)}r(u) &\equiv (-1)^{r(t)}r(t) \pmod p\\ \pm r(u) &\equiv r(t) \pmod p\\ \pm qu &\equiv qt \pmod p\\ \pm u &\equiv t \pmod p\\ r(u) &= r(t).\end{aligned}$$

Há $(p-1)/2$ valores diferentes para $(-1)^{r(u)}r(u)$, porque o somatório foi definido para $u = 2, 4, 6, p-1$. Como são todos distintos módulo p, eles devem portanto ser (módulo p) uma permutação da sequência $2, 4, 6, \ldots, p-1$.

Calculamos

$$\begin{aligned}\prod r(u) &\equiv \prod qu\\ &\equiv 2q \cdot 4q \cdot 6q \cdots (p-1)q\\ &\equiv q^{\frac{p-1}{2}} \prod u \pmod p.\end{aligned}$$

Mas como os $(-1)^{r(u)}r(u)$ são permutação de $2, 4, 6, \ldots, p-1$ módulo p,

$$\begin{aligned}\prod u &\equiv \prod (-1)^{r(u)}r(u)\\ \prod u &\equiv (-1)^{\sum r(u)} \prod r(u)\\ \prod u &\equiv (-1)^{\sum r(u)} q^{\frac{p-1}{2}} \prod u\\ 1 &\equiv (-1)^{\sum r(u)} q^{\frac{p-1}{2}}\\ (-1)^{\sum r(u)} &\equiv q^{\frac{p-1}{2}}\\ (-1)^{\sum r(u)} &\equiv \left(\frac{q}{p}\right) \pmod p.\end{aligned}$$

Ao analisar a demonstração de Eisenstein, Gauss observou que

$$\frac{qu}{p} = \left\lfloor \frac{qu}{p} \right\rfloor + \frac{r(u)}{p},$$

q é ímpar e u é par, temos

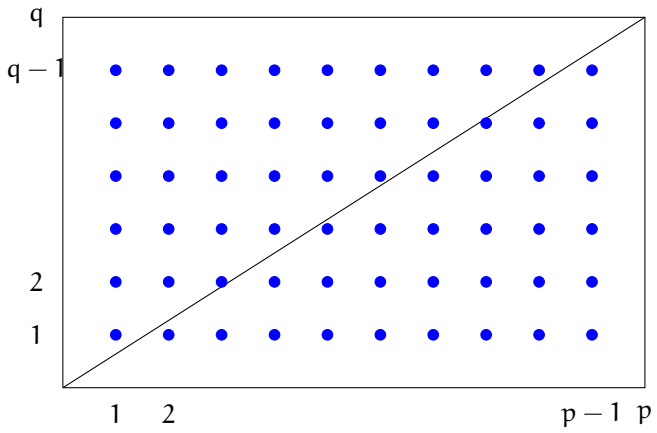
$$\left\lfloor \frac{qu}{p} \right\rfloor \equiv r(u) \pmod 2.$$

Assim,

$$\left(\frac{q}{p}\right) = (-1)^{\sum \left\lfloor \frac{qu}{p} \right\rfloor}. \qquad \square$$

Procedemos agora à demonstração da Lei da Reciprocidade Quadrática.

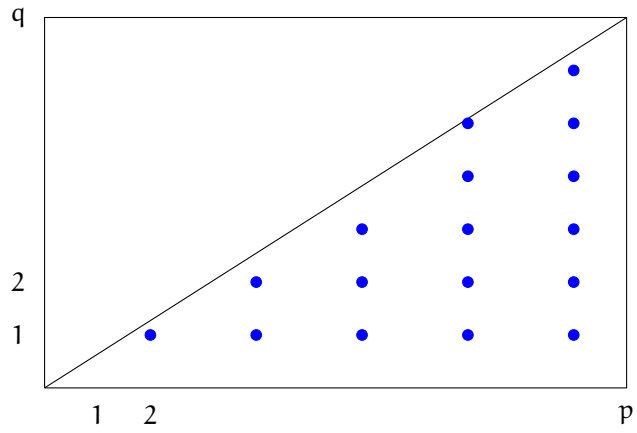
Demonstração. Observamos, no plano Cartesiano, o retângulo delimitado entre a origem e o ponto (p, q). A diagonal é dada pela reta $y = qx/p$.



Inicialmente observamos que:

- cada coluna tem um número par de pontos inteiros (que são os de ordenada $1, 2, \ldots, q-1$).
- não há pontos sobre a diagonal, que é definida pela reta $y = qx/p$, porque sendo p e q primos e $x < p$, qx/p não é inteiro.

Note que a quantidade de pontos nas colunas pares abaixo da diagonal é $\lfloor \frac{2q}{p} \rfloor$, $\lfloor \frac{4q}{p} \rfloor$, ..., $\lfloor \frac{(p-1)q}{p} \rfloor$.

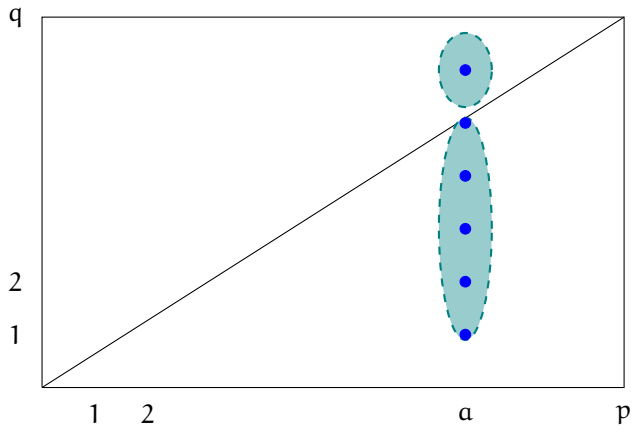


Assim, a soma de pontos nas colunas pares abaixo da diagonal é

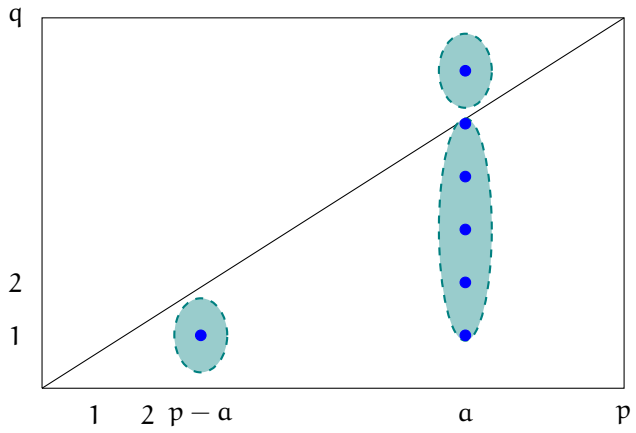
$$d = \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{4q}{p} \right\rfloor + \ldots + \left\lfloor \frac{(p-1)q}{p} \right\rfloor,$$

exatamente o expoente no lema de Eisenstein. Podemos portanto concluir que $(p/q) = (-1)^d$.

Como a quantidade total de pontos em cada coluna é par, a quantidade de pontos *acima* da diagonal, em cada coluna, deve ter a mesma paridade que a quantidade de pontos *abaixo* dela. A próxima figura mostra uma abscissa a e os pontos inteiros de a acima e abaixo da diagonal.



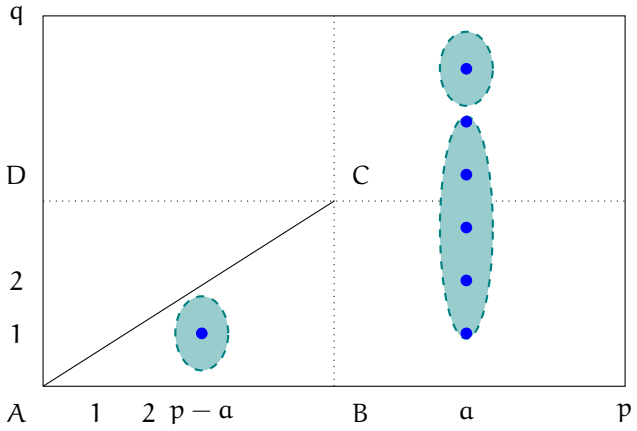
No entanto, a quantidade de pontos *acima* da diagonal na coluna a é a mesma que a quantidade *abaixo* da diagonal na coluna $p-a$. Isto é ilustrado na próxima figura. Note que, como p é ímpar e a é par, $p-a$ é ímpar.



Na figura acima, as três regiões marcadas (três trechos de colunas) tem quantidades de pontos inteiros com a mesma paridade. Observamos tam-

bém que há uma correspondência um-para-um entre a quantidade de pontos na abscissa a acima da diagonal e a quantidade de pontos da abscissa $p-a$, abaixo da diagonal.

A seguir dividimos o retângulo ao meio, na horizontal e na vertical, obtendo um novo retângulo $ABCD$.



A paridade da quantidade total de pontos com abscissa par abaixo da diagonal em $ABCD$ (que chamamos de d) é a mesma que a da quantidade total de pontos no triângulo ABC, que chamamos de α:

$$\sum \left\lfloor \frac{qu}{q} \right\rfloor \equiv \alpha \pmod 2.$$

Para verificar que isto vale, observamos que ao contar as paridades das colunas com abscissa par abaixo da diagonal, contamos as colunas pares dentro de ABC, e também as colunas pares após B – mas para cada uma dessas, há uma coluna ímpar em ABC.

Com este resultado, chegamos de imediato a

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}.$$

Trocando os papéis de 1 e p, e denotando a quantidade de pontos em ABD por β, obtemos também

$$\left(\frac{p}{q}\right) = (-1)^{\beta}.$$

Ou seja,

$$\left(\frac{q}{p}\right) = (-1)^{\alpha+\beta}$$

Mas a soma das quantidades de pontos nos dois triângulos é

$$\alpha + \beta = \frac{(p-1)}{2}\frac{(q-1)}{2},$$

o que nos dá imediatamente a Lei da Reciprocidade Quadrática:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\alpha}(-1)^{\beta} = (-1)^{(p-1)(q-1)/4}. \qquad \square$$

9.2.2 Demonstração de Rousseau

A demonstração a seguir, originalmente dada por G. Rousseau, usa apenas o Teorema de Wilson, o critério de Euler, e o Teorema Chinês dos Restos.

Demonstração. Sejam $p \neq q$ dois primos ímpares, e defina

$$P = \left\{ a \leq x \leq \frac{pq-1}{2} \;\middle|\; \operatorname{mdc}(x, pq) = 1 \right\}.$$

Ao excluir os elementos x com $\operatorname{mdc}(x, pq) > 1$, excluímos os múltiplos de p e de q (ou seja, os zeros módulo p e módulo q).

Este conjunto tem a primeira metade de $\mathbb{Z}_{pq}$, e vemos que

$$\mathbb{Z}_{pq} = P \cup -P.$$

Se $\mathbb{Z}_{pq}$ contém q vezes a sequência $1 \cdots p$ (módulo pq), então P contém metade delas, ou seja, $(q-1)/2$ sequências e mais meia sequência.

Calculamos o produtório de P:

$$\begin{aligned}
\prod_{x \in P} x &\equiv \frac{\left[(p-1)!\right]^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!} && \pmod{p} \\
&\equiv (-1)^{\frac{q-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!} && \pmod{p} && \text{(T. Wilson)} \\
&\equiv (-1)^{\frac{q-1}{2}} \left(q^{\frac{p-1}{2}}\right)^{-1} && \pmod{p} && \text{(simplificando)} \\
&\equiv (-1)^{\frac{q-1}{2}} q^{\frac{p-1}{2}} && \pmod{p} && \text{(inverso de } \pm 1 \text{ é ele mesmo)} \\
&\equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) && \pmod{p} && \text{(crit. Euler)}
\end{aligned}$$

Por simetria, o mesmo ocorre módulo q, e temos os seguintes dois fatos:

$$\begin{aligned}\prod_{x\in P} x &\equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p\\ &\equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q\end{aligned}$$

Não chegamos ainda na afirmativa do enunciado, porque os módulos nas equações são diferentes (p e q). Como mencionamos no início da demonstração, $\mathbb{Z}_{pq} = P \cup -P$. Mas pelo Teorema Chinês dos Restos, a função $\alpha : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$, com $\alpha(x) = (x, x)$, é bijetora.

$$\prod_{x\in P}\alpha(x) \equiv \left((-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right),\ (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right) \pmod{p,q} \tag{9.1}$$

Como α é bijetora, para cada par (a, b) o conjunto $\alpha(P)$ conterá (a, b) e $(-a, -b)$, com $a \in \mathbb{Z}_p$, $b \leq (q-1)/2$. Então

$$\prod_{x\in P}\alpha(x) \equiv \pm\left[(p-1)!^{\frac{q-1}{2}},\ \left(\frac{q-1}{2}\right)!^{p-1}\right] \pmod{(p,q)}$$

e pelo Teorema de Wilson,

$$\prod_{x\in P}\alpha(x) \equiv \pm\left[(-1)^{\frac{q-1}{2}},\ \left(\frac{q-1}{2}\right)!^{p-1}\right] \pmod{(p,q)} \tag{9.2}$$

Mas

$$\begin{aligned}-1 &\equiv (q-1)! && \pmod q\\ &\equiv \left[(1)(2)\cdots(\frac{q-1}{2})\right]\left[(-1)(-2)\cdots(-\frac{q-1}{2})\right] && \pmod q\\ &\equiv (-1)^{\frac{q-1}{2}}\left(\frac{q-1}{2}\right)!^2 && \pmod q\end{aligned}$$

E portanto,

$$\begin{aligned}\left(\frac{q-1}{2}\right)!^{p-1} &\equiv \left[\left(\frac{q-1}{2}\right)!^2\right]^{\frac{p-1}{2}}\\ &\equiv \left[-(-1)^{\frac{q-1}{2}}\right]^{\frac{p-1}{2}}\\ &\equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod q.\end{aligned}$$

Agora reescrevemos 9.2,

$$\prod_{x\in P} \alpha(x) \equiv \pm \left((-1)^{\frac{q-1}{2}},\ (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \right) \tag{9.3}$$

Finalmente, dividimos 9.1 por 9.3, obtendo $(1,1)$:

$$(1,1) \equiv \pm \left[\left(\frac{q}{p}\right),\ (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \right]$$

ou seja,

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right),$$

que é o enunciado da Lei da Reciprocidade Quadrática. □

9.3 Método para resolução de congruências quadráticas

Nos falta um método para determinar as raízes quadradas de a (as soluções para $x^2 \equiv a \pmod p$).

9.3.1 Módulo primo

Quando $p = 4k+3$ é bastante simples resolver equações quadráticas módulo p. Tratamos somente deste caso.

Teorema 9.16. *Seja $p = 4k+3$ primo, a um resíduo quadrático módulo p. Então $x \equiv a^{k+1} \pmod p$ é solução para $x^2 \equiv a \pmod p$.*

Demonstração.

$$\begin{aligned} x^2 &\equiv \left(a^{k+1}\right)^2 \\ &\equiv a^{2k+2} \\ &\equiv a^{2k+1} a \\ &\equiv a^{\frac{p-1}{2}} a && \text{(porque } p = 4k+3\text{)} \\ &\equiv a \pmod p. && \text{(critério de Euler)} \end{aligned}$$

Pudemos usar o critério de Euler no último passo porque já sabemos que a é resíduo quadrático. Assim, uma solução para $x^2 \equiv a \pmod p$ é a classe de congruências $a^{k+1} \pmod p$ – se p for da forma $4k+3$. □

Escolhemos para exemplo o módulo $11 = 4(2)+3$. Pelo critério de Euler,

3 é resíduo quadrático módulo 11:

$$3^{\frac{11-1}{2}} \equiv 3^5 \equiv 243 \equiv 1 \pmod{11}.$$

A raiz quadrada de 3 módulo 11 é

$$3^{k+1} \equiv 3^3 \equiv 27 \equiv 5 \pmod{11}.$$

Verificamos:

$$5^2 \equiv 25 \equiv 3 \pmod{11}. \tag{9.4}$$

9.3.2 Módulo potência de primo

Sabemos calcular as raízes quadradas de um número módulo p primo, mas não módulo potência de primo. O Teorema 9.17 é uma variante do Lema de Hensel (Lema 6.42). Ele nos permite usar as raízes módulo p para determinar as raízes p^k: se $x^2 \equiv a \pmod{p}$, então existe algum y tal que $y^2 \equiv a \pmod{p^k}$.

Teorema 9.17. *Seja p um primo ímpar. Se* $x^2 \equiv a \pmod{p^k}$*, então para qualquer* $m \leq k$*,*

$$y^2 \equiv a \pmod{p^{m+k}},$$

com

$$y = x + tp^k,$$
$$t = -\frac{x^2 - a}{2xp^k} \pmod{p^m}.$$

Exemplificamos a seguir. Sabemos que $(\pm 7)^2 \equiv 4 \pmod{5}$, e como $3 \equiv -7 \pmod{5}$, $3, 7$ são soluções para $x^2 \equiv 4 \pmod{5}$:

$$7^2 \equiv 49 \equiv 4 \pmod{5}$$
$$(-7)^2 \equiv (3)^2 \equiv 9 \equiv 4 \pmod{5}$$

Partindo das soluções $3, 7$ para módulo 5 obteremos soluções para módulo 5^3. Queremos resolver

$$y^2 \equiv 4 \pmod{5^{1+2}},$$

logo

$$y = 3 + t5,$$
$$t \equiv -\frac{3^2 - 4}{2(3)5} \pmod{5^2}.$$

Calculamos t:

$$t \equiv -\frac{5}{6(5)} \equiv -(6)^{-1} \equiv -126 \equiv 24 \pmod{25}.$$

Finalmente, obtemos y (uma raiz quadrada de 4 módulo 5^3):

$$y = 3 + 24(5) = 123.$$

Verificamos que

$$123^2 \equiv 15129 \equiv 4 \pmod{5^3}.$$

9.3.3 Módulo composto

Quando o módulo é composto, podemos usar as soluções módulo p para cada primo p na fatoração do módulo na construção de uma solução.

Lema 9.18. *Se p está na fatoração de m com expoente k (ou seja, $m = \cdots p^k \cdots$), e $x^2 \equiv y \pmod{m}$, então $x^2 \equiv y \pmod{p^k}$.*

Demonstração.

$$\begin{aligned} & x^2 \equiv y \pmod{m} \\ & m \mid x^2 - y \\ & p^k \mid x^2 - y && \text{(porque } p^k | m\text{)} \\ & x^2 \equiv y \pmod{p^k} && \square \end{aligned}$$

Suponha que queiramos resolver $x^2 = y \pmod{pq}$. Calculamos $\pm x \pmod{p}$, $\pm x \pmod{q}$, e depois obtemos as raízes quadradas módulo pq usando o Teorema Chinês dos Restos para resolver quatro sistemas (listados um por linha):

$$\begin{array}{llllll} (1) & x \equiv & r_1 & \pmod{p}, & x \equiv & r_2 \pmod{q} \\ (2) & x \equiv & -r_1 & \pmod{p}, & x \equiv & r_2 \pmod{q} \\ (3) & x \equiv & r_1 & \pmod{p}, & x \equiv & -r_2 \pmod{q} \\ (4) & x \equiv & -r_1 & \pmod{p}, & x \equiv & -r_2 \pmod{q} \end{array}$$

Exemplo 9.19. Sejam $p = 11, q = 19$. Encontraremos as raízes quadradas de 5 módulo $pq = 209$.

Vemos que $11 = 4(2) + 3$, e uma das raízes quadradas é $5^{2+1} \equiv 125 \equiv 4 \pmod{11}$. A outra é $-4 \equiv 7 \pmod{11}$.

Para $19 = 4(4) + 3$, uma solução é $x = 5^5 = 3125 \equiv 9 \pmod{19}$. A outra é $-9 \equiv 10 \pmod{19}$.

Agora resolvemos os quatro sistemas,

$$\begin{array}{lrcrcl}
(1) & x \equiv & 4 & \pmod{11}, & x \equiv & 9 \pmod{19} \\
(2) & x \equiv & 4 & \pmod{11}, & x \equiv & 10 \pmod{19} \\
(3) & x \equiv & 7 & \pmod{11}, & x \equiv & 9 \pmod{19} \\
(4) & x \equiv & 7 & \pmod{11}, & x \equiv & 10 \pmod{19}
\end{array}$$

As soluções são $180, 48, 161$ e 29. ◄

9.3.4 Equação geral do segundo grau

Determinar se a equação de segundo grau $ax^2 + bx + c \equiv 0 \pmod{m}$ tem soluções é equivalente a determinar se a equação $y^2 \equiv \Delta \pmod{m}$, onde $\Delta = b^2 - 4ac$, tem solução, já que

$$\begin{aligned}
x &\equiv \frac{-b \pm \sqrt{\Delta}}{2a} && \pmod{m} \\
2ax + b &\equiv \pm\sqrt{\Delta} && \pmod{m} \\
(2ax + b)^2 &\equiv \Delta && \pmod{m} \\
y^2 &\equiv \Delta && \pmod{m}
\end{aligned}$$

Isto vale desde que $\text{mdc}\,(2a, m) = 1$ (porque usamos a lei do cancelamento, multiplicando os dois lados por $2a$). Quando o módulo é primo, $2a$ será evidentemente co-primo com o módulo.

Resolveremos agora $x^2 - 6x + 5 \equiv 0 \pmod{11}$. Temos

$$\Delta = b^2 - 4ac = 36 - 20 = 16 \equiv 5 \pmod{11}.$$

O critério de Euler nos garante que 5 é resíduo quadrático módulo 11, conforme já calculamos na seção anterior (equação9.4). A raiz de Δ é, portanto,

$$5^{k+1} \equiv 5^3 \equiv 125 \equiv 4 \pmod{11}.$$

Podemos simplesmente calcular

$$\begin{aligned}
(2ax + b)^2 &\equiv \Delta && \pmod{11} \\
2ax + b &\equiv 4 && \pmod{11} \\
2x - 6 &\equiv 4 && \pmod{11} \\
2x &\equiv 10 && \pmod{11} \\
x &\equiv 5 && \pmod{11}
\end{aligned}$$

Por último, fazemos uma verificação:

$$\begin{aligned} x^2 - 6x + 5 &\equiv (5)^2 - 6(5) + 5 && \pmod{11} \\ &\equiv 25 - 30 + 5 && \pmod{11} \\ &\equiv 0 && \pmod{11} \end{aligned}$$

Exercícios

Ex. 202 — Calcule:

$$\left(\frac{21}{11}\right), \quad \left(\frac{31}{3}\right), \quad \left(\frac{122}{23}\right), \quad \left(\frac{119}{7}\right).$$

Ex. 203 — Resolva (deixe potências indicadas, não é necessário reduzir as classes de congruência), ou explique porque não é possível:

$$\begin{aligned} x^2 &\equiv 10 && \pmod{43} \\ X^2 &\equiv 5 && \pmod{31} \\ 3x^2 - x + 1 &\equiv 0 && \pmod{19} \\ x^2 - x + 4 &\equiv 0 && \pmod{29} \\ 2x^2 - 10 &\equiv 0 && \pmod{23} \\ 3x^2 - 5 &\equiv 0 && \pmod{18} \\ 4x^2 - 5 &\equiv 0 && \pmod{25} \end{aligned}$$

Ex. 204 — Prove que quando m é ímpar,

$$\left(\frac{a}{m}\right)\left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right).$$

Ex. 205 — Um resíduo quadrático módulo p pode ser raiz primitiva módulo pq, com p e q primos?

Ex. 206 — Seja p primo da forma $4k + 1$. Determine a soma dos resíduos quadráticos módulo p contidos em $[1, p)$.

Ex. 207 — Quantos resíduos quadráticos existem módulo m, onde $m = pq$, com p, q primos?

Ex. 208 — Prove que se p e q são primos ímpares tais que existe um x

inteiro positivo tal que $p = q + 4x$, então

$$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right).$$

Ex. 209 — Prove que todo primo p maior que 3 divide a soma de seus resíduos quadráticos; e que todo primo p maior que 5 divide a soma dos quadrados de seus resíduos quadráticos.

Ex. 210 — Prove que

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{se } p = 4k+1 \\ -1 & \text{se } p = 4k+3 \end{cases}$$

Ex. 211 — Prove que há infinitos primos da forma $5k-1$.

Ex. 212 — Mostre que $|Q_n| = \phi(n)/R$, onde R é a quantidade de elementos em U_n tais que $x^2 = a$, sendo a um resíduo quadrático em U_n.

Ex. 213 — Prove que se n é um inteiro ímpar livre de quadrados, então existe $k \in \mathbb{Z}$ tal que $\text{mdc}(k, n) = 1$ e $\left(\frac{k}{n}\right) = -1$.

Ex. 214 — Demonstre o Teorema 9.5.

Ex. 215 — Prove que a função $f : U_n \to Q_n$, tal que $f(x) = x^2$ é homomorfismo entre grupos.

Ex. 216 — Prove que se p é um primo ímpar e $a \neq 0$ um resíduo quadrático módulo p, então $-a$ é resíduo quadrático módulo p se e somente se $p = 4k+1$. (Use o resultado do Exercício 210).

Ex. 217 — Seja $m = pq$, com p e q primos ímpares. Se sortearmos um elemento $x \in \mathbb{Z}_m$, e verificarmos que seu símbolo de Jacobi é $+1$, qual é a probabilidade de x ser resíduo quadrático módulo m?

Ex. 218 — Prove a seguinte extensão do Teorema de Wilson: se p é primo e $p \nmid a$, então

$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \pmod{p}.$$

Ex. 219 — Prove que para n ímpar,

$$\left(\frac{-1}{c}\right) = (-1)^{(c-1)/2}$$

Ex. 220 — Determine uma forma fechada para

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right),$$

quando a, b são inteiros ímpares.

Ex. 221 — Seja p um primo ímpar, e n o menor resíduo quadrático positivo módulo p. Prove que $n < 1 + \sqrt{p}$.

Ex. 222 — Determine quais os primos p tais que 3 é resíduo quadrático módulo p.

Ex. 223 — Prove o Lema de Gauss: seja p primo e a coprimo com p; considere o conjunto $A = \{a, 2a, 3a, \ldots, [(p-1)/2]a\}$. Tome os menores representantes positivos dos elementos em A, módulo p. Seja n a quantidade desses $\mathrm{LR}_p(a_i)$ que são maiores que $p/2$:

$$n = \left| \left\{ x \in A \ : \ \mathrm{LR}_p(X) > \frac{p}{2} \right\} \right|.$$

Então

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Ex. 224 — Prove a Lei da Reciprocidade Quadrática usando o Lema de Gauss. **Não** use o argumento de contagem de pontos inteiros, como na demonstração de Eisenstein.

Ex. 225 — Prove a Lei da Reciprocidade Quadrática por indução (esta foi a primeira prova elaborada por Gauss).

a) Comece provando o Lema a seguir:

Lema 9.20. *Seja q um primo da forma $4k+1$. Então existe um primo ímpar p tal que*

$$\left(\frac{q}{p}\right) = -1.$$

b) Seja $p' = (-1)^{(p-1)/2}p$. Suponha que $p < q$. Faça indução em q, e separe em três casos:

i) $(p'/q) = +1$. Prove que $(q/p) = +1$.

ii) $(p'/q) = -1, q = 4k+3$. Prove que $(q/p) = -1$.

iii) $(p'/q) = -1, q = 4k+1$. Prove que $(q/p) = -1$.

Parte II

Capítulo 10

Soma de Quadrados

Abordamos aqui a representação de inteiros como soma de dois quadrados, ou seja, dado um inteiro n, estudamos a equação Diofantina não linear

$$a^2 + b^2 = n,$$

tentando determinar quantas soluções tem (se existem), e quais são. Mostramos também que todo inteiro pode ser representado como soma de quatro quadrados.

10.1 Existência de representação como soma de dois quadrados

Começamos identificando quais inteiros podem ser escritos como soma de dois quadrados, e quais deles pode ser escritos como soma de dois quadrados $x^2 + y^2$, com $\text{mdc}(x, y) = 1$.

Definição 10.1 (representação de inteiro como soma de quadrados)**.** Seja n um inteiro positivo. Dizemos que o par de inteiros positivos (x, y) é uma **representação** de n como soma de dois quadrados se $x^2 + y^2 = n$.

Se $\text{mdc}(x, y) = 1$, dizemos que se trata de uma representação *própria* de n. ♦

Por exemplo, 109 tem representação própria como soma de dois quadrados, já que $109 = 3^2 + 10^2$ e $\text{mdc}(3, 10) = 1$.

Já 117 tem representação, mas não própria, porque $117 = 3^2(13)$, e $\text{mdc}(6, 9) = 3$. A representação, imprópria, é $117 = 6^2 + 9^2$.

Começamos demonstrando um Lema.

Lema 10.2. -1 *sempre é resíduo quadrático módulo* p *quando* p *é um primo da forma* $4k + 1$.

Demonstração. A congruência, da forma como está escrita, já nos indica que o Teorema de Wilson pode ser usado: sabemos que $(p-1)! \equiv -1 \pmod{p}$. Agora,

$$\frac{p+1}{2} \leq x \leq p-1 \text{ se e somente se } -\frac{p-1}{2} \leq x-p \leq -1.$$

Portanto,

$$\begin{aligned}
(p-1)! &\equiv \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right) \overbrace{\left(\frac{p+1}{2} \cdot \frac{p+3}{2} \ldots (p-1)\right)}^{\text{cada um } \equiv -1,-2,\ldots,-(p-1)/2 \pmod{p}} && \pmod{p} \\
&\equiv (-1)^{(p-1)/2}\, 1^2\, 2^2\, 3^2 \cdots \left(\frac{p-1}{2}\right)^2 && \pmod{p} \\
&\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 && \pmod{p} \\
&\equiv -1 && \pmod{p},
\end{aligned}$$

e -1 é resíduo quadrático módulo p. □

Tratamos primeiro de caracterizar quando há representação própria para um inteiro. Depois trataremos do caso impróprio.

Teorema 10.3. *Um inteiro positivo n tem representação própria se e somente se não tem fatores da forma $4k+3$.*

Demonstração. Seja p um primo na fatoração de n (ou seja, $p|n$), e suponha que n tem representação própria: $n = x^2 + y^2$ e $\operatorname{mdc}(x,y) = 1$. Então p não pode dividir nem x nem y.

Deve portanto existir algum inteiro u tal que $y \equiv ux \pmod{p}$, e

$$\begin{aligned}
x^2 + y^2 &\equiv x^2 + u^2x^2 && \pmod{p} \\
&\equiv x^2(1+u^2) && \pmod{p} \\
&\equiv 0 && \pmod{p}. \qquad (p|n)
\end{aligned}$$

Mas $x > 0$, e $p \nmid x$, logo $x^2(1+u^2) \equiv 0 \pmod{p}$ só é possível se $(1+u^2) \equiv 0 \pmod{p}$, e

$$u^2 \equiv -1 \pmod{p}.$$

Então -1 é resíduo quadrático módulo p, e portanto p deve ser 2 ou algum primo da forma $4k+1$. □

Teorema 10.4. *Um inteiro positivo n é representável como soma de dois quadrados se e somente se sua fatoração em primos não contém potências ímpares de primos da forma $4k+3$.*

Como exemplo, o número $275 = (11)5^2$ contém uma potência ímpar de 11, que é da forma $4k+3$, por isso não pode ser representado como soma de dois quadrados.

Demonstração. ($\Rightarrow$) Seja p um primo da forma $4k+3$, e suponha que $p \mid n$, e que $2r+1$ é a ordem de p na fatoração de n. Suponha também que $n = x^2 + y^2$, com $x, y \in \mathbb{N}^*$, com $\operatorname{mdc}(x,y) = d$. Como $p \mid n$, então alguma potência de p divide d.

Então dividimos x e y por d e escrevemos

$$\begin{aligned} x/d = x' \quad &\Rightarrow \quad x = dx' \\ y/d = y' \quad &\Rightarrow \quad y = dy' \end{aligned}$$

Sabemos que $\operatorname{mdc}(x', y') = 1$. Agora, seja

$$\begin{aligned} m &= (x')^2 + (y')^2 \\ &= \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2. \end{aligned}$$

Assim, m é um inteiro com representação própria. Mas

$$\begin{aligned} p^{2r+1} &\mid n \\ p^{2r+1} &\mid x^2 + y^2 \\ p^{2r+1-2j} &\mid (x')^2 + (y')^2 \qquad \text{(divida por } d^2\text{)} \end{aligned}$$

Isto contradiz o Teorema 10.3, porque m será um inteiro com representação própria, e com $p = 4k+3$ em sua fatoração.

($\Leftarrow$) Agora mostramos que, se na fatoração de um inteiro n os primos da forma $4k+3$ só aparecem com expoentes pares, então n tem representação como soma de quadrados. Assim, presumimos que

$$n = ab^2,$$

onde a é livre de quadrados e não tem fatores primos da forma $4k+3$. Nos basta provar que a é representável, porque b^2 evidentemente é, e o produto de inteiros representáveis é, também, representável:

$$(a^2 + b^2)(\alpha^2 + \beta^2) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2.$$

Agora, a é produto de primos da forma $4k+1$. Precisamos somente mostrar que todo primo desta forma é representável. Mas pelo Lema 10.2, a congruência $x^2 \equiv -1 \pmod{p}$ tem solução, e a é representável como soma de quadrados. Mas se a é representável, n também é. $\square$

10.2 Quantidade de representações

Tendo estabelecido quando existe representação para um inteiro como soma de dois quadrados, tratamos agora de calcular a quantidade de representações de cada inteiro.

Definição 10.5. $R(n)$ é a quantidade de representações de n;
$r(n)$ é a quantidade de representações próprias de n;
$P(n)$ é a quantidade de representações próprias de n com $x > 0$;
$N(n)$ é a quantidade de soluções da congruência $a^2 \equiv -1 \pmod{n}$. ♦

Teorema 10.6. $\forall n > 0, \quad r(n) = 4N(n)$.

Demonstração. Provamos o caso $n = 1$ separadamente. Todo número é congruente a zero módulo um, já que a divisão por um nunca deixa resto. Assim, a equação $u^2 \equiv -1 \pmod{1}$ tem uma única solução (a única classe de congruências módulo um, representada pelo zero). O número de representações de um é, portanto, quatro. De fato,

$$\begin{aligned} 1 &= (+1)^2 + 0^2 \\ &= (-1)^2 + 0^2 \\ &= \quad 0^2 \ + (+1)^2 \\ &= \quad 0^2 \ + (-1)^2 \end{aligned}$$

Estas representações são próprias, porque $\operatorname{mdc}(0, \pm 1) = 1$.

Quando $n > 1$ e $n = x^2 + y^2$, vemos que necessariamente tanto x como y devem ser diferentes de zero, porque tratamos de representações próprias, e necessitamos que $\operatorname{mdc}(x, y) = 1$.

Como x e y são diferentes de zero, o número total de representações é igual a quatro vezes o número de representações positivas (para contabilizarmos as quatro possibilidades de sinais para x e y). Só precisamos agora mostrar que a quantidade de soluções de $u^2 \equiv -1 \pmod{n}$ é igual à quantidade de representações positivas de n.

Suponha que $n = x^2 + y^2$, com $x, y > 0$ e $\operatorname{mdc}(x, y) = 1$. Então $\operatorname{mdc}(x, n) = 1$. Mas isso implica que a equação $y \equiv ux \pmod{n}$ tem uma única solução. Podemos substituir y por ux, como a seguir.

$$\begin{aligned} x^2 + y^2 &\equiv x^2 + (ux)^2 && \pmod{n} \\ &\equiv x^2(u+1)^2 && \pmod{n} \\ &\equiv 0 && \pmod{n} \end{aligned}$$

Mas como $x^2 > 0$, é necessário que $(u+1)^2 \equiv 0 \pmod{n}$, e $u^2 \equiv -1 \pmod{n}$.

Agora, para cada u com $u^2 \equiv -1 \pmod{n}$, se tomarmos $y \equiv ux \pmod{n}$, teremos

$$\begin{aligned} y &\equiv ux && \pmod{n} \\ y^2 &\equiv u^2x^2 && \pmod{n} \\ y^2 &\equiv -x^2 && \pmod{n} \\ x^2 + y^2 &\equiv 0 && \pmod{n} \end{aligned}$$

E temos exatamente uma representação positiva para u. □

Teorema 10.7. *Para todo inteiro* $n > 0$,

$$R(n) = \sum_{d^2 | n} r\left(\frac{n}{d^2}\right)$$

Demonstração. Suponha que n é representado por x e y, e $\operatorname{mdc}(x, y) = d$. Dividimos a equação $x^2 + y^2 = n$ por d^2, e obtemos

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{n}{d^2}.$$

Isto nos dá uma representação própria de n/d^2, porque $\operatorname{mdc}(x/d. y/d) = 1$.

Agora suponha que u, w sejam representação própria de n/d^2, então

$$(ud)^2 + (wd)^2 = n$$

é representação de n, com $\operatorname{mdc}(ud, wd) = d$.

Mostramos que há uma correspondência um-para-um entre as representações de n e as representações próprias de n/d^2, como no enunciado. □

Lema 10.8. $N(n) = 2^{s+1}$, *onde* s *é a quantidade de primos distintos da forma* $4k + 1$ *que dividem* n.

Demonstração.

$$N(n) = N\left(s^h\right) \prod_i N\left(p^i\right) \prod_j N\left(q^j\right)$$

$$\begin{aligned} N(2) &= 1 \\ N(4) &= 0 \\ N(t) &= 0 \quad t > 4 \end{aligned}$$

Para os primos da forma $4k + 3$,

$$N(q^j) = 0, \quad j > 0$$

Mas para os da forma $4k+1$,

$$N(p) = 2$$

Pelo Lema de Hensel,

$$N(p^i) = 2, \;\; i > 0$$

Assim,

$$N(n) = 2^s$$

onde s é a quantidade de primos distintos da forma $4k+1$. □

Teorema 10.9. *Seja n um número tendo representação própria como soma de dois quadrados, e s a quantidade de primos da forma $4k+1$ que dividem n. Então $r(n) = 2^{s+2}$.*

Demonstração. Pelo Lema 10.8 e o Teorema 10.6,

$$r(n) = 4N(n) = (2^2)(2^s) = 2^{s+1}.$$ □

Teorema 10.10. *Seja n um número representável como soma de dois quadrados:*

$$n = 2^h \prod_p p^i \prod_q q^j,$$

onde os primos p são da foram $4k+1$ e os primos q são da forma $4k+3$.

Então $R(n) = 4\prod_p (j+1)$.

Demonstração.

$$\sum_{d^2|n} N\left(\frac{n}{d^2}\right) = \left(\sum_{c_i|a} N\left(\frac{a}{c_i^2}\right)\right)\left(\sum_{e_j|b} N\left(\frac{b}{e_j^2}\right)\right)$$

$$\sum_{d^2|n} N\left(\frac{n}{d^2}\right) = \left(\underbrace{\sum_{d^2|2^k} N\left(\frac{2^k}{d^2}\right)}_{(i)}\right) \prod_p \left(\underbrace{\sum_{d^2|p^i} N\left(\frac{p^i}{d^2}\right)}_{(ii)}\right) \prod_q \left(\underbrace{\sum_{d^2|b^j} N\left(\frac{q^j}{d^2}\right)}_{(iii)}\right)$$

(i) Se k é par, $d = 2^{k/2}$. Se k é ímpar, $d = 2^{k-1}/2$. O valor será 1;

(ii) Se i é par, $N(p^i/d^2) = 2$, para $(p/2)$ valores: $d \in \{1, p, p^2, \cdots p^{i/2-1}\}$. Se i é ímpar, $N(p^i/d^2) = 2$ para $d \in \{1, p, p^2, \cdots p^{(i-1)/2}\}$ – ou seja, o somatório resulta em $i+1$ de qualquer forma.

(iii) Quando j é par, q divide todos os q^j/d^2, e este termo desaparece. Quando j é ímpar, então o termo com $d = q^{(i/2)}$ é um, e os outros somem.

Logo, $R(n) = 4\prod_p (i+1)$. □

10.3 Soma de quatro quadrados

Lagrange demonstrou em 1770 que sempre é possível representar um inteiro positivo como soma de quatro quadrados (e portanto como soma de k quadrados, para qualquer $k \geq 4$).

Teorema 10.11. *Seja p primo. Então existem x, y, z inteiros, pelo menos um deles diferente de zero, tais que*

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p}.$$

Demonstração. Trataremos separadamente três casos: $p = 2$, $p = 4k+1$, e $p = 4k+3$.

Para $p = 2$, temos $x = y = 1$ como solução (com $z = 0$).

Para $p = 4k+1$, escolhemos $y = 1$, $z = 0$, e obtemos x resolvendo a congruência $x^2 \equiv -1 \pmod{p}$.

Para $p = 4k+3$, determinamos $z = 1$, e resolvemos a congruência: $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Seja d o menor número positivo que não é resíduo quadrático módulo p. Então temos

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = (-1)(-1) = +1.$$

Portanto $-d$ é resíduo quadrático modulo p, e $d \geq 2$, porque d não é resíduo quadrático. Escolhemos y tal que $y^2 \equiv -d \pmod{p}$.

Sabemos que $d \geq 2$, e também que d é o menor resíduo não-quadrático módulo p, logo $d-1$ deve ser resíduo quadrático módulo p. e x Assim, escolhemos x tal que $x^2 \equiv d-1 \pmod{p}$.

Temos portanto

$$\begin{aligned} x^2 + y^2 + z^2 &\equiv (d-1) + (-d) + 1 && \pmod{p} \\ &\equiv 0 && \pmod{p}. \end{aligned}$$

□

Da demonstração extraímos o Corolário 10.12.

Corolário 10.12. *Para todo p primo, existem u, v, tais que $u^2 + v^2 \equiv -1 \pmod{p}$.*

O Lema 10.13, de fácil verificação, será útil na demonstração do Teorema dos quatro quadrados.

Lema 10.13. *Sejam α, β inteiros Gaussianos tais que $\alpha \equiv \beta \pmod{p}$. Então $\alpha\overline{\alpha} \equiv \beta\overline{\beta} \pmod{p}$.*

Teorema 10.14 (de Lagrange)**.** *Todo inteiro é representável como soma de quatro quadrados.*

Demonstração. Como o produto de números representáveis por quatro quadrados é representável, só precisamos mostrar que primos são representáveis.

Quando $p = 2$ e $p = 3$ o Teorema é trivialmente válido. Suponha, portanto, que $p > 3$.

Sejam u, v tais que $u^2 + v^2 \equiv -1 \pmod{p}$ (cuja existência é garantida pelo Corolário 10.12), e $k = \lfloor \sqrt{p} \rfloor$.

O conjunto de inteiros Gaussianos

$$\{(a + bi) - (c + di)(u + vi) \ : \ a, b, c, d \in [0, k] \cap \mathbb{Z}\}$$

tem $(k + 1)^4$ elementos. Como $(k + 1)^4 > p^2$, pelo princípio da casa dos pombos deve haver pelo menos dois destes números que são congruentes módulo p. Sejam eles $(a_1 + b_1 i) - (c_1 + d_1 i)(u + vi)$ e $(a_2 + b_2 i) - (c_2 + d_2 i)(u + vi)$. Agora, definimos

$$\begin{aligned} A &= a_1 - a_2 \\ B &= b_1 - b_2 \\ C &= c_1 - c_2 \\ D &= d_1 - d_2. \end{aligned}$$

Sabemos que

$$|A|, |B|, |C|, |D| \leq k,$$

porque $a, b, c, d \leq k$. Além disso, nem todos são zero.

Tomamos A, B, C, D e escrevemos

$$\begin{aligned} A + Bi &\equiv (C + Di)(u + vi) \pmod{p} \\ A^2 + B^2 &\equiv (C^2 + D^2)(u^2 + v^2) \pmod{p} && \text{(Lema 10.13)} \\ A^2 + B^2 &\equiv -C^2 - D^2 \pmod{p} && (u^2 + v^2 \equiv -1) \\ A^2 + B^2 + C^2 + D^2 &\equiv 0 \pmod{p}. \end{aligned}$$

Então, $p | Z = A^2 + B^2 + C^2 + D^2$. Seja

$$Z \leq 4k^2 \leq 4p$$

Necessariamente, $Z = tp$, onde t pode ser 1, 2 ou 3.

Se $t = 1$,

$$p = A^2 + B^2 + C^2 + D^2,$$

como no enunciado.

Quando $t = 2$,

$$2p = A^2 + B^2 + C^2 + D^2.$$

Nesta situação há três possibilidades para a paridade dos números A, B, C, D: todos pares; todos ímpares; ou dois pares e dois ímpares. De qualquer forma, presumiremos, sem perda de generalidade, que A e B tem a mesma paridade; e que C e D tem a mesma paridade (não necessariamente a mesma que A e B). Assim, temos

$$A \pm B \text{ é par}$$
$$C \pm D \text{ é par}$$

Então

$$\begin{aligned} 2p &= A^2 + B^2 + C^2 + D^2 \\ p &= \frac{A^2}{2} + \frac{B^2}{2} + \frac{C^2}{2} + \frac{D^2}{2} \\ &= \left(\frac{A+B}{2}\right)^2 + \left(\frac{A-B}{2}\right)^2 + \left(\frac{C+D}{2}\right)^2 + \left(\frac{C-D}{2}\right)^2. \end{aligned}$$

Como as somas nos numeradores são pares, as frações acima são todas inteiras, e p é representável como soma de quatro quadrados.

Finalmente, quando $t = 3$,

$$3p = A^2 + B^2 + C^2 + D^2.$$

Para qualquer inteiro k, temos que $k^2 \equiv 0 \pmod 3$ ou $k^2 \equiv 1 \pmod 3$, porque quadrados não podem deixar resto 2 quando divididos por 3. Trataremos agora os dois casos:

i) todos os quadrados na fórmula acima são divisíveis por 3;

ii) três deles deixam resto um, e o outro é divisível por 3: $a^2, b^2, c^2 \equiv 1 \pmod 3$, mas $d^2 \equiv 0 \pmod 3$.

No caso (i), como a^2, b^2, c^2, d^2 são quadrados divisíveis por 3, são também divisíveis por nove.

$$\begin{aligned} 3p &= A^2 + B^2 + C^2 + D^2 \\ 3p &= 9A' + 9B' + 9C' + 9D' \\ p &= \frac{9A'}{3} + \frac{9B'}{3} + \frac{9C'}{3} + \frac{9D'}{3} \\ p &= 3A' + 3B' + 3C' + 3D' \\ p &= 3w, \end{aligned}$$

mas p é primo, e $p > 3$, logo não pode ser múltiplo de 3.

Observamos o caso (ii). Suponha, sem perda de generalidade, que $A^2, B^2, C^2 \equiv 1 \pmod 3$, e $D^2 \equiv 0 \pmod 3$. Então

$$\begin{aligned} A &\equiv \pm 1 \pmod 3 \\ D &\equiv 0 \pmod 3. \end{aligned}$$

No entanto, podemos trocar A por $-A$ se necessário (porque será elevado ao quadrado), e dizer que $A \equiv +1 \pmod 3$.

$$\begin{aligned} n_1 &= A + B + C \\ n_2 &= A - B + D \\ n_3 &= -A + C + D \\ n_4 &= B - C + D \end{aligned}$$

$$\begin{aligned} n_1^2 + n_2^2 + n_3^2 + n_4^2 &= (A + B + C)^2 + (A - B + D)^2 + (-A + C + D)^2 + (B - C + D)^2 \\ &= 3(A^2 + B^2 + C^2 + D^2) \\ &= 9p \end{aligned}$$

Logo,

$$p = \left(\frac{n_1}{3}\right)^2 + \left(\frac{n_2}{3}\right)^2 + \left(\frac{n_3}{3}\right)^2 + \left(\frac{n_4}{3}\right)^2,$$

e completamos a demonstração. □

10.4 Soma de três quadrados

O problema da representação de inteiros como soma de três quadrados é bem mais difícil, em parte porque para três quadrados não podemos contar com uma regra de composição que vale para dois e para quatro quadrados: enquanto 3 e 5 são representáveis como soma de três quadrados ($3 = 1 + 1 + 1$; $5 = 4 + 1 + 0$), 15 não é.

Enunciamos o Teorema que dá as condições para que um inteiro seja representável como soma de três quadrados, mas apresentamos a demonstração de apeans uma direção do "se e somente se".

Teorema 10.15 (de Legendre)**.** *Um inteiro positivo é representável como soma de três quadrados se e somente se não é da forma* $4^m(8k + 7)$.

Demonstração. (*apenas o "somente se")* Todo quadrado é congruente a $0, 1$ ou 4 módulo 8.

Assim, a soma de três quadrados só pode ser congruente a $0, 1, 2, 3, 4, 5$ ou 6 módulo oito (ou seja, qualquer dos possíveis restos, exceto sete). Nenhum número da forma $8k + 7$ (ou seja, nenhum número $x \equiv 7 \pmod 8$), portanto, é representável.

Se $4 \mid n$ e n é soma de três quadrados, $n = x^2 + y^2 + z^2$, então x, y, z devem ser pares de forma que se possa dividir seus quadrados por 4. Mas isso significa que $n/4$ também deveria ser soma de quadrados. Logo, se n é soma de quadrados, não pode ser quatro vezes um número que não é representável. □

Exercícios

Ex. 226 — Prove que se p é um primo da forma $4k + 1$ então p pode ser representado *unicamente* (a não ser por ordem e sinal) como soma de dois quadrados.

Ex. 227 — Quantas triplas existem de inteiros consecutivos, todos os três representáveis como soma de dois quadrados?

Ex. 228 — Prove que todo inteiro positivo pode ser representável como a soma de no máximo três números triangulares. (Use o teorema dos três quadrados, de Legendre)

Ex. 229 — Prove que se n é representável como soma de dois quadrados de racionais ($n = (a/b)^2 + (c/d)^2$), então n também é representável como soma de dois quadrados de inteiros.

Ex. 230 — Como corolário do exercício 229, mostre que um racional m/n é soma de quadrados de dois racionais se e somente se mn é soma de dois quadrados de inteiros.

Ex. 231 — Verifique o Corolário 10.12 e o Lema 10.13.

Ex. 232 — Prove que, *como consequência direta do Teorema de Legendre*, todo inteiro é a soma de quatro quadrados (não use o Teorema 10.11 nem o caminho usado na demonstração de Lagrange. Só é necessário mostrar que todo inteiro *da forma* $4^a(8k + 7)$ é representável).

Ex. 233 — Prove o Teorema dos quatro quadrados de Lagrange, desta vez usando o seguinte argumento. Primeiro, defina

$$A = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

e considere o reticulado gerado por A em $\mathbb{R}^4$. Considere a bola em $\mathbb{R}^4$ com pontos $\mathbf{x} = (x_1, x_2, x_3, x_4)$ tais que $x_1^2 + x_2^2 + x_3^3 + x_4^4 < 2p$. Observe o volume da bola, e argumente que existe algum ponto *do reticulado* tal que $x_1^2 + x_2^2 + x_3^3 + x_4^4 = p$.

Ex. 234 — As funções aritméticas definidas neste Capítulo são aditivas? Multiplicativas?

Ex. 235 — Seja $r_k(n)$ a quantidade de representações de n como soma de k quadrados. r_k é aditiva? Multiplicativa?

Capítulo 11

Formas Quadráticas Binárias

O Capítulo 10 trata da representações de inteiros como soma de dois, três ou quatro quadrados. Passamos agora à generalização dessa idéia para a representação de inteiros por *formas quadráticas binárias*, $ax^2 + bxy + cy^2$.

Uma forma quadrática é uma soma da forma

$$f(x_1, x_2, \ldots, x_n) \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

e uma forma quadrática é binária quando é definida para duas variáveis, quando escrevemos

$$f(x, y) = ax^2 + bxy + cy^2.$$

Definimos, antes de formas quadráticas, as formas bilineares.

11.1 Formas Bilineares e Quadráticas

Definição 11.1 (forma bilinear)**.** Uma **forma bilinear** em um espaço vetorial V de dimensão finita sobre um corpo K é uma função $f : V \times V \to K$ que é linear em cada um deseus argumentos, ou seja, para todos $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ e $\lambda \in K$,

$$\begin{aligned} f(\mathbf{v} + \lambda\mathbf{u}, \mathbf{w}) &= f(\mathbf{v}, \mathbf{w}) + \lambda f(\mathbf{u}, \mathbf{w}) \\ f(\mathbf{v}, \mathbf{u} + \lambda\mathbf{w}) &= f(\mathbf{v}, \mathbf{u}) + \lambda f(\mathbf{v} + \mathbf{w}). \end{aligned}$$ ♦

Definição 11.2 (matriz de uma forma bilinear)**.** Seja f uma forma bilinear em um espaço vetorial V com base $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$. Então a **matriz da**

forma f é a matriz de Gram[1] $m_{ij} = f(\mathbf{b_i}, \mathbf{b_j})$:

$$M = \begin{pmatrix} f(\mathbf{b_1}, \mathbf{b_1}) & f(\mathbf{b_1}, \mathbf{b_2}) & \dots & f(\mathbf{b_1}, \mathbf{b_n}) \\ f(\mathbf{b_2}, \mathbf{b_1}) & f(\mathbf{b_2}, \mathbf{b_2}) & \dots & f(\mathbf{b_2}, \mathbf{b_n}) \\ \vdots & & \ddots & \vdots \\ f(\mathbf{b_n}, \mathbf{b_1}) & f(\mathbf{b_n}, \mathbf{b_2}) & \cdots & f(\mathbf{b_n}, \mathbf{b_n}) \end{pmatrix}. \qquad \blacklozenge$$

Teorema 11.3. *Toda forma bilinear é determinada por sua matriz. Se a matriz de f é F, então*

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T F \mathbf{y}.$$

Para demonstrar o Teorema 11.3 basta desenvolver $f(\mathbf{x}, \mathbf{y})$ em somatórios representando $\mathbf{x}$ e $\mathbf{y}$ como combinações lineares da base do espaço, e chega-se a $f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T F \mathbf{y}$.

Definição 11.4 (forma bilinear simétrica)**.** Uma forma bilinear f é **simétrica** se $f(\mathbf{x}, \mathbf{y}) = f(\mathbf{y}, \mathbf{x})$. $\blacklozenge$

Proposição 11.5. *Uma forma bilinear é simétrica se e somente se sua matriz é simétrica.*

Demonstração. A matriz da forma é simétrica se e somente se $f(\mathbf{b_i}, \mathbf{b_j}) = f(\mathbf{b_j}, \mathbf{b_i})$. $\square$

Definição 11.6 (forma quadrática)**.** Seja V um espaço vetorial de dimensão finita n. A **forma quadrática** associada a uma forma bilinear $f : V \times V \to K$ é $q(\mathbf{x}) = f(\mathbf{x}, \mathbf{x})$.

n é o **grau** da forma quadrática. Quando $n = 2$ a forma é chamada de **forma quadrática binária**, e usualmente escrevemos

$$q(x, y) = ax^2 + bxy + cy^2.$$

Tratamos somente de formas quadráticas com coeficientes em $\mathbb{Z}$.

Uma forma quadrática é **primitiva** se o polinômio que ela define é primitivo (ou seja, se o MDC de seus coeficientes é um). $\blacklozenge$

Exemplo 11.7. A forma quadrática $3x_1^2 - x_2^2 + x_3^2 - 2x_1x_2 + x_2x_3$ é representada pela matriz

$$\begin{pmatrix} 3 & -1 & 0 \\ -1 & -1 & 1/2 \\ 0 & 1/2 & 1 \end{pmatrix},$$

[1] A matriz de Gram de n vetores é usualmente definida como a matriz onde o elemento na posição i, j é o produto interno do i-ésimo com o j-ésimo vetor. Uma forma bilinear pode não ser produto interno, porque $f(\mathbf{v}, \mathbf{v})$ pode ser negativo, e porque $f(v, w)$ pode ser diferente de $f(w, v)$, mas ainda assim usamos o nome "matriz de Gram".

porque

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 3 & -1 & 0 \\ -1 & -1 & 1/2 \\ 0 & 1/2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 3x_1^2 - x_2^2 + x_3^2 - 2x_1x_2 + x_2x_3. \quad \blacktriangleleft$$

A forma quadrática binária $ax^2 + bxy + cy^2$ é representada pela matriz

$$Q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

O Teorema 11.8 define uma bijeção entre formas bilinearese e formas quadráticas.

Teorema 11.8. *Seja* q *uma forma quadrática em um espaço vetorial* V*, tal que* $q(\mathbf{x}) = f(\mathbf{x}, \mathbf{x})$*, onde* f *é uma forma bilinear.*

Se $1 + 1 \neq 0$ *no corpo subjacente*[2] *a* V*, então a forma bilinear* f *é única.*

Demonstração. Sejam $\mathbf{v}, \mathbf{w} \in V$. Então

$$\begin{aligned} q(\mathbf{v} + \mathbf{w}) &= f(\mathbf{v} + \mathbf{w}, \mathbf{v} + \mathbf{w}) \\ &= f(\mathbf{v}, \mathbf{v}) + 2f(\mathbf{v}, \mathbf{w}) + f(\mathbf{w}, \mathbf{w}) \\ &= q(\mathbf{v}) + q(\mathbf{w}) + 2f(\mathbf{v}, \mathbf{w}) \end{aligned}$$

e

$$f(\mathbf{v}, \mathbf{w}) = \frac{q(\mathbf{v} + \mathbf{w}) - q(\mathbf{v}) - q(\mathbf{w})}{2},$$

definida unicamente. □

Definição 11.9. O **determinante** de uma forma quadrática é o determinante de sua matriz. ♦

Exemplo 11.10. A forma quadrática $3x^2 - 2xy - 2y^2$ tem matriz associada

$$\begin{pmatrix} 3 & -1 \\ -1 & -2 \end{pmatrix},$$

cujo determinante é -7; dizemos que o determinante da forma $3x^2 - 2xy - 2y^2$ é -7. ◀

Uma forma quadrática pode assumir valores maiores, menores ou iguais a zero; quando a forma é definida em duas variáveis, visualizamos que algumas formas (as que tem discriminante $\Delta < 0$) nunca cruzam o plano xy, e portanto seus valores são sempre positivos ou sempre negativos – dizemos que estas formas são *definidas positivas* ou *definidas negativas*. Uma forma

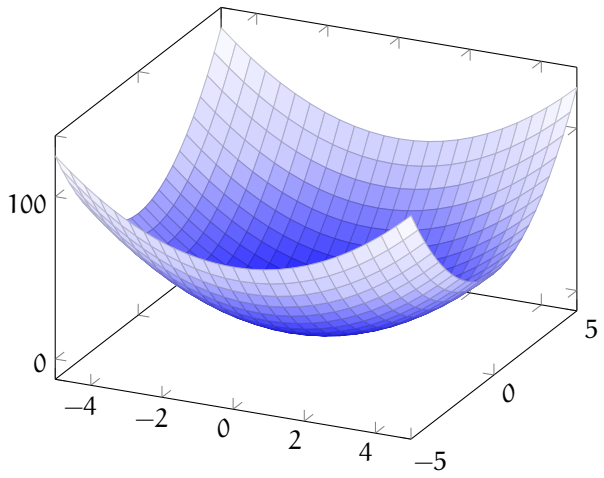
[2] Ou seja, se V tem característica diferente de 2. O Teorema não vale, por exemplo, em $\mathbb{Z}_2$, o corpo finito contendo apenas 0 e 1, e onde $1 + 1 = 0$.

quadrática que cruze o plano xy é *indefinida*. Consolidamos estas idéia na Definição 11.11.

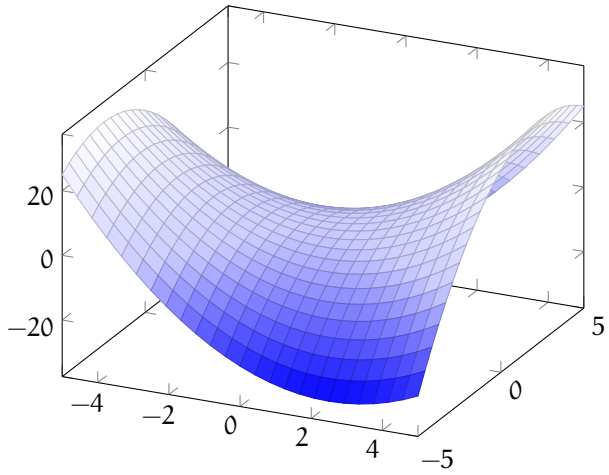
Definição 11.11 (formas definidas e indefinidas)**.** Uma forma quadrática f é **positiva definida** quando $f(\mathbf{x}) = 0$ implica em $\mathbf{x} = \mathbf{0}$; **positiva semidefinida** quando $f(\mathbf{x}) \geq 0$ para todos os valores de $\mathbf{x}$; e **indefinida** quando pode assumir valores positivos e negativos.

Formas quadráticas **negativas definidas** e **negativas semidefinidas** são definidas de forma análoga às positivas. ⧫

A forma $f(x, y) = 2x^2 + 3y^2$ é positiva definida, porque assume valores positivos para todos x, y exceto para $x = 0, y = 0$, quando seu valor é zero. A figura a seguir mostra o gráfico de f quando o domínio é estendido aos reais.



Já $g(x, y) = x^2 + xy - y^2$ é indefinida, porque $f(1, 0) = 1$, e $f(0, 1) = -1$. Da mesma forma que o gráfico anterior, o domínio foi estendido aos reais.



11.1.1 Representação de inteiros e equivalência de formas

Definição 11.12 (representação por forma quadrática; representação própria)**.** Uma forma quadrática f **representa** um inteiro n se existe $\mathbf{x} = (x_1, \ldots, x_k)$ tal que $f(\mathbf{x}) = n$. Se $\operatorname{mdc}(x_1, \ldots, x_k) = 1$ dizemos que f é representação **própria** de n. ♦

Exemplo 11.13. A forma $f(x, y) = 2x^2 - xy + 3y^2$ representa, dentre outros, os inteiros $3, 4, 6$ e 29, 48, porque

$$\begin{aligned} f(0,1) &= 3 \\ f(1,1) &= 4 \\ f(-1,1) &= 6 \\ f(2,3) &= 29 \\ f(2,4) &= 48. \end{aligned}$$

O último número mostrado, 48, tem representação imprópria, porque $\operatorname{mdc}(2,4) = 2$. ◄

A forma, no entanto, não representa o inteiro -1, porque não existem x e y tais que $f(x, y) = -1$.

Definição 11.14 (formas quadráticas equivalentes)**.** Duas formas quadráticas são **equivalentes** se se existe matriz unimodular U tal que $F = UGU^T$. Escrevemos $f \sim g$ quando f é equivalente a g. ♦

O Teorema 11.15 é apresentado sem sua demonstração, que é bastante simples.

Teorema 11.15. *A relação $\sim$ é de equivalência.*

O próximo teorema caracteriza equivalência entre formas a partir de transformações em suas matrizes.

Teorema 11.16. *Formas equivalentes representam os mesmos conjuntos de números inteiros.*

Demonstração. Suponha que $f \sim g$, e que portanto haja U unimodular tal que $F = UGU^T$.

$F(\mathbf{v}) = n$ é o mesmo que $\mathbf{v}(UGU^T)\mathbf{v}^T = n$, que podemos reescrever $(\mathbf{v}U)G(U^T\mathbf{v}^T) = n$, que significa que G representa n, porque $G(\mathbf{v}U) = n$. □

Corolário 11.17. *Se $f \sim g$ então as matrizes de f e g tem o mesmo determinante.*

Demonstração. Claramente, se $F = UGU^T$ e U é unimodular, os determinantes de F e G são iguais, porque $\det(UU^T) = 1$. □

Proposição 11.18. *Se $f \sim g$ então as matrizes de f e g tem o mesmo posto.*

O resto desta Seção trata da finitude da quantidade de classes de formas com o mesmo grau e determinante.

Teorema 11.19. *Para cada determinante $D \neq 0$ e grau n existe um número finito de classes de equivalência de formas quadráticas.*

Demonstração. □

11.1.2 Aplicação: soma de três quadrados

11.2 Formas quadráticas binárias

Deste ponto adiante a discussão ficará restrita a formas quadráticas binárias com coeficientes em $\mathbb{Z}$.

Definição 11.20 (forma quadrática binária)**.** Uma **forma quadrática binária** é uma forma quadrática em duas variáveis. É usual denotar uma forma $ax^2 + bxy + cy^2$ por (a, b, c). ⧫

Definição 11.21 (discriminante)**.** O **discriminante** de uma forma quadrática $ax^2 + bxy + cy^2$ é $\Delta = b^2 - 4ac$. ⧫

Como $\Delta_A = -4 \det A$, podemos dizer que formas equivalentes tem o mesmo discriminante, ou ainda, que o discriminante é uma *invariante* das formas quadráticas, conforme a Definição 11.22.

Definição 11.22. Seja s uma função definida sobre os coeficientes de uma forma quadrática. Se $f = (a, b, c) \sim g = (A, B, C)$ implica que $s(a, b, c) = s(A, B, C)$ dizemos que s é uma **invariante** de formas quadráticas. ⧫

O Teorema 11.23 implica que não há formas com discriminante das formas $4k + 2$ e $4k + 3$.

Teorema 11.23. *O discriminante de uma forma quadrática sempre é congruente a zero ou um módulo* 4*, ou seja,* Δ *é da forma* $4k$ *ou* $4k + 1$*.*

Além disso, se um inteiro Δ *é da forma* $4k$ *ou* $4k + 1$*, há pelo menos uma forma quadrática com discriminante* Δ*.*

Demonstração. Para ver que Δ é da forma dada, basta analisar $b^2 - 4ac \pmod 4$. $4ac$ sempre é congruente a 0 módulo 4, portanto Δ será congruente a b^2 módulo 4, mas quadrados somente deixam resto um ou zero módulo 4.

Se $\Delta \equiv 0 \pmod 4$ então

$$x^2 - \frac{\Delta}{4}y^2$$

tem discriminante Δ. Da mesma forma, se $\Delta \equiv 1 \pmod 4$, então

$$x^2 - \frac{\Delta - 1}{4}y^2$$

terá discriminante Δ. □

Da demonstração extraímos o conceito de *forma principal*, na Definição 11.24.

Definição 11.24 (forma principal)**.** A **forma principal** de um discriminante Δ é

$$\left(1, 0, \frac{-\Delta}{4}\right) \text{ se } \Delta \equiv 0,$$
$$\left(1, 1, \frac{-(\Delta - 1)}{4}\right) \text{ se } \Delta \equiv 1.$$ ⧫

Exemplo 11.25. A forma principal para o discriminante -8 é $(1, 0, 2)$, ou $x^2 + 2y^2$; a forma principal para o discriminante -17 é $(1, 1, 4)$, ou $x^2 + 4y^2$; para o discriminante 12, é $(1, 0, -3)$, ou $x^2 - 3y^2$. ◄

Teorema 11.26. *Seja* $f(x, y) = ax^2 + bxy + cy^2$ *uma forma quadrática com discriminante* Δ*. Esta forma é indefinida se* $\Delta > 0$*; semidefinida (mas não definida) se* $\Delta = 0$*; e definida quando* a *e* c *tiverem o mesmo sinal, e* $\Delta < 0$*.*

Quando a forma é definida, será positiva quando $a > 0$ *e negativa quando* $a < 0$ *.*

Teorema 11.27. *Uma forma quadrática binária é produto de duas formas lineares se e somente se seu discriminante é quadrado perfeito.*

Demonstração. Se $a = 0$ então a forma é $bxy + cy^2$ e o discriminante é b^2. Mas $bxy + cy^2 = y(bx + cy)$, produto de duas formas lineares.

Presumiremos no resto da demonstração que $a \neq 0$.

Seja $\Delta = b^2 - 4ac$ o discriminante da forma. Observamos que

$$4a\, f(x, y) = (2ax + by)^2 - \Delta y^2,$$

Se Δ é quadrado – por exemplo, $\Delta = z^2$ – então

$$\begin{aligned} 4af(x, y) &= (2ax + (b - z)y)(2ax + (b + z)y) \\ f(x, y) &= \frac{(2ax + (b - z)y)(2ax + (b + z)y)}{4a}, \end{aligned}$$

e f é produto de dois fatores lineares racionais, ou seja, há $k, m \in \mathbb{Z}$ tal que

$$\begin{aligned} f(x, y) &= \frac{k}{m} p(x, y)q(x, y) \\ df(x, y) &= kp(x, y)q(x, y), \end{aligned}$$

com $k, m > 0$ e $\operatorname{mdc}(k, m) = 1$.

Pelo Lema 5.36 (lema de Gauss), $c(pq) = c(p)\, c(q)$ e portanto

$$\begin{aligned} mf(x, y) &= kp(x, y)q(x, y) \\ m\, c(f) &= k \end{aligned}$$

Como $\operatorname{mdc}(k, m) = 1$, $m = 1$, e f é produto de duas formas lineares. □

Exemplo 11.28. A forma $2x^2 - xy - y^2$ tem discriminante $(-1)^2 - 4(2)(-1) = 9$, quadrado perfeito, e pode se decomposta em $(2x + y)(x - y)$. ◀

Teorema 11.29. *Um número $n \in \mathbb{Z}$ tem representação própria por uma forma quadrática binária $f(x, y)$ se e somente se é coeficiente de x^2 em alguma forma equivalente a f.*

Demonstração. Primeiro, mostramos que se um número é coeficiente de x^2 em uma forma equivalente a f, ele tem representação própria por f.

Seja $f = ax^2 + bxy + cy^2$, e seja $f \sim g = \alpha x^2 + \beta xy + \gamma y^2$, tal que exista U unimodular com $G = UFU^T$:

$$\begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix} = \begin{pmatrix} m & n \\ r & s \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} m & r \\ n & s \end{pmatrix}$$

Mas expandindo o produto das três matrizes obtemos

$$\alpha = am^2 + bmn + cn^2,$$

ou seja, $\alpha = f(m,n)$, e como a U é unimodular, $ms - nr = 1$, e $\mathrm{mdc}(m,n) = 1$. Esta representação de α por f é própria.

Agora suponha que $\alpha \in \mathbb{Z}$ é representável propriamente por f, ou seja, existem $m,n \in \mathbb{Z}$ tais que $f(m,n) = \alpha$. Provaremos que α é coeficiente de m^2 em alguma forma equivalente a f. Devem existir r,s tais que $ms - nr = 1$, e portanto existe uma matriz unimodular U tal que $F = UGU^T$:

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = \begin{pmatrix} m & n \\ r & s \end{pmatrix} \begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix} \begin{pmatrix} m & r \\ n & s \end{pmatrix}$$

Novamente expandimos o produto no lado direito da equação para verificar que a, coeficiente de x^2 em g, será α:

$$a = \alpha m^2 + \beta mn + \gamma n^2. \qquad \square$$

Exemplo 11.30. A forma $f(x,y) = -3x^2 + xy - y^2$ representa o número -9, porque $f(-1,2) = -9$. Esta forma tem matriz

$$F = \begin{pmatrix} -3 & 1/2 \\ 1/2 & -1 \end{pmatrix}.$$

A matriz F pode ser transformada em $G = UFU^T$ com $U = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$, e obteremos

$$G = \begin{pmatrix} -9 & -23/2 \\ -23/2 & -15 \end{pmatrix}$$

que representa a forma $g(x,y) = -9x^2 - 23xy - 15y^2$, com -9 no coeficiente de x^2. ◀

O Teorema 11.31 e o Corolário11.32 conectam formas quadráticas binárias com a teoria de resíduos quadráticos.

Teorema 11.31. *Sejam $n \neq 0$ e Δ inteiros. Então há uma forma quadrática binária que representa propriamente n, com discriminante Δ, se e somente se Δ é resíduo quadrático módulo $4|n|$.*

Demonstração. Suponha que $f(a,b,c) = n$ e $k^2 = \Delta \pmod{4|n|}$. Pelo Teorema 11.29, existe $g \sim f$ com $g = nx^2 +, sxy +, ty^2$. Como f e g tem o mesmo discriminante,

$$\begin{aligned} \Delta &= s^2 - 4nt \\ \Delta &\equiv s^2 \pmod 4. \end{aligned}$$

Para a recíproca, suponha que exista k tal que $k^2 \equiv \Delta \pmod{4|n|}$. Existe então r tal que $\Delta = k^2 - 4|n|r$. A forma $g = |n|x^2 + kxy + ry^2$ tem discriminante $k^2 - 4|n|r = \Delta$, e $g(1,0,0)$ é representação própria de n. $\square$

Corolário 11.32. *Seja Δ congruente a 1 ou 0 módulo 4 e p um primo ímpar. Então existe uma forma quadrática binária com discriminante Δ que representa p se e somente se Δ é diferente de zero e resíduo quadrático módulo p.*

Demonstração. Como p é primo, qualquer representação sua é própria, e pelo Teorema 11.31, Δ é quadrado módulo $4p$. Assim, $(\Delta/p) = 1$. A recíproca: se $(\Delta/p) = 1$ então Δ é resíduo quadrático módulo p. O enunciado determina que $\Delta \equiv 0, 1 \pmod 4$, o que significa que Δ é quadrado módulo 4 (porque um inteiro é quadrado módulo 4 se e somente se é congruente a 0 ou 1 módulo 4). Pelo Teorema Chinês dos Restos, como p é ímpar e

$$\begin{aligned} \Delta &\equiv r^2 \pmod p \\ \Delta &\equiv k^2 \pmod 4, \end{aligned}$$

Δ é quadrado módulo $4p$, e portanto, pelo Teorema 11.31, p tem representação própria por alguma forma com discriminante Δ. □

A Lei da Reciprocidade Quadrática define para quais primos ímpares $(\Delta/p) = 1$, sendo assim relevante para determinar que primos são representáveis por um dado discriminante.

Proposição 11.33. *Não há formas quadráticas binárias primitivas equivalentes a formas não-primitivas.*

Definição 11.34 (discriminante fundamental)**.** Δ é um **discriminante fundamental** se todas as formas com discriminante Δ são primitivas. ♦

Teorema 11.35. *Os discriminantes fundamentais são*

i) $\Delta = 4k + 1$ *livre de quadrados;*

ii) $\Delta = 4k$*, com* k *igual a* $4r + 2$ *ou* $4r + 3$*.*

Demonstração. Seja algum Δ como definido no enunciado, e suponha (por absurdo) que Δ seja discriminante de uma forma não primitiva $ax^2 + bxy + cy^2$. Seja $k = \operatorname{mdc}(a, b, c)$. Claramente, $k^2 | \Delta$, portanto Δ precisa ser to tipo (ii). A única possibilidade, portanto, é $\Delta = 2$. Isso implica que $a = 2\alpha$, $b = 2\beta$, $c = 2\gamma$, e $\Delta' = \Delta/4 = \beta^2 - 4\alpha\gamma$. Então $\Delta' = 4k$ ou $4k + 1$, o que é impossível, porque determinamos que Δ é to dipo (ii). Presumimos portanto que se Δ é de um dos dois tipos dados, não pode ser discriminante de uma forma não primitiva.

A recíproca: Suponha agora que Δ *não* seja como definido no enunciado. Tratamos dois casos: se $\Delta = 4k + 1$, tendo um quadrado como fator, então $\Delta = \Delta' m^2$, e a forma

$$mx^2 + mxy - \left(\frac{m(\Delta - 1)}{4}\right) y^2$$

tem discriminante Δ, mas claramente não é primitiva, porque m divide todos os coeficientes.

Se $\Delta = 4k$, verificamos três casos, k livre de quadrados; $k = 4r$; e $k = 4r+1$. Para os dois primeiros, a forma

$$mx^2 - \frac{k}{m}y^2 2$$

tem discriminante Δ e não é primitiva, porque m divide os dois coeficientes não nulos.

Se $k = r+1$, a forma

$$2x^2 + 2xy - \frac{k-1}{2}$$

tem discriminante Δ e não é primitiva, porque 2 divide todos os coeficientes. Assim, se Δ como no enunciado, qualquer forma que o tenha como discriminante é não-primitiva. □

11.2.1 Redução de formas

Como cada forma pode ser equivalente a várias outras, é interessante definir algum critério para determinar que uma forma é "reduzida". Veremos que para classes de formas definidas positivas, a forma reduzida é única, e portanto pode ser usada para comparar formas: para saber se duas formas f e g estão na mesma classe de equivalência, basta reduzir ambas e verificar se a forma reduzida das duas é a mesma.

Primeiro mostraremos que qualquer forma (a, b, c) é equivalente a outra forma (A, B, C) com $|B| \leq |A| \leq |C|$, e depois usaremos esta propriedade para definir forma reduzida, mas apenas para formas definidas positivas.

Lema 11.36. *Dados $a, b, c, k \in \mathbb{Z}$, então*
(i) $(a, b, c) \sim (c, -b, -a)$*, e*
(ii) $(a, b, c) \sim (a, b + 2ka, ak^2 + bk + c)$.

Demonstração.

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

são unimodulares, e levam (a, b, c) às duas formas equivalentes dadas no enunciado:

$$S^T F S = (c, -b, a)$$
$$(T^k)^T F T^k = (a, b + 2ka, ak^2 + bk + c)$$ □

Note que se $|a| > |c|$, a transformação S leva a uma forma (A, B, C) com $|A| < |C|$, porque troca a posição dos dois argumentos. Se $|b| > |a|$, a pode-

se escolher k tal que a transformação T^k leva a uma forma (A, B, C) com $|B| < |A|$. Assim, se uma forma (a, b, c) não é como desejado, o Lema 11.36 permite encontrar uma forma equivalente (A, B, C) em que $|A| \leq |C|$ ou $|B| \leq |A|$. Após uma quantidade finita de passos, chega-se a uma forma em que os coeficientes tem a propriedade que queremos:

1. Se $|a| > |c|$, troque (a, b, c) por $(c, -b, -a)$ (use S);
2. Se $|b| > |a|$, troque (a, b, c) por (a, B, C), onde $B = b + 2ak$, com k escolhido tal que $|B| \leq |a|$ (use T^k);
3. Se a forma obtida não for tal que $|b| \leq |a| \leq |c|$, repita os dois passos anteriores.

Teorema 11.37. *Em cada classe de equivalência relacionada a um discriminante que não seja quadrado perfeito existe pelo menos uma forma com* $|b| \leq |a| \leq |c|$.

Demonstração. Iniciando com uma forma qualquer (a, b, c) na classe de equivalência, basta aplicar o algoritmo descrito no parágrafo anterior ao enunciado. O algoritmo necessariamente para, e chega a uma forma com $|b| \leq |a| \leq |c|$. □

Definiremos *para formas definidas positivas* o conceito de forma reduzida. Para as formas indefinidas o algoritmo apresentado funciona, mas pode haver mais de uma forma com a caracterização dada; o tratamento de formas indefinidas é usualmente feito de maneira diferente, e não o abordaremos.

Definição 11.38 (forma quadrática positiva definida reduzida e semirreduzida)**.** Uma forma quadrática positiva definida (a, b, c) é **semirreduzida** se $|b| \leq a \leq c$; **reduzida** se

i) $-a \leq b < a < c$, ou

ii) $0 \leq b \leq a = c$. ♦

Teorema 11.39. *Se duas formas semirreduzidas são equivalentes, então elas são*

i) $(a, b, a) \sim (a, -b, a)$ *ou*

ii) $(a, a, c) \sim (a, -a, c)$.

Demonstração. Sejam $f = (a, b, c) \sim g = (A, B, C)$. Então existe $U = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, unimodular, tal que $G = UFU^T$. Mostramos inicialmente que $a = A$: suponha, sem perda de generalidade, que $A \leq a$. A transformação determina

que

$$\begin{aligned} A &= ar^2 + brt + ct^2 \\ B &= s(2ar + bt) + u(2ct + br) \\ C &= as^2 + bsu + cu^2. \end{aligned}$$

Suponha, sem perda de generalidade, que $a \geq A$.

$$\begin{aligned} a &\geq A \\ &\geq ar^2 - a|rt| + at^2 \\ &= a|rt| + a(|r| - |t|)^2 \\ &\geq a|rt|, \end{aligned}$$

e $a \geq A \geq a|rt|$. $|rt|$ deve ser, portanto menor ou igual que um, ou teríamos $a \geq a|rt| > a$. Mas r e t não podem ser ambos zero, porque dessa forma teríamos U com determinante zero. As possibilidades para r e t são $(0, \pm 1)$, $(\pm 1, 0)$, $(\pm 1, \pm 1)$, $(\pm 1, \mp 1)$.

Também comcluímos que quando r, t são ambos diferentes de zero, $a \geq A \geq a|rt|$ e $|rt| = 1$ implicam que $a = A$.

O mesmo raciocínio aplicado usando $c \geq C$ leva à conclusão de que na segunda coluna de U, as possibilidaes de valores para s e u são as mesmas.

Além disso, para que $\det U = 1$, se $r = 0$ ou $u = 0$, então $t = -s$, e se $s = 0$ ou $t = 0$, $u = r$.

Dividimos as matrizes integrais com estas restrições em três casos, de acordo com a primeira coluna. Note que nos dois primeiros casos a primeira coluna igual a $(1, 0)$ ou $(0, 1)$ determina um dos elementos da segunda, para que o determinante seja 1.

$$\begin{aligned} \pm \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, &\quad (a, b, c) \to (a, b \pm 2as, \ldots) \\ \pm \begin{pmatrix} 0 & -1 \\ 1 & u \end{pmatrix}, &\quad (a, b, c) \to (c, b \pm 2au, \ldots) \\ \pm \begin{pmatrix} 1 & s \\ \pm 1 & u \end{pmatrix}, &\quad (a, b, c) \to (a \pm b + c, \ldots, \ldots) \end{aligned}$$

Os valores de s e u devem ser 0 ou ± 1, e no terceiro caso exatamente um deles deve ser zero.

No primeiro caso, se $s = 0$ a matriz é a identidade; quando $s = 1$, $b \pm 2as = b \pm 2a$ e a desigualdade $|b \pm 2a| \leq |a|$ só é possível com $a = -b$, e teremos $(a, a, c) \to (a, -a, c)$. Quando $s = -1$, $a = b$ e a transformação é $(a, -a, c) \to (a, a, c)$.

No segundo caso, a transformação determina que o primeiro coeficiente

passa a ser c. Como as duas formas são semirreduzidas, $a \leq c \leq a$ implica que $a = c$ e $f = (a, b, a)$. Se $u = 0$, a transformação leva de (a, b, a) em $(a, -b, a)$. Se $u = 1$, a transformação é $(a, b, a) \to (a, -b \pm 2a, \dots)$, mas é necessário que $|-b + 2a| \leq |a|$, o que só é possível se $a = b$, e temos $(a, a, a) \to (a, -a, a)$. Quando $u = -1$, $a = -b$ e a transformação é $(a, -a, a) \to (a, a, a)$.

No último caso, o primeiro coeficiente de g é $a + b + c$, mas como r e t são diferentes de zero, $a = A$ e $b = -c$. Como as duas formas são semirreduzidas, $a = \pm b$, $f = (a, a, a)$ ou $f = (a, -a, a)$. As matrizes do terceiro caso representam as transformações $(a, a, a) \to (a, -a, a)$, $(a, -a, a) \to (a, a, a)$, $(a, a, a) \to (a, a, a)$ e $(a, -a, a) \to (a, -a, a)$. □

Corolário 11.40. *Uma classe de equivalência de formas quadráticas definidas positivas tem uma e somente uma forma reduzida.*

11.2.2 Quantidade de representações

Definição 11.41 (automorfismo de forma quadrática)**.** Seja f uma forma quadrática com matriz F. Um **automorfismo** de f é uma matriz unimodular U tal que $UFU^T = F$.

A **quantidade de automorfismos** de f é denotada por $w(f)$. ♦

Exemplo 11.42. Seja $f = (2, -1, 1)$. A matriz de f é $F = \begin{pmatrix} 2 & -1/2 \\ -1/2 & 1 \end{pmatrix}$. Um automorfismo de F é $U = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$, porque

$$UFU^T = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1/2 \\ -1/2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} = F. \qquad \blacktriangleleft$$

A quantidade de automorfismos para cada forma definida positiva é limitada.

Teorema 11.43. *Os automorfismos de uma forma quadrática binária positiva definida reduzida f são exatamente*

$$\begin{cases} x = \pm X \\ y = \pm Y \end{cases} \quad \begin{cases} x = \pm X \\ y = \mp Y \end{cases} \qquad \text{se } f = (a, 0, a)$$

$$\begin{cases} x = \pm X \\ y = \pm Y \end{cases} \quad \begin{cases} x = \pm X \\ y = \mp X \mp Y \end{cases} \quad \begin{cases} x = \pm X \pm Y \\ y = \mp X \end{cases} \qquad \text{se } f = (a, a, a)$$

$$\begin{cases} x = \pm X \\ y = \pm Y \end{cases} \qquad \text{em outros casos,}$$

e portanto $w(f)$ pode ser 4, 6 ou 2, conforme os casos acima.

Demonstração. Lembramos, do Teorema 11.36, que

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

O Teorema 11.39 determina as equivalências possíveis entre formas semi-reduzidas. Para selecionar os automorfismos, eliminamos $(a, a, c) \to (a, -a, c)$, porque a única forma que esta transformação leva em si mesma é $(a, -a, a)$, que é semirreduzida mas não reduzida. Para o caso $(a, b, a) \to (a, -b, a)$, é necessário que $b = 0$ ou $b = a$. Portanto, dentre as transformações listadas naquele Teorema as seguintes são automorfismos:

- $\pm I$, duas possibilidades para o caso geral;
- $\pm S$ é automorfismo para $(a, 0, a)$, e para estas formas temos mais duas possibilidades, totalizando quatro.
- As transformações $\pm ST = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ e $\pm (ST)^2 = \pm \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, também dentre aquelas listadas no Teorema 11.39, levam (a, a, a) em (a, a, a). Assim, além das duas transformações $\pm I$, há mais quatro, totalizando seis.

Todas as outras transformações entre formas reduzidas necessariamente modificam a forma.

As transformações identificadas, quando aplicadas a $\begin{pmatrix} X \\ Y \end{pmatrix}$, resultam nas trocas de variáveis listadas no enunciado. □

Corolário 11.44. *Se f é uma forma primitiva positiva com discriminante Δ, então*

$$w(f) = \begin{cases} 6 & \text{se } \Delta = -3, \\ 4 & \text{se } \Delta = -4, \\ 2 & \text{se } \Delta < -4. \end{cases}$$

11.2.3 Número de classe

Além do número de representações de um inteiro, nos interessa a quantidade de classes de equivalência existentes para cada determinante.

Definição 11.45 (número de classe)**.** O **número de classe** de um discriminante fundamental Δ, denotado $h(\Delta)$, é o número de classes de equivalência próprias de formas primitivas com tal discriminante. ♦

Fórmula de Dirichlet para o número de classe

Teorema 11.46. *Se $\Delta = -p$, com $p \neq 3$ um primo da forma $4k+3$, então*

$$h(-p) = \frac{B - A}{p},$$

onde

- A = *soma dos números entre 0 e p que são resíduos quadráticos módulo p, e*

- B = *soma dos números entre 0 e p que não são resíduos quadráticos módulo p.*

Exercícios

Ex. 236 — Prove que a seguinte definição é equivalente à dada no texto.

Definição 11.47 (forma quadrática)**.** Seja V um espaço vetorial de dimensão finita sobre um corpo K com característica diferente de 2 (ou seja, $1 + 1 \neq 0$ em K). Uma função $f : V \times V \to K$ é uma **forma quadrática** se

- $\forall\, k \in K$, $\mathbf{v} \in V$, $f(k\mathbf{v}) = k^2 f(\mathbf{v})$
- a função $b(\mathbf{v}, \mathbf{w}) = f(\mathbf{v} + \mathbf{w}) - f(\mathbf{v}) - f(\mathbf{w})$ é uma forma bilinear. ♦

Ex. 237 — (Fácil) Seja $f = ax^2 + bxy + cy^2$ uma forma quadrática binária. Mostre que $b \equiv \Delta(f) \pmod 2$.

Ex. 238 — Quais das formas são equivalentes? $x^2 + 2xy + 4y^2$, $x^2 - 2xy - 21y^2$, $-2x^2 - y^2$, $2x^2 + 4xy + 3y^2$.

Ex. 239 — Seja $\Delta \in \mathbb{Z}$ um quadrado perfeito. Mostre que existe um forma quadrática binária $ax^2 + bxy + cy^2$ com discriminante Δ e $a = 0$.

Ex. 240 — Demonstramos que se f e g são equivalentes (existe matriz unimodular U, $F = U^T G U$). Agora tente seguir os passos na direção da recíproca:
Suponha que para todo $n \in \mathbb{Z}$, f representa n se e somente se g também representa n. Então:

i) Existe uma matriz que transforma G em F?

ii) Com determinante ± 1?

iii) E integral?

Ex. 241 — Seja f uma forma quadrática binária com discriminante negativo e $n \in \mathbb{Z}$. Mostre como resolver a equação diofantina $f(x, y) = n$.

Ex. 242 — Seja f uma forma quadrática binária com discriminante negativo e $n \in \mathbb{R}$. Mostre que a quantidade de soluções para $f(x, y) = n$ é finita.

Ex. 243 — Prove que todo discriminante pode ser escrito de forma única como $k^2\Delta$. onde Δ é discriminante fundamental.

Ex. 244 — Prove que Δ é discriminante fundamental se e somente se

i) Δ não é divisível pelo quadrado de um primo ímpar; e

ii) Δ é da forma $16k + 8$ ou da forma $16k + 12$.

Ex. 245 — Um discriminananante fundamental $\Delta \in \mathbb{Z}$ é **primo** se é divisível por exatamente um inteiro primo. Prove que se $\Delta \in \mathbb{Z}$ é um discriminante fundamental, então Δ pode ser escrito de forma única (a não ser por ordem) como produto de discriminantes primos.

Ex. 246 — Demonstre: sejam $n, \Delta \in \mathbb{Z}$, com $n > 3$ e $\text{mdc}(n, \Delta) = 1$. Então n tem representação própria por forma primitiva com discriminante Δ se e somente se Δ é resíduo quadrático módulo n.

Ex. 247 — Encontre uma definição sucinta para forma quadrática definida reduzida. A definição deve valer para formas positivas e negativas, sem a necessidade de separar explicitamente estes dois casos.

Ex. 248 — Demonstre o final do Teorema 11.43.

Ex. 249 — Demonstre o Corolário 11.44.

Ex. 250 — Prove que um automorfismo de uma forma quadrática binária (a, b, c) sempre é da forma

$$\begin{pmatrix} \frac{j - bk}{2} & ak \\ -ck & \frac{j + bk}{2} \end{pmatrix}$$

onde $j, k \in \mathbb{Z}$ são soluções da equação de Pell $j^2 - \Delta k^2 = 4$.

Ex. 251 — Prove que os automorfismos de uma forma quadrática binária formam um grupo.

Ex. 252 — Prove que os grupos de automorfismos das formas primitivas com um mesmo determinante são isomorfos.

Ex. 253 — Prove que toda forma definida com determinante 1 é equivalente à forma $x^2 + y^2$.

Ex. 254 — Prove que todo primo da forma $4k + 1$ pode ser escrito como soma de dois quadrados, usando o Teorema 11.31. (Ou seja, apresente uma demonstração alternativa para o Teorema 10.3).

Ex. 255 — Prove que se o determinante de uma forma quadrática binária f é quadrado perfeito, então existem $x, y \in \{0, 1\}$, pelo menos um deles diferentes de zero, tais que $f(x, y) = 0$.

Capítulo 12

Formas Modulares, Grupo Modular

Este Capítulo é um esboço

12.1 O grupo modular

Uma *transformação linear fracionária* é uma função $f : \mathbb{C} \to \mathbb{C}$, da forma

$$f(z) = \frac{az + b}{cz + d},$$

Representamos transformações como matrizes:

$$f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Se tivermos f como dada acima, e definirmos uma outra transformação

$$g(z) = \frac{\alpha z + \beta}{\gamma z + \delta},$$

então a composição de f e g será

$$f(g(z)) = \frac{(b\gamma + a\alpha)z + b\delta + a\beta}{(d\gamma + c\alpha)z + d\delta + c\beta}.$$

É conveniente que a multiplicação de matrizes pode ser usada para representar a composição de transforamções lineares fracionárias. Se f e g são

da forma já dada, e F e G são suas matrizes, então

$$FG = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} b\gamma + a\alpha & b\delta + a\beta \\ d\gamma + c\alpha & d\delta + c\beta \end{pmatrix}$$

representa a composição de f com g.

O *grupo linear geral* de grau n, denotado $GL(n, F)$, é o grupo de matrizes invertíveis $n \times n$ sobre o corpo F, com a operação de multiplicação de matrizes. O *grupo linear especial* $SL(n, F)$ é o subgrupo de $GL(n, F)$ contendo apenas as matrizes com determinante $+1$.

O grupo que representa as transformações lineares fracionárias que nos interessam é um subgrupo de $SL(n, F)$ chamado de *grupo modular*, ou *grupo linear especial projetivo*. Em $SL(n, F)$, as matrizes A e $-A$ são tratadas como o mesmo elemento.

Definição 12.1 (grupo modular / grupo linear especial projetivo $PSL(2, \mathbb{Z})$)**.** As matrizes 2×2 com elementos integrais e determinante 1, usando a operação usual de multiplicação de matrizes, formam o *grupo modular*, também chamado de *grupo linear especial projetivo*. Equivalentemente, as transformações da forma

$$T(z) = \frac{az + b}{cz + d},$$

com $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$, e usando a operação de composição de funções, formam o grupo modular. Este grupo é denotado por $PSL(2, \mathbb{Z})$, ou por Γ. ♦

Como exemplo,

$$M = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \in \Gamma,$$

porque todos os $m_{i,}$ são inteiros, e $\det M = 1$.

Teorema 12.2. *O grupo Γ é gerado pelas transformações $S(z) = -z^{-1}$ e $T(z) = z + 1$, ou seja,*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

já definidos no Lema 11.36 do Capítulo 11 (página 217).

Demonstração. O efeito das matrizes S e T é simples: S realiza troca de linhas, e como o determinante deve se manter um, S também realiza a troca do sinal do determinante; T soma a segunda linha à primeira.

$$T \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ c & d \end{pmatrix}, \quad S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

Para mostrar que qualquer matriz de Γ é produto das matrizes T e S, começamos com uma matriz qualquer de Γ:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Suponha que c seja zero. Como $\det M = 1$ e os elementos são todos inteiros, então a diagonal só pode ser $a = d = \pm 1$. Mas isto significa que M é T^n, para algum n, já que

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Suponha, então, que $c > 0$. Suponha também que $|a| > |c|$ (se não for, pode-se usar S para trocar as linhas).

Agora faremos a divisão de a por c: $a = qc + r$, com $0 \leq r < |c|$. Isto pode ser realizado multiplicando T^{-q}:

$$T^{-q}M = \begin{pmatrix} a - qc & b - qd \\ c & d \end{pmatrix}.$$

Se $a - qc$ for zero, paramos. Senão, usamos S para trocar as linhas e recomeçamos. Este é essencialmente o algoritmo de Euclides para cálculo de MDC, e eventualmente o valor na posição $(1,1)$ da matriz será zero, e usaremos S uma última vez para trocar as linhas para que a posição $(2,1)$ passe a ser zero. Como o determinante da matriz não foi alterado (porque só usamos T e S), a diagonal será composta por uns, com o mesmo sinal, e portanto será igual a T^k, para algum k. □

Corolário 12.3. *Toda matriz $M \in \Gamma$ pode ser escrita como*

$$M = T^{k_1} S T^{k_2} S \cdots T^{k_n}.$$

É relevante também que $S^2 = (ST)^3 = I$.

Exploramos a seguir a ação do grupo modular no meio-plano superior.

Definição 12.4 (meio-plano superior)**.** Denotamos por $\mathbb{H}$ o *meio plano superior*, que no plano complexo contém os números com parte imaginária positiva,

$$\mathbb{H} = \{a + bi \,:\, a, b \in \mathbb{R}, b > 0\}$$ ♦

Definição 12.5 (pontos equivalentes em $\mathbb{H}$)**.** Dois pontos $z, z' \in \mathbb{H}$ são equivalentes quando existe $g \in \Gamma$ tal que $g(z) = z'$. Denotamos $z \sim z'$. ♦

Definição 12.6 (região fundamental)**.** Dado um grupo de transformações no plano, a *região fundamental* (também chamada de *"domínio fundamental"*) do grupo é uma região do plano que não contém dois pontos equivalentes, mas contém pontos representando todas as classes de equivalência. ♦

Por exemplo, as duas transformações $f(x,y) = (x+1, y)$, e $g(x,y) = (x, y+2)$ geram um grupo de transformações: o grupo contendo as transformações

$$\{h(x,y) = (ax, 2by) \ : \ a, b \in \mathbb{Z}\},$$

e a operação de composição de funções. Uma região fundamental desse grupo é o retângulo com vértices $(0,0)$, $(1,0)$, $(1,2)$, $(0,2)$.

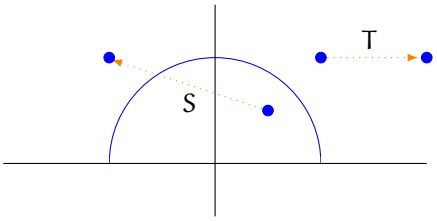
Há algumas observações importantes sobre o efeito de S e T em $\mathbb{H}$.

A transformação S leva a parte imaginária de seu argumento

- de dentro para fora do círculo unitário, se $N(z) < 1$;
- de fora para dentro do círculo unitário, se $N(z) > 1$;
- da borda para para algum outro ponto também na borda do círculo unitário, se $N(z) = 1$, porque $S(z)$ deverá, neste caso, ter também norma um.

A interpretação geométrica: $1/z = \bar{z}/N(z)$, ou seja, inverter um complexo é realizar uma reflexão pelo eixo das abscissas, e mudar a magnitude do vetor. Logo, $-1/z$ realiza uma reflexão pelo eixo das ordenadas e divide a magnitude por $N(z)$.

A transformação T realiza uma translação, não alterando a parte imaginária do número.



A seguir identificaremos um domínio fundamental para Γ.

Lema 12.7. *O ponto $\rho = (-1 + i\sqrt{3})/2$ é mapeado em si mesmo somente pelas transformações*

$$z' = z, \quad z' = -\frac{1}{z+1}, \quad z' = -1 - \frac{1}{z},$$

ou seja, a identidade, ST e $T^{-1}S$.

O ponto i é mapeado em si mesmo somente pela identidade e por S,

$$z' = z, \quad z' = -\frac{1}{z},$$

Qualquer outro ponto em $\mathbb{R}$ é mapeado em si mesmo apenas pela identidade.

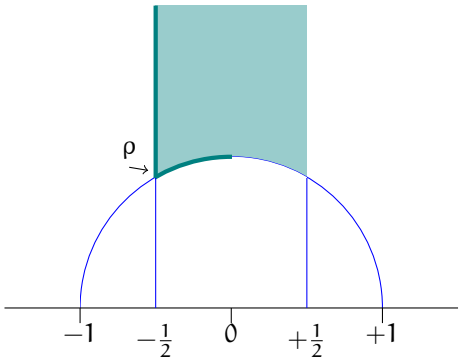
As transformações ST e $T^{-1}S$ mapeiam ρ nele mesmo porque S tem o mesmo efeito que T em ρ. Em i, S claramente não tem efeito, porque i é unidade.

Teorema 12.8. *Seja*

$$R = \left\{ z \in \mathbb{H} \ : \ \mathrm{Re}(z) \in \left[-\frac{1}{2}, +\frac{1}{2} \right), N(z) > 1 \right\}$$
$$\bigcup \left\{ z \in \mathbb{H} \ : \ \mathrm{Re}(z) \in \left[-\frac{1}{2}, 0 \right), N(z) = 1 \right\}$$

Então R *é região fundamental de* Γ.

A figura a seguir ilustra a região R, e o ponto $\rho = (-1 + \sqrt{3})/2$. Note que a região é fechada no segundo quadrante, e aberta no primeiro. Isto é importante, porque de outra forma, teríamos dois pontos equivalentes na região fundamental: por exemplo, se $x = i - 1/2$ e $y = i + 1/2$, então ambos estariam em R e $y = T(x)$.



Demonstração. Demonstraremos que (i) para todo $z \in \mathbb{H}$, $z = f(z')$, com $f \in \Gamma$; e (ii) que se $z, z' \in R$, e existe $f \in \Gamma$, com $z = f(z')$, então $z = z'$.

(i) Passo um: seja $z \in \mathbb{H}$, e suponha que $N(z) > 1$. Então existe alguma n-ésima potência de T tal que $T^n(z)$ tem a parte real em $[-1/2, +1/2)$. Se, além disso, $T^n(z)$ está em R, terminamos. Senão, é porque a translação levou de fora para dentro do círculo unitário, mas não para dentro de R. Então a norma é menor que 1, e usamos o passo dois.

Passo dois: se $N(z) < 1$, realizamos uma inversão com S. Esta inversão aumentará a parte imaginária de z. Se o resultado é um ponto em R, terminamos. Senão, voltamos ao passo um.

Estes passos (T^k seguido de S) podem ter que ser repetidos um número finito de vezes, porque eventualmente a parte imaginária será maior que 1, e uma translação será suficiente para chegar a R.

Como T e S são bijeções, todo $z \in \mathbb{H}$ é igual a $f(z')$, para algum $f \in \Gamma$ e algum $z' \in R$.

(ii) Suponha que $g \in \Gamma$, e $z \in R$. Agora, suponha que $g(z) = z'$. Suponha também, sem perda de generalidade, que $\mathrm{Im}(gz) \geq \mathrm{Im}(z)$, ou seja, que z' está acima de z no meio-plano $\mathbb{H}$. Mas para que isto seja verdade,

$$|cz + d| \leq 1.$$

Como $|z| > 0$, então necessariamente $|c| \leq 1$. Uma vez que $c \in \mathbb{Z}$, então

$$c \in \{-1, 0, +1\}.$$

Se $c = -1$, podemos trocar g por $-g = \left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$, e teremos a mesma transformação com $c = +1$, por isso tratamos apenas dos casos $c = 0$ e $c = +1$.

Se $c = 0$, então

$$g(z) = \frac{az + b}{cz + d} = \frac{az + b}{d}$$

Mas $ad - bc = 1$, e como $c = 0$, temos $ad = 1$, com $a, d \in \mathbb{Z}$. Assim, $a, d = \pm 1$. Com isso teremos

$$g(z) = z + b,$$

e $g(z) = T^n(z)$. Mas como a translação não pode mudar a parte imaginária de um número, e a largura da região que escolhemos como domínio fundamental é 1, então $b = 0$ e g é a identidade, logo $z = z'$.

Se $c = +1$, então há duas possibilidades: (i) $d = 0$, ou (ii) $d = 1$ e $z = \rho$. No primeiro caso, com $d = 0$ e $c = 1$, temos $|cz + d| \leq 1$, logo $|z + 1| \leq 1$. Mas isso implica que $|z| = 1$. Como $ad - bc = 1$, então $-bc = 1$, e $b = -c = -1$. A transformação teria que ser, portanto,

$$g(z) = \frac{az + b}{cz + d} = a - \frac{1}{z},$$

ou seja, $T(S(z))$. Mas, como a parte imaginária de z estava em R, era maior que um. E esta transformação muda a parte imaginária para algo menor que um (porque aplica S, e em seguida T), e portanto z e $g(z)$ não podem estar ambos em R.

No segundo caso, $c = +1$, $z = \rho$, $d = 1$,

$$g(z) = \frac{az + b}{z + 1}$$

Mas $ad - bc = 1$, portanto $a - b = 1$, e

$$\begin{aligned} g(z) &= \frac{az + (a-1)}{z+1} \\ &= a - \frac{1}{\rho + 1}, \end{aligned}$$

novamente uma inversão seguida de translação. Mas como $N(\rho) = 1$, sua parte imagniária não é modificada por g, e a transformação é uma translação – novamente, temos que necessariamente g é a identidade, e $g(\rho) = \rho$. □

12.2 Formas Quadráticas Binárias Definidas

Se uma forma quadrática (a, b, c) é positiva definida tem discriminante menor que zero, e por isso as raízes da equação $ax^2 + bx + c = 0$ são dois números complexos, com parte imaginária diferente de zero. Isso nos permite usar uma definição bastante simples para forma reduzida.

Sejam $z, \bar{z}$ as duas raízes da equação. Uma delas tem a parte imaginária positiva, e portanto está no meio-plano superior. Sem perda de generalidade, suponha que esta seja z. Tome o representante da classe de equivalência de z na região fundamental de Γ.

Teorema 12.9. *Se uma forma quadrática $ax^2 + bxy + cy^2$ definida positiva está na forma reduzida – ou seja,*

$$-a < b \leq a < c \quad \textit{ou} \quad 0 \leq b \leq a = c,$$

então uma de suas duas raízes complexas está no domínio fundamental de Γ.

Demonstração. Seja z a raiz de $ax^2 + bx + c$ que está em $\mathbb{H}$. Separamos as partes real e imaginária de z

$$\begin{aligned} z &= \frac{-b + \sqrt{\Delta}}{2a} \\ &= \frac{-b}{2a} + \frac{\sqrt{\Delta}}{2a} \\ &= \frac{-b}{2a} + i\frac{\sqrt{-\Delta}}{2a} \end{aligned}$$

A norma de z é

$$\begin{aligned} N(z) &= \frac{b^2}{4a^2} + \frac{-\Delta}{4a^2} \\ &= \frac{b^2 - b^2 + 4ac}{4a^2} \\ &= \frac{c}{a}. \end{aligned}$$

Desta forma, para que $z \in R$, é necessário que a parte real esteja em $[-1/2, +1/2)$,

$$\begin{aligned} -\frac{1}{2} \leq \frac{-b}{2a} &< \frac{1}{2} \\ -a \leq -b &< a \\ a \geq b &> -a, \end{aligned}$$

e que a norma seja > 1 quando a parte real é positiva, e ≥ 1 quando a parte real é ≤ 0. No primeiro caso,$c/a > 1$ implica imediatamente que $c > a$. No segundo, temos $-b/2a > 0$ e $c/a = 1$, o que implica que $b \geq 0$ e $c = a$. Combinando as possibilidades, concluímos que uma forma definida positiva tem representante no domínio fundamental de Γ se

$$-a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c,$$

conforme o enunciado. □

Na demonstração do Teorema 12.8, que afirma que R é domínio fundamental de Γ, há um algoritmo para trazer um ponto qualquer ed $\mathbb{H}$ para R. O mesmo algoritmo pode ser usado para transformar uma forma em outra equivalente, com raiz dentro de R. Basta aplicar as transformações na matriz da forma, ao invés de aplicá-las nos pontos (a aplicação das transformações S e T^k em uma matriz F é efetuada por $S^T F S$ e $(T^K)^T F T^K$). Este algoritmo é o mesmo apresentado no estudo das formas quadráticas reduzidas no Capítulo 11.

12.3 Formas quadráticas indefinidas

Exercícios

Ex. 256 — Prove que o grupo Γ também pode ser gerado por

$$\begin{aligned} t(z) &= z + 1 \\ u(z) &= \frac{z}{z+1} \end{aligned}$$

Ex. 257 — Prove que o grupo Γ pode ser gerado por duas transformações de ordem finita no grupo (a transformação T, que usamos no gerador de Γ, não tem ordem finita!)

Ex. 258 — Encontre um domínio fundamental para Γ que contenha somente números com norma menor ou igual a um. Depois, formule uma definição alternativa de forma quadrática positiva definida reduzida usando esta região como referencia, e não a região R definida neste texto.

Ex. 259 — Seja n o produto de k primos da forma $8k+1$ ou $8k+3$. Prove que há 2^{k+1} representações próprias de n na forma x^2+2y, com $x, y > 0$.

Ex. 260 — Fixe $n \in \mathbb{Z}$, tal que $1 < n < 5$. Sejam

- Γ_1 o *grupo* gerado por $s(z) = -z^{-1}$ e $u(z) = z + \sqrt{n}$.
- Γ_2 o *conjunto* de todas as transformações lineares fracionárias das formas

$$q(z) = \frac{az + b\sqrt{n}}{c\sqrt{n} + d}, \quad ad - nbc = 1$$
$$r(z) = \frac{a\sqrt{n}z + b}{cz + d\sqrt{n}}, \quad adn - bc = 1,$$

  com $a, b, c, d \in \mathbb{Z}$.

Prove que Γ_2 é grupo, e que $\Gamma_2 = \Gamma_1$. Identifique um domínio fundamental para Γ_1, e prove que de fato é domínio fundamental. Se $\Gamma_2 \neq \Gamma_1$, faça o mesmo para Γ_2.

Capítulo 13

Partições de um Inteiro

13.1 Funções geradoras

A expansão de $(1+x)^n$ é o polinômio

$$\begin{aligned}(1+x)^n &= \binom{n}{0}x^0 + \binom{n}{1}x^1 + \cdots + \binom{n}{n-1}x^{n-1}\binom{n}{n}x^n \\ &= \sum_{j=0}^{n}\binom{n}{j}x^j\end{aligned}$$

Dizemos que $(1+x)^n$ é a *função geradora* de $\binom{n}{k}$, uma vez que $(1+n)^n$ descreve completamente os valores de $\binom{m}{k}$. Note que não demos atenção ao valor de $(1+x)^n$, mas apenas os coeficientes em sua expansão; e note também que a função geradora *determina completamente* a sequência de coeficientes. Neste Capítulo usaremos *séries formais de potencias*. Estas são semelhantes a polinômios, mas podem ter infinitos termos, e usualmente as tratamos como objetos algébricos – elementos que somamos e multiplicamos dentro de uma estrutura algébrica – e não como funções.

Definição 13.1 (série formal de potências)**.** Seja R um anel comutativo. Então uma **série formal de potencias** na variável x sobre R é um objeto da forma

$$\sum_{j\geq 0} a_j x^j,$$

onde $a_j \in R$.

As séries formais de potências onde os coeficientes pertencem a R e a variável é x formam um anel, denotado $R[[x]]$. ♦

Definição 13.2 (função geradora)**.** Seja $(a_n) = a_1, a_2, a_3, \ldots$ uma sequên-

cia infinita de inteiros. Então a série formal de potências

$$\sum_{j=0}^{\infty} a_j x^j$$

é a **função geradora** da sequência (a_n). ♦

Por exemplo,

$$\frac{1}{1-x}$$

é função geradora da sequência $(1, 1, 1, \ldots)$: note que

$$\lim_{k\to\infty} \sum_{j=0}^{k} x^j = \frac{1}{1-x},$$

e os coeficientes na soma ($\sum x^j$) são todos iguais a um.

Para um segundo exemplo, a sequência $(2, 1+1/2, 1+1/3, \ldots, 1+1/k, \ldots)$ tem como função geradora

$$-\ln(1-x),$$

já que

$$\lim_{m\to\infty} \sum_{j=0}^{m} \left(1 + \frac{1}{j}\right) x^j = -\ln(1-x).$$

13.2 Partições

Definição 13.3 (partição de um inteiro)**.** Uma **partição** de um inteiro positivo n é uma representação de n como soma de outros inteiros positivos. Definimos que o número zero tem somente uma partição, vazia. ♦

Por exemplo, as partições de 4 são

$$\begin{aligned} 4 &= 1 + 1 + 1 + 1 \\ &= 2 + 1 + 1 \\ &= 2 + 2 \\ &= 3 + 1 \\ &= 4. \end{aligned}$$

Definição 13.4 ($p(n)$, quantidade de partições)**.** Denotamos por $p(n)$ a quantidade total de partições do inteiro n. Definimos que $p(n) = 0$ se $n < 0$. ♦

Note que a Definição 13.3 implica que $p(0) = 1$.

Definição 13.5 (representação gráfica de partições, diagrama de Ferrers)**.** Cada partição de um inteiro pode ser representado por um **diagrama Ferrers**, onde cada parte é representada por uma linha, e em cada linha ficam dispostas marcas (pontos) na quantidade igual à parte. ⧫

Uma das partições de sete é $7 = 4 + 2 + 1$. O diagrama de Ferrers desta partição é

$$\begin{array}{cccc} \circ & \circ & \circ & \circ \\ \circ & \circ & & \\ \circ & & & \end{array}$$

Teorema 13.6. *Para todo* n *inteiro positivo,* $p(S_{\leq m}, n) = P(S_{\#m}, n)$.

Demonstração. Há uma bijeção entre partições e partições conjugadas: para cada partição com no máximo m partes, há exatamente uma conjugada com partes não maiores que m – basta observer a representação gráfica das partições. □

Teorema 13.7.

$$p_1(\hat{\mathbb{N}}, n) - p_2(\hat{\mathbb{N}}, n) = \begin{cases} (-1)^s & n = s\frac{(3s\pm1)}{2} \\ 0 & \textit{caso contrário.} \end{cases}$$

Teorema 13.8. *Para todo* n *inteiro positivo,* $p(\hat{1}, n) = p(\hat{\mathbb{N}}_1, n)$.

É interessante estudar duas demonstrações diferentes deste Teorema.

Demonstração. Suponha que uma partição de um número n tenha apenas partes ímpares. Então

$$n = 1 + \ldots + 1 + 3 + \ldots + 3 + \ldots + (2k+1) + \ldots + (2k+1). \tag{13.1}$$

$$n = 1(s_1) + 3(s_2) + \ldots + (2k+1)(s_{2k+1})$$

Cada um dos termos pode ser representado em base dois, *e como nesta partição só há partes ímpares, o número dois não aparece em qualquer das partes, de forma que as representações em base 2 são distintas e não tem fatores em comum.*

$$n = (1)2^{r_1} + (3)2^{r_2} + \ldots + 2k + 1(s^{r_{2k+1}}). \tag{13.2}$$

Então, para cada partição contendo partes ímpares, existe uma partição com partes distintas.

Observamos que toda partição tem parte distintas, quando posta na base 2 ficará na forma da Equação 13.2, e poderá ser transformada, revertendo os passos, em partição com partes ímpares, como na Equação 13.1 □

Teorema 13.9. *Sejam n um inteiro positivo e $S \in \mathbb{N}$. Então*

$$\sum_{n=0}^{\infty} p(\hat{S}, n)x^n = \prod_{n \in S} \frac{1}{1-x^n}.$$

Demonstração. A série geométrica $a + ax + ax^2 + ax^3 + \cdots$, quando $|x| < 1$, converge para o valor

$$\frac{a}{1-r},$$

portanto, usando $r = x^n$,

$$\begin{aligned}
\prod_{n \in S} \frac{1}{1-x^n} &= \prod_{n \in S} \left((x^n)^0 + (x^n)^1 + (x^n)^2 + (x^n)^3 + \dots\right) \\
&= \prod_{n \in S} \left(1 + x^n + x^{2n} + x^{3n} + \dots\right) \\
&= \sum_{(k_1, \dots, k_j) \in \mathbb{Z}^j} x^{s_1 k_1 + \dots + s_j k_j},
\end{aligned}$$

onde $S = \{s_1, s_2, \dots, s_j\}$.

O número de vezes que x^n aparece no somatório é o número de soluções distintas para

$$n = s_1 k_1 + \dots + s_j k_j, \tag{13.3}$$

sendo cada solução uma partição de n em $\hat{S}$. Tendo definido uma bijeção entre as soluções da equação 13.3 e as partições de cada n em $\hat{S}$, temos finalmente

$$\sum_{n=0}^{\infty} p(\hat{S}, n)x^n = \prod_{n \in S} \frac{1}{1-x^n}. \tag{13.4}$$

Falta, para completar a demonstração, tratar da convergência dos dois lados da igualdade.

No lado esquerdo da equação 13.4, a soma $\sum_{n=0}^{\infty} p(\hat{S}, n)x^n$ converge:

$$\begin{aligned}
\sum_{n=0}^{s_p} p(\hat{S}, n)x^n &\leq \prod_{i=1}^{p} \frac{1}{1-x^{s_i}} \\
&< \prod_{i=1}^{\infty} \frac{1}{1-x^i}
\end{aligned}$$

E o último produto converge.

No lado direito da equação 13.4, $\left(1 + x^n + x^{2n} + x^{3n} + \dots\right)$ é convergente quando $|x| < 1$, e $\prod_{n \in S} \left(1 + x^n + x^{2n} + x^{3n} + \dots\right)$ é, portanto, produto finito de séries convergentes.

Veja também que

$$\lim_{m\to\infty}\prod_{i=1}^{p}\frac{1}{1-x^{s_i}}=\prod_{i=1}^{\infty}\frac{1}{1-x^i}$$

e

$$\sum_{n=0}^{\infty}p(\hat{S},n)x^n\geq\prod_{i=1}^{p}\frac{1}{1-x^{s_i}}.$$ □

13.3 Crescimento de $p(n)$

Teorema 13.10. *Para todo inteiro positivo* n*,*

$$s^{\lfloor\sqrt{n}\rfloor}<p(n)<e^{\pi\sqrt{\frac{2n}{3}}}.$$

13.4 Exercícios

Ex. 261 — Prove que a quantidade de partições auto-conjugadas de um inteiro positivo n é igual à quantidade de partições com partes ímpares distintas desse mesmo inteiro.

Ex. 262 — Mostre algum $\hat{S}$ tal que $p(\hat{S},n)$ seja igual à quantidade de partições onde a distância entre cada duas partes é no mínimo 3, ou prove que não existe um $\hat{S}$ com esta propriedade.

Capítulo 14

Frações Contínuas

No Capítulo 2 realizamos a construção conceitual dos números naturais, inteiros e racionais. Os racionais, no entanto, não são suficientes sequer para a simples descrição de grandezas físicas fundamentais. Tome por exemplo a medida da diagonal de um quadrado de lado unitário – seu valor, $\sqrt{2}$, não é racional; outro exemplo simples está na razão entre perímetro e o diâmetro de qualquer círculo, π, que também não é racional. Faz-se necessário, portanto, definir rigorosamente um conjunto de números mais amplo que os racionais (e ao definir um novo conjunto, definimos sobre ele as operações de soma e multiplicação, obtendo assim uma nova estrutura algébrica). Trataremos de frações contínuas, números definidos como frações recursivas, e com elas obteremos umnovo modelo para os racionais, identificaremos os irracionais e construiremos um modelo para os reais.

Frações contínuas tem importância maior que a de uma simples ferramenta para mais uma construção dos reais[1]. Elas tem interessantes aplicações, e examinaremos algumas delas.

14.1 Frações Contínuas Finitas e Números Racionais

Revemos mais uma vez a seguir os passos do algoritmo de Euclides para cálculo do MDC. Desta vez, mudamos a notação: denotamos os restos por

[1] Há mais de vinte maneiras de construir $\mathbb{R}$.

x_i e os quocientes por y_i.

$$\begin{aligned} x_0 &= y_1 x_1 + x_2 && (x_0 \div x_1 = y_1, \text{ resto } x_2) \\ x_1 &= y_2 x_2 + x_3 \\ &\vdots \\ x_{n-1} &= y_n x_n \ (+0) \end{aligned}$$

No desenvolvimento do algoritmo estendido de Euclides, nosso foco de interesse eram os restos – isolamos as variáveis que representam os restos para descrever o último resto como função dos dois números iniciais. Agora nos interessam os quocientes y_i.

$$y_i = \frac{x_{i-1}}{x_i} - \frac{x_{i+1}}{x_i}$$

Definimos

$$q_i = \frac{x_i}{x_{i+1}}$$

E obtemos

$$q_i = y_i + \frac{1}{q_{i+1}}$$

Então

$$\begin{aligned} q_0 &= y_0 + \frac{1}{q_{i+1}} \\ &= y_0 + \cfrac{1}{y_1 + \cfrac{1}{q_2}} \\ &\vdots \\ &= y_0 + \cfrac{1}{y_1 + \cfrac{1}{y_2 + \quad \ddots \quad + \cfrac{1}{y_n + \cfrac{1}{y_{n+1}}}}} \end{aligned}$$

Por exemplo, se calcularmos $\mathrm{MDC}(111, 495)$,

$$\begin{aligned} 495 &= 4(111) + 51 \\ 111 &= 2(51) + 9 \\ 51 &= 5(9) + 6 \\ 9 &= 1(6) + 3 \\ 6 &= 2(3) + 0 \end{aligned}$$

teremos da primeira linha que

$$\frac{495}{111} = 4 + \frac{51}{111},$$

obtendo assim a parte inteira da fração. Se fizermos o mesmo com $51/111$, e assim sucessivamente, chegaremos a

$$\frac{495}{111} = 4 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

Esta é uma representação do racional $495/111$ na forma de fração contínua.

Definição 14.1 (fração contínua)**.** Uma **fração contínua finita** é uma expressão da forma

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \quad \ddots \quad + \cfrac{1}{x_n}}}$$

também denotada $[x_0; x_1, x_2, \ldots, x_n]$. Os x_i são os **coeficientes parciais** da fração contínua.

Se x_i é inteiro quando $i > 0$, dizemos que a fração contínua é **simples**. ♦

Frações contínuas finitas representam números racionais: expandimos $495/111$, por exemplo, até chegar a uma fração contínua. Fazemos agora o oposto: a partir de $[4; 1, 5, 4]$ obtemos um racional.

$$[4; 1, 5, 4] = 4 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{4}}} = \frac{121}{25}.$$

Teorema 14.2. *Toda fração contínua finita representa um número racional.*

Demonstração. Segue claramente da maneira como frações contínuas finitas são definidas – apenas soma e divisão são usadas, e estas operações são fechadas em $\mathbb{Q}$. □

Teorema 14.3. *Todo racional pode ser representado por frações contínuas finitas*

Demonstração. Executamos o algoritmo de Euclides com o racional a/b, e obteremos sua expansão em fração contínua. Como o algoritmo de Euclides sempre para, a expansão em fração contínua sempre será finita. □

Mesmo racionais que tem representação infinita em base dez (como $1/3 = 0.3333\ldots$, por exemplo) tem representação finita como fração contínua.

Nos falta investigar a unicidade da representação de racionais como frações contínuas. Interessantemente, a representação de racionais como frações contínuas não é única: há *exatamente* duas expansões para cada racional, mas isto já nos serve. Por exemplo,

$$[1;1,5] = 1 + \cfrac{1}{1 + \cfrac{1}{5}}, \qquad [1;1,4,1] = 1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1}}},$$

e ambas são evidentemente iguais (as duas valem $11/6$).

O Lema 14.4 mostra que é trivial determinar o inverso de uma fração contínua; ele será útil logo mais na demonstração da unicidade da representação.

Lema 14.4. *Se* $p > q$*, e* $p/q = [x_0;x_1,x_2,\ldots,x_n]$*, então o inverso* q/p *é* $[0;x_0,x_1,x_2,\ldots,x_n]$.

Demonstração.

$$\begin{aligned}
\frac{q}{p} &= \frac{1}{p/q} \\
&= \frac{1}{[x_0;x_1,x_2,\ldots,x_n]} \\
&= \cfrac{1}{x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \quad \ddots \quad + \cfrac{1}{x_n}}}} \\
&= [0;x_0,x_1,x_2,\ldots,x_n]
\end{aligned}$$

□

Já podemos afirmar que um racional só pode ser representado por uma única fração contínua (com último quociente diferente de um).

Lema 14.5. *Se duas frações contínuas simples* $[x_0; x_1, x_2, \ldots, x_r]$ *e* $[y_0; y_1, y_2, \ldots, y_s]$ *representam o mesmo número racional com* $x_r \neq 1$ *e* $y_s \neq 1$*, então* $r = s$ *e* $x_i = y_i$ *para todo* $0 \leq i \leq r$*.*

É importante que tenhamos definido que $x_r \neq 1$ e $y_s \neq 1$, porque já sabemos que com o último quociente parcial igual a um teríamos uma representação extra de cada número.

Demonstração. Suponha que $a = [x_0; x_1, x_2, \ldots, x_r] = [y_0; y_1, y_2, \ldots, y_s]$. Observe que

$$a = x_0 + [0; x_1, x_2, \ldots, x_r]$$

e também que

$$[0; x_1, x_2, \ldots, x_r] = \cfrac{1}{x_1 + \cfrac{1}{x_2 + \quad \ddots \quad + \cfrac{1}{x_r}}}$$

Como $x_i \geq 1$, o denominador é positivo e $0 < [0; x_1, x_2, \ldots, x_r] < 1$. Assim, $x_0 = \lfloor a \rfloor$. Como o mesmo vale para y_0, vemos que

$$\lfloor a \rfloor = x_0 = y_0,$$

e só precisamos mostrar que $[0; x_1, x_2, \ldots, x_r] = [0; y_1, y_2, \ldots, y_s]$.

Agora, pelo Lema 14.4

$$[0; x_1, x_2, \ldots, x_r]^{-1} = [x_1; x_2, \ldots, x_r],$$
$$[0; y_1, y_2, \ldots, y_s]^{-1} = [y_1; y_2, \ldots, y_s],$$

e pelo mesmo argumento de antes, $x_1 = y_1$. Podemos verificar portanto que, por indução, teremos $x_i = y_i$ para todo i.

Quanto a r e s, claramente, se todo x_i for igual a todo y_i, suponha que $r > s$. Teríamos

$$[x_0; x_1, \ldots x_r, x_{r+1}] = [y_0; y_1, \ldots y_r, x_{r+1}] < a. \qquad \square$$

Terminamos as demonstrações dos Lemas, e finalmente enunciamos o Teorema da unicidade das representações.

Teorema 14.6. *Há exatamente duas representações de cada racional como fração contínua finita simples; e uma representação de cada racional como fração contínua finita simples com último coeficiente diferente de um.*

Demonstração. Uma fração contínua não pode representar mais que um racional, portanto basta mostrar que um racional não pode ser representado por mais que duas frações contínuas, que é o que o Lema 14.5 afirma. □

14.2 Frações Contínuas Infinitas e Números Irracionais

No início do Capítulo dissemos que os racionais tem uma limitação que os torna insuficientes para medidas simples: há números que queremos representar, mas que não é possível expressar como razão entre dois inteiros.

Um exemplo de extrema simplicidade é $\sqrt{2}$, solução de $x^2 = 2$ e medida da diagonal do quadrado unitário. Sua expansão em fração contínua pode ser obtida facilmente:

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1) \\
&= 1 + \frac{1}{1+\sqrt{2}} \\
&= 1 + \frac{1}{1 + \left(1 + \frac{1}{1+\sqrt{2}}\right)} \\
&= 1 + \frac{1}{2 + \frac{1}{2+\sqrt{2}}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}
\end{aligned}$$

Notamos que a expansão é infinita: $\sqrt{2} = [1; 2, 2, 2, \ldots]$. É interessante que como mostramos que uma fração contínua infinita representa $\sqrt{2}$, e já havíamos demonstrado que racionais sempre tem representação finita como frações contínuas, o que temos é uma prova de que $\sqrt{2}$ é irracional. Precisamos portanto definir frações contínuas infinitas, e verificar o que elas representam e o que podemos concluir a respeito desses números.

Definição 14.7 (fração contínua infinita)**.** Uma fração contínua é **infinita** se tem infinitos quocientes parciais. ⧫

Por exemplo,

$$\begin{aligned} e &= [2;1,2,1,1,4,1,1,6,1,1,8,\ldots] \\ \pi &= [3;7,15,1,292,1,1,1,2,1,3,1,14,\ldots] \\ \phi &= [1;1,1,1,1,1,1,1,1,\ldots] \\ \sqrt{2} &= [1;2,2,2,2,2,2,2,2,\ldots] \\ \sqrt{3} &= [1;1,2,1,2,1,2,1,2,\ldots] \end{aligned}$$

A representação de alguns números como frações contínuas infinitas são aparentemente aleatóreas, como a de π; outras claramente apresentam padrões, como as de e, ϕ, $\sqrt{2}$ e $\sqrt{3}$. Um caso particular de número irracional que apresenta um claríssimo padrão em representação decimal é a *constante de Champernowne*, que é construída concatenando os números naturais,

$$C = 0,1234567891011121314\cdots,$$

cuja representação em frações contínuas é

$$C = [0;8,9,1,149083,1,1,1,4,1,1,1,3,4,1,1,1,15,\omega,6,1,1\ldots],$$

sem padrão aparente na sequência de coeficientes (o número ω tem 166 dígitos em representação decimal[2]).

14.2.1 Convergentes

Neste texto iniciamos com um semianel ($\mathbb{N}$) e aos poucos o aumentamos para obter estruturas mais úteis: o anel $\mathbb{Z}$ e o corpo $\mathbb{Q}$ (nesse caminho passamos brevemente pelo anel sem ordem dos inteiros Gaussianos).

Há diversos números que queremos representar, mas que não estão no corpo ordenado $\mathbb{Q}$: a diagonal do quadrado de lado um; a razão entre comprimento e diâmetro de uma circunferencia, e diversos outros. Estes são números que identificamos inicialmente por *aproximações sucessivas* – sequências de racionais que aos poucos se aproximam de algum número, que no entanto não é racional (não pode ser expresso como razão de dois inteiros). Inicialmente estudamos o que acontece quando truncamos frações contínuas: tratamos dos seus *convergentes*.

Definição 14.8 (convergente)**.** Seja $\alpha = [a_0;a_1,a_2,\ldots]$ um número irracional. Uma fração contínua $[a_0;a_1,a_2,\ldots,a_k]$ é chamada de **convergente** de α. Denotamos o i-ésimo convergente da fração contínua $[a_0;a_1,\ldots]$ por p_i/q_i, ou ainda, por $\alpha^{(i)}$. ♦

[2] $\omega = 4\,575\,401\,113\,910\,310\,764\,836\,466\,282\,429\,561\,185\,996\,039\,397\,104\,575\,550\,006\,620\,043\,930\,902\,626\,592\,563\,149\,379\,532\,077\,471\,286\,563\,138\,641\,209\,375\,503\,552\,094\,607\,183\,089\,984\,575\,801\,469\,863\,148\,833\,592\,141\,783\,010\,987$.

Por exemplo, os primeiros convergentes de $\sqrt{2}$ são

$$\begin{aligned}
p_0/q_0 &= [1] = 1 \\
p_1/q_1 &= [1;2] = 1 + \frac{1}{2} = \frac{3}{2} = 1.5 \\
p_2/q_2 &= [1;2,2] = 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5} = 1.4 \\
p_3/q_3 &= [1;2,2,2] = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{17}{12} = 1.416666\ldots \\
p_4/q_4 &= [1;2,2,2,2] = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = \frac{41}{29} = 1.413793\ldots
\end{aligned}$$

A sequencia não é crescente nem decrescente.

Teorema 14.9. *Se* $a = [a_0; a_1, a_2, \ldots]$ *então os convergentes* p_i/q_i *de* a *são*

$$\begin{aligned}
p_i &= a_i p_{i-1} + p_{i-2} \\
q_i &= a_i q_{i-1} + q_{i-2}
\end{aligned}$$

com

$$\begin{aligned}
p_0 &= a_0 & q_0 &= 1 \\
p_{-1} &= 1 & q_{-1} &= 0.
\end{aligned}$$

Ou ainda, em notação matricial,

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix}$$

A demonstração pode ser feita por indução no índice do convergente (i).

Corolário 14.10.

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$$

Demonstração. Segue trivialmente, já que

$$\det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = -1. \qquad \square$$

Corolário 14.11. *Para qualquer* $i \geq 0$, $\operatorname{mdc}(p_i, q_i) = 1$.

Demonstração. $p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$, logo qualquer divisor comum de p_i e q_i é divisor de ± 1. □

Teorema 14.12. *Seja* $1 < a \in \mathbb{R}$. *Então*

$$[x_0; \ldots, x_{k-1}, a] = \frac{a p_{k-1} + p_{k-2}}{a q_{k-1} + q_{k-2}}$$

Demonstração. Por indução em k. Para a base, seja $k = 1$. Então, usando os valores de p_0, q_0, p_1, q_1 no Teorema 14.9,

$$\begin{aligned} \frac{a p_{k-1} + p_{k-2}}{a q_{k-1} + q_{k-2}} &= \frac{a x_0 + 1}{a(1) + 0} \\ &= x_0 + \frac{1}{a} \\ &= [x_0; a]. \end{aligned}$$

Para o passo, presuma que

$$[x_0; \ldots, x_{k-1}, a] = \frac{a p_{k-1} + p_{k-2}}{a q_{k-1} + q_{k-2}}$$

Então,

$$\begin{aligned} [x_0; \ldots, x_k, a] &= [x_0; \ldots, x_{k-1}, x_k + 1/a] \\ &= \frac{(x_k + 1/a) p_{k-1} + p_{k-2}}{(x_k + 1/a) q_{k-1} + q_{k-2}} \\ &= \frac{a p_k + q_{k-1}}{a q_k + q_{k-1}}. \end{aligned}$$

□

Teorema 14.13. *Para qualquer fração contínua simples,*

$$\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{(-1)^{i+1}}{q_i q_{i+1}}$$

Demonstração. O Corolário 14.10 determina que

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}.$$

Dividindo a equação por $q_i q_{i-1}$, chegamos ao enunciado. □

Teorema 14.14. *Para qualquer fração contínua infinita simples com convergentes* p_i/q_i,

$$\left| \frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} \right| \leq \frac{1}{2^i},$$

e a sequência é convergente.

Demonstração. Denote por F_i o i-ésimo número de Fibonacci. Como $q_i \geq F_i$, então $q_i q_{i+1} \geq F_i F_{i+1} \geq 2^i$, e

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} \leq \frac{(-1)^i}{2^i},$$

donde se conclui que a sequência $(a)_i$ converge, já que 2^{-i} chega arbitrariamente próximo de zero. □

Teorema 14.15. *A sequência de convergentes de índice par é estritamente crescente; a sequencia de convergentes com índice ímpar é estritamente decrescente:*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots$$
$$\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots$$

Definição 14.16 (valor de fração contínua simples infinita)**.** Dizemos que o **valor** de uma fração contínua simples infinita com convergentes p_i/q_i é

$$\lim_{i\to\infty} \frac{p_i}{q_i},$$

que pelo Teorema 14.14 sempre existe. ♦

Teorema 14.17. *Seja $x = [x_0; x_1, \dots]$ uma fração contínua simples infinita (x é o valor da fração contínua, como na definição 14.16). Seja r_k definido indutivamente, de forma que*

$$r_0 = \lfloor x \rfloor$$
$$x = r_0 + \frac{1}{r_1}$$
$$r_i = \lfloor r_i \rfloor + \frac{1}{r_{i+1}}$$

Então

$$x = [x_0; x_1, \dots, x_{k-1}, r_k]$$

Demonstração. Segue de maneira simples por indução em k. □

Teorema 14.18. *Para qualquer fração contínua infinita simples com convergentes p_i/q_i e valor x,*

$$\left| x - \frac{p_i}{q_i} \right| < \frac{1}{2q_i^2}.$$

Teorema 14.19. *Seja x um número irracional, de forma que*

$$x = [\xi_0; \xi_1; \dots, \xi_{k-1}, x_k]$$

Então

$$x = \frac{x_k p_i + p_{i-1}}{x_k q_i + q_{i-1}}.$$

Demonstração. Segue facilmente por indução. □

Tendo demonstrado que toda fração contínua infinita converge, nos falta verificar que, partindo de um irracional, chegaremos na mesma fração contínua. Isto é garantido pelo Teorema 14.20.

Teorema 14.20. *Seja x um número irracional, cuja expansão em fração contínua tem convergentes p_i/q_i. Então*

$$x = \lim_{i\to\infty} \frac{p_i}{q_i}$$

Demonstração. Segue dos Teoremas 14.17 e 14.15, e da Definição 14.16. □

Teorema 14.21. *Duas frações contínuas infinitas simples diferentes não podem convergir para o mesmo valor.*

Se $x = [x_0; x_1, \ldots] = [y_0; y_1, \ldots]$, então $x_0 = y_0 = \lfloor x \rfloor$. Indutivamente, o mesmo vale para todos os outros coeficientes ($x_i = y_i$), e as duas frações parciais são idênticas.

14.3 Melhor aproximação

O estudo de convergentes nos permite determinar algo mais sobre frações contínuas: os convergentes são, em certo sentido, a melhor maneira possível de aproximar um número irracional. Aqui, definimos "melhor" como "tendo o menor denominador possível". A ideia é tentar obter a fração contínua mais curta possível que aproxime o número por no máximo uma dada distância.

Definição 14.22 (melhor aproximação)**.** Dizemos que a/b é a **melhor aproximação** de um número x se

$$|qx - p| < |bx - a|$$

implica que $q > b$. ⧫

Lema 14.23. *Se a/b é melhor aproximação para um número x, então*

$$\left|x - \frac{p}{q}\right| < \left|x - \frac{a}{b}\right|$$

implica que $q > b$.

Embora possa parecer que as duas afirmações são equivalentes, não é o caso, e a recíproca não vale (um contraexemplo é pedido no Exercício 274)

Demonstração. Suponha que o enunciado não valha. Então

$$\left|x - \frac{p}{q}\right| < \left|x - \frac{a}{b}\right|$$
$$q < b$$

Multiplicando a primeira desiguladade pela segunda (ou seja, multiplicando o lado esquerdo da primeira desigualdade por q e o lad odireito por b),

$$|qx - p| < |bx - a|.$$

E a/b não seria melhor aproximação, porque p/q seria melhor. □

Teorema 14.24. *Os convergentes p_i/q_i da fração contínua de qualquer $x \in \mathbb{R}$ são uma sequência de melhores aproximações para x.*

Demonstração. Como $q_{i+1} > q_i$, concluímos que $q_{i+1} \geq 2$. Sabemos que

$$\left|x - \frac{p_i}{q_i}\right| < \frac{1}{2q_i^2}.$$

Agora suponha que p/q seja melhor aproximação. com $q < q_i$.

$$\begin{aligned}
\left|\frac{p}{q} - \frac{p_i}{q_i}\right| &\leq \left|\frac{p}{q} - x\right| + \left|x - \frac{p_i}{q_i}\right| && \text{(desigualdade de triângulo)} \\
&\leq 2\left|x - \frac{p_i}{q_i}\right| && (p/q \text{ mais próximo de } x \text{ – Lema 14.23}) \\
&< \frac{1}{q_i^2}.
\end{aligned}$$

No entanto,

$$\left|\frac{p}{q} - \frac{p_i}{q_i}\right| = \left|\frac{pq_i - p_i q}{q_i q}\right| > \frac{1}{q_i q} \geq \frac{1}{q_i^2}.$$

Como chegamos a uma contradição, a suposição de que p/q existe é falsa. □

Teorema 14.25. *Se a/b é uma melhor proximação para um número x, então a/b é convergente na expansão de x em fração contínua.*

Demonstração. Suponha que a/b seja melhor aproximação para x. Analisamos três casos, (i) $a/b < x_0$; (ii) a/b fica entre dois convergentes, x_{i-1}, x_{i+1}, e (iii) $a/b > p_1/q_1$.

(i) É impossível que $a/b < a_0$, porque se assim fosse, 1 seria melhor aproximação do que a/b:

$$|(1)x - x_0| < \left|x - \frac{a}{b}\right| \leq |bx - x|. \qquad (1 \leq b)$$

(ii) Se a/b está entre dois convergentes, então

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| = \left|\frac{aq_{k-1} - bp_{k-1}}{bq_{k-1}}\right| \geq \frac{1}{bq_{k-1}}$$
$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}$$

o que determina, claramente, que

$$q_k < b.$$

Mostramos que $q_k < b$ porque queremos mostrar que p_k/q_k seria melhor aproximação do que a/b.

Continuamos, observando que

$$\left|x - \frac{a}{b}\right| \geq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right|$$
$$\geq \frac{1}{bq_{k+1}}$$

Multiplicando a desigualdade por b,

$$|bx - a| \geq \frac{1}{q_{k+1}},$$

Mas já temos estabelecido que

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}$$
$$|q_k x - p_k| \leq \frac{1}{q_{k+1}},$$

então

$$|q_k x - p_k| \leq |bx - a|,$$

e a/b não pode ser melhor aproximação, porque $p_k q_k$ é melhor.

(iii) Se $a/b > p_1/q_1$, então a distância de x até a/b é maior do que até p_1/q_1:

$$\left|x - \frac{a}{b}\right| > \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geq \frac{1}{bq_1}$$

Então, multiplicando por b,

$$|bx - a| > \frac{1}{q_1} = \frac{1}{x_1}$$

Pode-se verificar faclimente que

$$|(1)x - x_0| \leq \frac{1}{x_1},$$

Mas neste caso 1 seria melhor aproximação do que a/b:

$$|bx - a| > |(1)x - x_0| \qquad (1 \leq b)$$

Nos três casos chegamos a contradições, portanto a/b precisa ser um dos convergentes na expansão de x. □

Teorema 14.26 (de Hurwitz)**.** *Na expansão em fração contínua de qualquer número irracional x, pelo menos um a cada três convergentes p/q são tais que*

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2\sqrt{5}}.$$

14.4 Frações Contínuas Periódicas

Há frações contínuas que apresentam padrões recorrentes. Por exemplo, em $[1; 1, 2, 1, 2, \dots]$ o padrão "$1, 2$" se repete indefinidamente. Os números com expansão em frações contínuas contendo estes padrões são exatamente as soluções irracionais para equações quadráticas.

Definição 14.27. Uma fração contínua é **eventualmente periódica** se, para todo i maior que algum n, o quociente parcial x_i é igual a x_{i_t}, onde t é o período.

Denotamos por $[x_0; x_1; x_2, \dots, \overline{x_n, \dots, x_{n+t}}]$ a fração contínua eventualmente periódica, onde o período é $x_n, \dots, x_{n_t}$. ♦

Assim, $[1; \overline{1, 2}]$ denota a fração contínua que mencionamos no primeiro parágrafo desta seção, em que o padrão "$1, 2$" é repetido infinitas vezes.

Definição 14.28 (irracional quadrático)**.** Um **irracional quadrático** é uma solução irracional para uma equação quadrática. ♦

Um exemplo de irracional quadrático é $\sqrt{2}$, cuja expansão, $[1; \overline{2}]$, já derivamos na Seção 14.2.

Como outro exemplo, a solução de $x^2 - x - 1 = 0$ é a razão áurea, ϕ, com expansão em fração contínua igual a $[1; \overline{1}]$

Teorema 14.29. *Toda fração contínua eventualmente periódica representa um irracional quadrático.*

Demonstração. Seja

$$x = [\xi_0; \xi_1, \ldots, \overline{\xi_k \ldots, \xi_n}]$$

Escrevemos somente a parte periódica, e chegamos a

$$\begin{aligned} x_k &= [\xi_k; \ldots, \xi_n, x_k] \\ x_k &= \frac{x_k p_n + p_{n-1}}{x_k q_n + q_{n-1}} \end{aligned}$$

Esta última equação é claramente quadrática em x_k. Temos agora $x = [x_0; x_1; \ldots, x_k]$, onde x_k é da forma $(\alpha + \sqrt{\beta})/\gamma$, e pode-se facilmente verificar que x também deve necessariamente ser dessa forma. □

Teorema 14.30. *A expansão em fração contínua de qualquer irracional quadrático é eventualmente periódica.*

Demonstração. Seja $[\xi_0; \xi_1, \ldots]$ a expansão de x em fração contínua, e $x_k = [\xi_k; \xi_{k+1}, \ldots]$. Suponha que x é raiz de uma equação quadrática, ax^2+bx+c. Então, pelo Teorema 14.19,

$$x = \frac{x_k p_{k-1} + p_{k-1}}{x_k q_{k-1} - q_{k-2}},$$

e

$$a\left(\frac{x_k p_{k-1} + p_{k-1}}{x_k q_{k-1} - q_{k-2}}\right)^2 + b\left(\frac{x_k p_{k-1} + p_{k-1}}{x_k q_{k-1} - q_{k-2}}\right) + c = 0$$

$$a(x_k p_{k-1} + p_{k-1})^2 + b(x_k p_{k-1} + p_{k-1})(x q_{k-1} - q_{k-2}) + c(x q_{k-1} - q_{k-2}) = 0$$

Uma mudança de variável transforma esta equação em

$$A_k x_k^2 + B_k x_k + C_k = 0,$$

com

$$\begin{aligned} A_k &= a p_{k-1}^2 + b p_{k-1} q_{k-1} + c q_{k-1}^2 \\ B_k &= 2a p_{k-1} p_{k-2} + b(p_{k-1} q_{k-2} + p_{k-2} q_{k-1}) + 2c q_k + q_{k-2} \\ C_k &= a p_{k-3}^2 + b p_{k-3} q_{k-3} + c q_{k-2}^2 \\ &= A_{k-1} \end{aligned}$$

Definimos, portanto, sequências de coeficientes A_k, B_k, C_k, que descrevem os convergentes de x.

O discriminante $\Delta_k = B_k^2 - 4A_kC_k$ é igual ao discriminante da forma original, $\Delta = b^2 - 4ac$, e não depende de k.

$$\left| x - \frac{p_i}{q_i} \right| < \frac{1}{2q_i^2}.$$

logo

$$p_{k-1} = xq_{k-1} + \frac{|z_{n-1}|}{q_{n-1}} \qquad (|z-1|<1)$$

Assim, A_k pode ser reescrito como

$$\begin{aligned} A_k &= a\left(xq_{k-1} + \frac{z_{k-1}}{q_{k-1}}\right)^2 + b\left(xq_{k-1} + \frac{z_{k-1}}{q_{k-1}}\right)q_{k-1} + cq_{k-1}^2 \\ &= \left(ax^2 + bx + c\right)q_{k-1}^2 + 2axz_{k-1} + a\frac{z_{k-1}}{q_{k-1}^1} + bz_{k-1} \\ &= 2axz_{k-1} + a\frac{z_{k-1}^2}{q_{k-1}^1} + bz_{k-1} \qquad (ax^2+bx+c=0) \end{aligned}$$

Então, como $|z_{k1}| < 1$,

$$|A_k| = \left| 2axz_{k-1} + a\frac{z_{k-1}^2}{q_{k-1}^2} + bz_{k-1} \right| < 2|ax| + |a| + |b|,$$

ou seja, $|A_k|$ é limitado por uma expressão que depende apenas de a, x e b, e portanto é consatnte (não depende de k). Como $C_k = A_{k-1}$, C_k também é limitado.

Como $\Delta_k = \Delta$ é constante e tanto A_k como B_k são limitados, então $B_k = \sqrt{\Delta - 4A_kC_k}$ também é limitado superiormente. Mais ainda – como A_k, B_k e C_k são inteiros, e as sequências são infinitas, pelo princípio da casa dos pombos, em algum momento haverá $A_k = A_{k+t}$, $B_k = B_{k+t}$ e $C_k = C_{k+t}$. E como o próximo elemento de cada sequência (A_k, B_k, C_k) depende somente dos anteriores, ela será eventualmente periódica. □

14.5 Construção de $\mathbb{R}$ com frações contínuas

Gostaríamos de incluir os números irracionais (que surgem em diversos problemas e mensurações físicas) no corpo que estamos usando, e isto é equivalente a incluir "o elemento para o qual convergem" estas aproximações a que demos o nome de convergentes.

Definição 14.31 (métrica; espaço métrico)**.** Uma **métrica** sobre um conjunto A é uma função $d : A \times A \to \mathbb{R}$, tal que para todos $x, y, z \in A$,

(i) $x(x, y) \geq 0$

(ii) $d(x,y) = 0$ se e somente se $x = y$

(iii) $d(x,y) = d(y,x)$

(iv) $d(x,z) \leq d(x,y) + d(y,z)$

Um conjunto onde se define uma métrica é chamado de **espaço métrico**. ♦

Definição 14.32 (sequência de Cauchy)**.** Uma **sequência** é **de Cauchy** em um espaço métrico se, para N suficientemente grande, todos os termos posteriores a N são arbitrariamente próximos entre si, usando a métrica daquele espaço. ♦

Exemplo 14.33. Em $\mathbb{Q}$, usando a métrica $d(a,b) = |a-b|$, a sequência $a_n = 2^{-n}$ é uma sequência de Cauchy. Dado qualquer $\varepsilon > 0$, existe N tal que para quaisquer $n, k > N$,

$$|a_n - a_k| < \varepsilon,$$

bastando tomar $N = -(\log_2(\varepsilon)) + 1$, de forma que $2^{-N+1} < \varepsilon$. Se $n, k > N$, então

$$\begin{aligned} |a_n - a_k| &= \left| \frac{1}{2^n} - \frac{1}{2^{-k}} \right| \\ &< \frac{1}{2^n} + \frac{1}{2^k} \\ &< \frac{1}{2^N} + \frac{1}{2^N} \\ &< \frac{1}{2^{N-1}} \\ &< \varepsilon. \end{aligned}$$ ◄

Exemplo 14.34. Em $\mathbb{Q}$, com a distância usual, as sequências $a_n = (-1)^n$ e $b_n = \sum_{j=1}^{n} 1/j$ não são de Cauchy, porque não convergem. ◄

Definição 14.35 (espaço métrico completo)**.** Um espaço métrico A é **completo** se toda sequência de Cauchy em A converge para algum elemento também em A. ♦

Os racionais com a métrica $d(x,y) = |x-y|$ são um espaço métrico que não é completo: a sequência de Cauchy

$$\begin{aligned} &[1] \\ &[1;2] \\ &[1;2;2] \\ &[1;2;2,2] \\ &\vdots \end{aligned}$$

não converge para um racional, porque sabemos que $[1;\overline{2}] = \sqrt{2} \notin \mathbb{Q}$.

A seguir mostramos que, partindo das frações contínuas finitas (que representam os racionais), podemos construir um modelo para os reais, incluindo no conjunto as frações contínuas infinitas. Com isso toda sequências de Cauchy convergirá para um elemento no conjunto. Obteremos um corpo ordenado que também é espaço métrico completo – e que chamaremos de *corpo ordenado compelto*.

Definimos um símbolo ω tal que $\omega > n$ para todo $n \in \mathbb{N}$, e assim podemos denotar todas as frações contínuas como infinitas,

$$[a_0; a_1, a_2, \ldots, a_n] \;\to\; [a_0; a_1, a_2, \ldots, a_n, \omega, \omega, \ldots],$$

desde que os coeficientes ω estejam sempre à direita de todos os outros.

Sejam $a \neq b$,

$$a = [a_0; a_1, a_2, \ldots],$$
$$b = [b_0; b_1, b_2, \ldots],$$

e $k = k(a, b)$. Claramente,

$$a < b \text{ se e somente se } \begin{cases} a_k < b_k & \text{se } 2 \mid k \\ a_k > b_k & \text{se } 2 \nmid k \end{cases}$$

Claramente, se $a < b$. então

$$a^{(2i)} < b^{(2i)}$$
$$a^{(2i+1)} < b^{(2i+1)}$$

O Teorema a seguir é de G. J. Rieger, que propôs a construção dos reais com frações contínuas:

Teorema 14.36. *Seja* K *o conjunto de todas as frações contínuas (finitas e infinitas). Se* $\emptyset \neq M \subset K$ *e* M *é limitado superiormente, então* M *tem supremo. Mais ainda – para toda fração contínua* a*,*

$$a = \sup \left\{ a^{(2i)} \;:\; i \geq 0 \right\}.$$

O Teorema 14.36 garante que toda sequência de Cauchy no conjunto das frações contínuas converge para uma fração contínua – temos portanto um espaço métrico completo.

A operação de soma e o inverso aditivo são definidos a seguir.

$$a + b = \sup\left\{a^{(2n)} + b^{(2n)} \ : \ n \geq 0\right\}$$
$$-a = \sup\left\{-a^{(2n+1)} \ : \ n \geq 0\right\}$$

Valor absoluto e multiplicação:

$$|a| = \sup\{a, -a\}$$
$$ab = \begin{cases} \sup\left\{a^{(2n)}b^{(2n)} \ : \ n \geq 0\right\} & a \geq 0, b \geq 0 \\ -(|a| \cdot b) & a < 0, b > 0 \\ -(a \cdot |b|) & a > 0, b < 0 \\ |a| \cdot |b| & a < 0, b < 0 \end{cases}$$

A definição de inverso – para que possamos operar divisões – é

$$a^{-1} = \begin{cases} \sup\left\{\frac{1}{a^{(2n+1)}} \ : \ n \geq 0\right\} & a > 0 \\ -|a|^{-1} & a < 0 \end{cases}$$

O Teorema 14.37 nos garante que o que construímos foi de fato o corpo dos números Reais.

Teorema 14.37. *Todos os corpos ordenados completos são isomorfos.*

14.6 e é irracional

Já mostramos a irracionalidade de ϕ e de $\sqrt{k}$, quando k não é quadrado perfeito. Tratamos agora de e. Esta seção traz uma demonstração, elaborada por Henry Cohn, de que a expansão de e em fração contínua é de fato $[2; 1, 2, 1, 1, 4, 1, 1, 6, \dots]$, e com isso ganhamos também a prova de que e é irracional, e de que não é quadrático (porque a sequencia não é periódica). Após esta, apresentamos outra demonstração, de Fourier, sem o uso de frações contínuas, e mais curta, mas que não leva à irracionalidade de e^2.

14.6.1 Demonstração de Cohn, com frações contínuas

Primeiro observe que

$$[1;0,1,1,2,1,1,4,1,1,6,1,1,8,\ldots,1,1,2n,\ldots] = 1 + \cfrac{1}{0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \ddots}}}},$$

é o mesmo que

$$[2;1,2,1,1,4,1,1,6,1,1,8,\ldots,1,1,2n,\ldots] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}},$$

A primeira fração periódica não segue o padrão que impusemos, porque tem um coeficiente zero, mas ela pode ser descrita mais facilmente por relações de recorrência – por isso demonstraremos que ela é a expansão de e em fração contínua.

Além disso, observe que há um padrão nos coeficientes: eles são descritos por uma relação de recorrencia de ordem 3: $e = [1;0,1,\ \ 1,2,1,\ \ 1,4,1,\ \ \ldots]$. logo os coeficientes são

$$\begin{aligned} a_{3_i} &= 1 \\ a_{3i+1} &= 2i \\ a_{3_i+2} &= 1 \end{aligned}$$

Observamos os convergentes da fração contínua

i	0	1	2	3	4	5	6	7	8	9
p_i	1	1	2	3	8	11	19	87	106	193
q_i	1	0	1	1	3	4	7	32	39	71

e os descrevermos também como relação de recorrência:

$$\begin{aligned} p_{3n} &= p_{3n-1} + p_{3n-2} & \qquad q_{3n} &= q_{3n-1} + q_{3n-2} \\ p_{3_n+1} &= 2np_{3n} + p_{3n-1} & \qquad q_{3n+1} &= 2nq_{3n} + q_{3n-1} \\ p_{3n+2} &= p_{3n+1} + p_{3n} & \qquad q_{3n+2} &= q_{3n+1} + q_{3n} \end{aligned}$$

Note que a sequência é descrita com três equações para p e três para q.

Quando demonstrarmos propriedades desta sequência, faremos uma afirmação para cada um dos três casos $(3n, 3n+1, 3n+2)$.

Agora definimos três sequências, A_k, B_k e C_k, cada uma definida por uma integral:

$$A_n = \int_0^1 \frac{x^n(x-1)^n}{n!} e^x dx$$
$$B_n = \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x dx$$
$$C_n = \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x dx$$

É fácil verificar que A_n, B_n e C_n tendem a zero quando $n \to \infty$.

Com o Lema 14.38 queremos identificar três sequências da forma $q_n e - p_n$, que mais adiante usaremos. Note que, como mencionamos anteriormente, separamos em casos $3n$, $3n+1$ e $3n+2$.

Lema 14.38. *Para todo n natural,*

$$A_n = q_{3n} e - p_{3n}$$
$$B_n = p_{3n+1} - q_{3n+1} e$$
$$C_n = p_{3n+2} - q_{3n+2} e$$

Demonstração. Só precisamos mostrar que valem as condições iniciais

$$A_0 = e - 1,$$
$$B_0 = 1,$$
$$C_0 = 2 - e,$$

e que

$$A_n = -B_{n-1} - C_{n-1} \tag{14.1}$$
$$B_n = -2nA_n + C_{n-1} \tag{14.2}$$
$$C_n = B_n - A_n \tag{14.3}$$

As condições iniciais podem ser verificadas observando que, substituindo $n = 0$ nas integrais, a relação de recorrência é satisfeita:

$$A_0 = q_{3(0)} e - p_{3(0)} = q_0 e - p_0 = e - 1$$
$$B_0 = p_{3(0)+1} - q_{3(0)+1} e = p_1 - q_1 e = 1$$
$$C_0 = p_{3(0)+2} - q_{3(0)+2} e = p_2 - q_2 e = 2 - e$$

Para mostrar que 14.1 vale, basta integrar os dois lados de

$$\frac{x^n(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n-1}}{(n-1)!}e^x + \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x = \frac{d}{dx}\left(\frac{x^n(x-1)^n}{n!}e^x\right).$$

Para 14.2, integre também os dois lados da equação:

$$\frac{x^{n+1}(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n-1}}{(n-1)!}e^x + \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x = \frac{d}{dx}\left(\frac{x^n(x-1)^{n+1}}{n!}e^x\right).$$

Já 14.3 pode ser verificada trivialmente. □

Teorema 14.39.

$$e = [1; 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, \ldots, 1, 1, 2n, \ldots]$$

Demonstração. Claramente, A_n, B_n e C_n tendem a zero quando $n \to \infty$. Observando o enunciado do Lema 14.38, isto significa que

$$\lim_{i\to\infty}(q_i e - p_i) = 0.$$

Como $q_i \geq 1$ e $i \geq 2$, temos

$$e = \lim_{i\to\infty}\frac{p_i}{q_i}.$$ □

Como a fração contínua de e é infinita, concluímos que e não é racional. A fração contínia de e também não é periódica, portanto e não é raiz de euqação quadrática, e concluímos que e^2 *também não é racional*.

14.6.2 Demonstração de Fourier, sem frações contínuas

A demonstração da irracionalidade de e com frações contínuas é interessante, e nos dá também a irracionalidade de e^2. agora apresentamos, para comparação, uma demonstração mais curta – dada por Joseph Fourier – da irracionalidade de e.

(Prova da irracionalidade de e, de Fourier). Partimos de

$$e = \sum_{k=0}^{\infty}\frac{1}{k!}.$$

Suponha que e seja racional: $e = p/q$, com $p, q \in \mathbb{N}$. Então

$$\begin{aligned} e = \frac{p}{q} &= \sum_{k=0}^{\infty} \frac{1}{k!} \\ q!\frac{p}{q} &= \sum_{k=0}^{\infty} \frac{q!}{k!} \\ (q-1)!p &= \sum_{k=0}^{\infty} \frac{q!}{k!} \\ &= \underbrace{\sum_{k=0}^{q} \frac{q!}{k!}}_{A} + \underbrace{\sum_{k=q+1}^{\infty} \frac{q!}{k!}}_{B}. \end{aligned}$$

O lado esquerdo, $(q-1)!p$, é inteiro, portanto o lado direito deve ser também. Mas A é claramente inteiro, porque

$$\begin{aligned} A &= \frac{q!}{1} + \frac{q!}{2} + \cdots \frac{q!}{q!} \\ &= q! + [3 \cdot 4 \cdot q] + \cdots + [(q-2)(q-1)q] + [(q-1) \cdot q] + 1. \end{aligned}$$

Assim, B deve também ser inteiro. Mas mostraremos que (i) $B > 0$, e (ii) $B < 1$, de forma que B não pode ser inteiro, levando a uma contradição.

Para (i), note que os termos de B são todos maiores que zero. Para (ii), basta calcular

$$\begin{aligned} B &= \sum_{k=q+1}^{\infty} \frac{q!}{k!} \\ &= \sum_{k=q+1}^{\infty} \frac{1}{(q+1)(q+1)\cdots k} \\ &< \sum_{k=q+1}^{\infty} \frac{1}{(q+1)^k} \\ &< \sum_{k=1}^{\infty} \frac{1}{(q+1)^k} \\ &= \frac{1}{q+1}\left(\frac{1}{1-\frac{1}{q+1}}\right) \\ &= \frac{1}{q} \\ &< 1. \end{aligned}$$

□

14.7 π é irracional

Uma vez que são conhecidos muitos dos primeiros dígitos de π, também conhecemos muitos dos primeiros coeficientes de sua expansão em fração contínua,

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \dots]$$

No entanto, não conhecemos forma fechada para estes coeficientes – o que é o mesmo que dizer que não conhecemos uma descrição completa da expansão de π em frações contínuas simples, *da forma como as definimos*. No entanto, há várias expansões de π em frações contínuas onde as regras de formação que impusemos são quebradas. Algumas delas são

$$\pi = \cfrac{4}{1+\cfrac{1^2}{3+\cfrac{2^2}{5+\cfrac{3^2}{7+\cfrac{4^2}{9+\ddots}}}}} \qquad \pi = \cfrac{4}{1+\cfrac{1^2}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{2+\ddots}}}}}$$

$$\pi = 3+\cfrac{1}{6+\cfrac{3^2}{6+\cfrac{5^2}{6+\cfrac{7^2}{6+\cfrac{9^2}{6+\ddots}}}}} \qquad \frac{\pi}{2} = 1+\cfrac{1}{1+\cfrac{1}{1/2+\cfrac{1}{1/3+\cfrac{1}{1/4+\ddots}}}}$$

Nesta seção não derivaremos uma fração contínua para π; ao invés disso, obteremos a expansão de $\tan(x)$ em fração contínua, e dela concluiremos que π^2 e π são irracionais – esta é em essência a mesma demonstração dada por Johann Lambert em 1761.

Lema 14.40. *Se*

$$x = \cfrac{a_1}{b_1+\cfrac{a_2}{b_2+\cfrac{a_3}{b_3+\cfrac{a_4}{b_4+\ddots}}}}$$

e, para i *maior que algum* N *suficientemente grande sempre for verdade que* $|a_i| < |b_i|$*, então* x *é irracional.*

Lema 14.41.

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \ddots}}}$$

Teorema 14.42. *π é irracional.*

Demonstração. Suponha que π é racional. Então π/4 também é:

$$\frac{\pi}{4} = \frac{a}{b}, \quad a, b \in \mathbb{Z}.$$

Substituimos π/4 por a/b na expansão em fração contínua de $\tan(\pi/4)$:

$$\tan\left(\frac{\pi}{4}\right) = \tan\left(\frac{a}{b}\right).$$

Como $\tan(\pi/4) = 1$, podemos igualar 1 à expansão em fração contínua de $\tan(a/b)$:

$$1 = \cfrac{\frac{a}{b}}{1 - \cfrac{\frac{a^2}{b^2}}{3 - \cfrac{\frac{a^2}{b^2}}{5 - \cfrac{\frac{a^2}{b^2}}{7 - \ddots}}}}$$

$$= \cfrac{a}{b - \cfrac{a^2}{3b - \cfrac{a^2}{5b - \cfrac{a^2}{7b - \ddots}}}}$$

Notamos que os a_i são constantes (são todos iguais a a^2), mas os b_i crescem, e eventualmente, $kb_i > a^2 + 1$. Isto significa que a expansão é irracional – o que é absurdo, já que este é o número um. □

Como π é a razão entre o comprimento e o diâmetro de qualquer circunferência, resulta que um dos dois (diâmetro ou circunferência) necessariamente será irracional. Ao traçar uma circunferência com raio (e diâmetro) racional, estamos desenhando uma linha de comprimento irracional!

14.8 ϕ é irracional

O valor ϕ, também chamado de *razão áurea*, é definido como segue. Para quaisquer números reais, a, b, com $a > b > 0$, se

$$\frac{a}{b} = \frac{a+b}{a}.$$

então $\phi = a/b$.

Isto implica que

$$\begin{aligned}\phi &= \frac{a+b}{a} \\ &= \frac{a}{a} + \frac{b}{a} \\ &= 1 + \frac{b}{a} \\ &= 1 + \frac{1}{\phi},\end{aligned}$$

e ϕ deve ser a raiz positiva de $\phi = 1 + 1/\phi$, ou seja, a raiz positiva de

$$\phi^2 - \phi - 1 = 0.$$

Teorema 14.43. *ϕ, solução da equação $\phi^2 - \phi - 1 = 0$, é irracional.*

Demonstração. O fato de $\phi = 1 + 1/\phi$ já nos dá a expansão em fração contínua, $\phi = [1; 1, 1, 1, \cdots]$, que é infinita (e periódica!). □

Há algumas outras demonstrações muito curtas e simples de que ϕ é irracional. Estas demonstrações não envolvem usar frações contínuas ou qualquer ferramenta de Cálculo.

Demonstração. Suponha que $\phi = a/b$, com $a, b \in \mathbb{Z}$, seja raiz positiva da equação. Então

$$\begin{aligned}\left(\frac{p}{q}\right)^2 - \frac{p}{q} - 1 &= 0 \\ \left(\frac{p}{q}\right)^2 - \frac{p}{q} &= 1 \\ p^2 - pq &= q^2 \\ p(p-q) &= q^2,\end{aligned}$$

o que implica que $p|q^2$, e poratnto p e q tem um fator comum. Como presumimos que isto não acontece, somos obrigados a admitir que p seja 1. Mas

isso implicaria que

$$q = \frac{1}{\phi},$$

que não é inteiro. □

Como ϕ é a solução positiva de $\phi^2 - \phi - 1 = 0$, então

$$\phi = \frac{1+\sqrt{5}}{2}.$$

Isto pode ser usado em outra demonstração da irracionalidade de ϕ. Esta demonstração presume que já se estabeleceu que $\sqrt{5} \notin \mathbb{Q}$.

Demonstração. Suponha que

$$\frac{1+\sqrt{5}}{2} \in \mathbb{Q}.$$

Então

$$2\left(\frac{1+\sqrt{5}}{2}\right) - 1 = \sqrt{5},$$

mas então obtivemos um irracional ($\sqrt{5}$) simplesmente realizando uma divisão e uma subtração em um racional – o que é impossível. □

14.9 Exercícios

Ex. 263 — Represente $2/3$, $20/3$, $11/13$ e $21/13$ como frações contínuas.

Ex. 264 — Expanda as frações contínuas como números racionais: $[0;1,2,3]$, $[0;3,2,1]$, $[0;10,10,10]$, $[1;9,9]$.

Ex. 265 — Determine as expansões de $\sqrt{11}$ e $\sqrt{12}$ como frações contínuas.

Ex. 266 — Obtenha a expansão de $\sqrt{5}$ em fração contínua, e conclua que $\sqrt{5}$ é irracional.

Ex. 267 — Determine a expansão em fração contínua de $(b+\sqrt{b^2-4ac})/2a$.

Ex. 268 — Seja $x \in \mathbb{R}$ positivo, e a_1, b_1, a_2, b_2 tais que $a_2b_1 - a_1b_2 = 1$, e

$$\frac{a_1}{b_1} < x < \frac{a_2}{b_2}.$$

Prove que uma das duas frações deve ser convergente na expansão de x.

Ex. 269 — Seja $x = [x_0; x_1, x_2, \dots]$ um número irracional, e sejam $y_1, y_2, \dots$ uma sequência de inteiros positivos. Prove que

$$\lim_{k\to\infty} [x_0; x_1, \dots, x_k, y_1, y_2, \dots] = x$$

Ex. 270 — Seja A um número representável por fração contínua periódica. Prove que A é da forma

$$\frac{a + \sqrt{b}}{c},$$

onde $a, b, c \in \mathbb{Z}$ e b não é quadrado perfeito.

Ex. 271 — Seja

$$A = \frac{a + \sqrt{b}}{c},$$

onde $a, b, c \in \mathbb{Z}$ e b não é quadrado perfeito. Prove que A pode ser escrito como fração contínua periódica.

Ex. 272 — Dado um intervalo, como determinar o racional dentro dele que tenha o menor numerador e o menor denominador? (Dica: represente as extremidades como frações contínuas).

Ex. 273 — Seja $x = [x_0; x_1, x_2, \dots]$

$$P_k = \begin{pmatrix} x_0 & -1 & 0 & \cdots & 0 & 0 \\ 1 & x_1 & -1 & & & 0 \\ 0 & 1 & \ddots & & & 0 \\ \vdots & & & & & \vdots \\ 0 & & & & x_{n-1} & -1 \\ 0 & 0 & 0 & \cdots & 1 & x_k \end{pmatrix}$$

e Q_k a matriz obtida removendo a primeira linha e aprimeira coluna de P_k Prove que $p_k = \det P_k$, e que $q_k = \det Q_k$.

Ex. 274 — Encontre um contraexemplo para a recíproca do Lema 14.23.

Ex. 275 — É possível construir um espaço métrico a partir de $\mathbb{Q}^2$ usando a distância de Manhattan,

$$d\Big((x_1, y_1), (x_2, y_2)\Big) = |x_1 - x_2| + |y_1 - y_2|.$$

Para cada vetor $v = (x, y)$, com $x, y \in \mathbb{Q}$, é possível definir uma sequência

$$s_n^v = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

com $a, b, c \in \mathbb{Q}$. Determine precisamente quando s_n^v é de Cauchy (para quais noções de distância, e quais, a, b, c, x, y).

Ex. 276 — O número $0,999\cdots$, onde a quantidade de noves após a vírgula é infinita, é o número um. Como consequência,

$$1,999\cdots = 2,$$
$$2,5999\cdots = 2,6.$$

Prove, usando a construção de reais que demos neste Capítulo, que $0,999\cdots = 1$.

Capítulo 15

Corpos Quadráticos

Os números representados por frações contínuas infinitas e não periódicas (os exemplos usuais são e, π, ϕ, $\sqrt{2}$) não pertencem ao corpo dos racionais. Para incluí-los, e ainda assim obter um corpo, constrói-se um novo corpo, $\mathbb{R}$, que contém o corpo $\mathbb{Q}$. Isso é desenvolvido na Seção 14.5, usando frações contínuas, embora possa ser feito de diversas maneiras. Semelhantemente, percebendo que $x^2 = -1$ não tem solução em $\mathbb{R}$, criamos um outro corpo, $\mathbb{C}$, que contém $\mathbb{R}$, e onde postulamos que existe um elemento $i = \sqrt{-1}$.

15.1 Extensões de Corpos

Dizemos que $\mathbb{R}$ é uma *extensão* do corpo $\mathbb{Q}$, e que $\mathbb{C}$ é uma extensão de $\mathbb{R}$.

Definição 15.1 (extensão de corpo)**.** Se E e F são corpos, e $F \subset E$, então E é uma **extensão** de F, o que denotamos por E/F a **extensão de** E **sobre** F. ⧫

Exemplo 15.2. Os corpo dos reais são extensão do corpo dos racionais; o corpo dos complexos é extensão do corpo dos reais. ◀

Exemplo 15.3. $\mathbb{Z}_2$ é um corpo, contendo os elementos 0 e 1, e onde as operações são as usuais, mas módulo dois. É usual denotar $GF(2)$ ao invés de $\mathbb{Z}_2$. Podemos construir um corpo com quatro elementos, que é uma extensão de $GF(2)$. O conjnuto de polinômios

$$GF(4) = \{0, 1, x, x + 1\},$$

quando dotado de soma e multiplicação módulo $x^2 + x + 1$, é um corpo.

Como $GF(2) \subset GF(4)$, então esta é uma extensão de $GF(2)$. ◀

Cada número complexo pode ser descrito por dois reais, e é fácil verificar que as operações de soma e multiplicação fazem de $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$; uma possível base para este espaço é $\{1, i\}$. Isso vale também para

qualquer extensão de corpos: $\mathbb{R}$ é também um espaço vetorial sobre $\mathbb{Q}$, com dimensão infinita.

Teorema 15.4. *Se* E *é extensão de um corpo* F*, então* E *é um espaço vetorial sobre* F*.*

Demonstração. A operação de soma em E define um grupo comutativo, portanto já temos comutatividade, associatividade, neutro e inverso para soma, além de estar claro que a operação é fechada em E.

A multiplicação de $x \in F$ por $y \in E$ resulta em elemento de E (porque $F \subset E$, e portanto $x, y \in E$). Além disso, a multiplicação é associativa e distributiva (porque E é um corpo).

Há neutro para multiplicação: como $F \subset E$, e o neutro deve ser único, o mesmo elemento neutro em F é o neutro em E. □

Definição 15.5 (grau de extensão de corpo; extensão finita)**.** O **grau da extensão** E **sobre** F, denotado $[E : F]$, é a dimensão de E como espaço vetorial sobre F. Quando $[E : F]$ é finito, dizemos que E é uma extensão finita de F. ♦

Exemplo 15.6. $[\mathbb{C} : \mathbb{R}] = 2$, porque $\mathbb{C}$ é espaço de dimensão dois sobre $\mathbb{R}$. ◀

Exemplo 15.7. $\mathrm{GF}(4)$ é espaço vetorial sobre $\mathrm{GF}(2)$, onde a base é $B = \{1, x\}$. Os elementos de $\mathrm{GF}(4)$ são combinações lineares dessa base, onde os coeficientes estão em $\mathrm{GF}(2)$:

$$\begin{aligned} (\alpha)(\beta) &= \cdots && (\alpha{\in}\mathrm{GF}(2),\ \beta{\in}B) \\ (1)(0) &= 0 \\ (1)(1) &= 1 \\ (1)(x) &= x \\ (1)(x) + (1)(1) &= x + 1. \end{aligned}$$

Em todos os casos, o resultado é módulo $x^2 + x + 1$.

Como os $\mathrm{GF}(4)$ é espaço vetorial sobre $\mathrm{GF}(2)$, com base $\{1, x\}$, de tamanho dois, então $[\mathrm{GF}(4) : \mathrm{GF}(2)] = 2$. ◀

Teorema 15.8. *Se* E *é extensão de* F*, e* F *é extensão de* K*, então*

$$[E : K] = [E : F][F : K].$$

15.2 Corpos Quadráticos

Os corpos quadráticos são extensões de $\mathbb{Q}$ que nos interessam.

Definição 15.9 (corpo quadrático)**.** Seja $d \in \mathbb{Z}$ livre de quadrados, com $|d| > 1$. Então

$$\mathbb{Q}[\sqrt{d}] = \left\{ a + b\sqrt{d} \ : \ a, b \in \mathbb{Q} \right\}$$

Quando $d > 0$, dizemos que $\mathbb{Q}[\sqrt{d}]$ é um **corpo quadrático real**; quando $d < 0$ dizemos que $\mathbb{Q}[\sqrt{d}]$ é um corpo **quadrático imaginário**. ♦

É simples verificar que $\mathbb{Q}[\sqrt{d}]$ é de fato um corpo.

Exemplo 15.10. Com $d = 2$, há o corpo quadrático

$$\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \ : \ a, b \in \mathbb{Q} \right\}.$$

Já com $d = -1$,

$$\mathbb{Q}[i] = \{a + bi \ : \ a, b \in \mathbb{Q}\}.$$ ◄

Exemplo 15.11. Com $d = 6$, o corpo quadrático é

$$\mathbb{Q}[\sqrt{6}] = \mathbb{Q}[\sqrt{2}\sqrt{3}] = \left\{ a + b\sqrt{2}\sqrt{3} \ : \ a, b \in \mathbb{Q} \right\}.$$

◄

Antes de definir os conceitos de conjugado, traço e norma, damos uma motivação. Representamos os membros de $\mathbb{Q}[\sqrt{d}]$ usando um isomorfismo[1] com matrizes 2×2,

$$a + b\sqrt{d} \quad \leftrightarrow \quad \begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \tag{15.1}$$

de onde chegamos naturalmente à definição 15.12.

Definição 15.12 (conjugado, norma e traço)**.** Se Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}[d]$, representado usando o isomorfismo na Equação 15.1 como $A = \left(\begin{smallmatrix} a & bd \\ b & a \end{smallmatrix}\right)$. Os dois autovalores da matriz são **conjugados**, de forma que o **conjugado** de α é $\overline{\alpha} = a - b\sqrt{d}$. A *norma* de α é o determinante da matriz A, $N(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 d$, e o *traço* de α é o traço da matriz A, $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2a$.

A matriz em 15.1 é chamada de **representação regular** do número $a + b\sqrt{d}$. ♦

Exemplo 15.13. Em $\mathbb{Q}[\sqrt{2}]$, seja $\alpha = 3 + 4\sqrt{2}$.

$$\begin{aligned} N(\alpha) &= 9 - 16(2) = -23 \\ \mathrm{Tr}(\alpha) &= 6 \\ \overline{\alpha} &= 3 - \sqrt{2}. \end{aligned}$$

Ilustra-se aqui também que a norma pode ser negativa. ◄

[1] Se trocarmos $\mathbb{Q}$ por $\mathbb{R}$ e tomarmos $d = -1$, resulta o corpo $\mathbb{C}$ – cujos elementos $z = x + yi$ podem ser representados por matrizes $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right)$, onde x é a parte real e y a parte imaginária. De fato, $i^2 = -1$, e $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Tendo dois autovalores diferentes, a representação regular de $z = a + b\sqrt{d}$ é sempre uma matriz diagonalizável.

Teorema 15.14. *Se* $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$*, então* $N(\alpha\beta) = N(\alpha)N(\beta)$*, e* $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.

Evidentemente, $Tr(\alpha) = Tr(\overline{\alpha})$, e $N(\alpha) = N(\overline{\alpha})$. É também simples verificar, calculando, que todo $\alpha \in \mathbb{Q}[\sqrt{d}]$ tem norma em $\mathbb{Q}$.

Teorema 15.15. *Todo* $\alpha \in \mathbb{Q}[\sqrt{d}]$ *é raiz do polinômio característico de sua representação como matriz – portanto mônico, de grau dois e com coeficientes racionais.*

Demonstração.

$$\begin{aligned}(r - \alpha)(r - \overline{\alpha}) &= r^2 - (\alpha + \overline{\alpha})r + \alpha\overline{\alpha} \\ &= r^2 - Tr(\alpha)r + N(\alpha) \qquad (15.2)\end{aligned}$$

Este é evidentemente o polinômio característico de $\left(\begin{smallmatrix} x & yd \\ y & x \end{smallmatrix}\right)$, quando $\alpha = x + y\sqrt{d}$. □

Definição 15.16 (inteiro em corpo quadrático)**.** Dizemos que α é **inteiro** em $\mathbb{Q}[\sqrt{d}]$ (também chamado de **inteiro quadrático**) se o polinômio 15.2, que define α, tem coeficientes em $\mathbb{Z}$. ♦

Exemplo 15.17. Em $\mathbb{Q}[\sqrt{2}]$, $1 + 3\sqrt{2}$ é inteiro, porque sua representação natural é

$$\begin{pmatrix} 1 & 6 \\ 3 & 1 \end{pmatrix},$$

que tem polinômio característico $x^2 - 2x - 17$, com coeficientes em $\mathbb{Z}$. ◀

Teorema 15.18. *Se* $\alpha \in \mathbb{Q}[\sqrt{d}]$ *é inteiro quadrático, então* $N(\alpha) \in \mathbb{Z}$ *e* $Tr(\alpha) \in \mathbb{Z}$.

Demonstração. Segue trivialmente da definição de inteiro quadrático. O polinômio 15.2 tem coeficientes em $\mathbb{Z}$, e tanto a norma como o traço são coeficientes. □

O Lema 15.19 será usado na demonstração do Teorema 15.20, que identifica a forma dos inteiros em $\mathbb{Q}[\sqrt{d}]$.

Lema 15.19. *Se* $t^2 d \in \mathbb{Z}$*, e* d *é livre de quadrados, então* $t \in \mathbb{Z}$.

Demonstração. Seja m/n a representação do racional t como fração, já reduzida, e seja p algum primo na fatoração do denominador n. Então

$$dt^2 = d\frac{m^2}{p^2 w^2},$$

e como d é livre de quadrados, não há como algum fator de d cancelar p^2. Logo, se $dt^2 \in \mathbb{Z}$ e d é livre de quadrados, então $t \in \mathbb{Z}$, como determina o enunciado. □

Teorema 15.20. *Os inteiros em $\mathbb{Q}[\sqrt{d}]$ são de uma das duas formas a seguir.*

$$\begin{cases} \left\{ x + y\sqrt{d} \ : \ x, y \in \mathbb{Z} \right\} & \text{se } d \neq 4k+1 \\ \left\{ \dfrac{x + y\sqrt{d}}{2} \ : \ x, y \in \mathbb{Z}, x, y \text{ tem mesma paridade} \right\} & \text{se } d = 4k+1 \end{cases}$$

Demonstração. ($\Rightarrow$) Primeiro mostramos que os elementos das duas formas dadas são realmente inteiros quadráticos.

Suponha que $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, então o traço e a norma de α são $2a$ e $a^2 = b^2 d$, inteiros – portanto os coeficientes do polinômio característico associado são inteiros.

Agora suponha que $\alpha = \frac{a+b\sqrt{d}}{2}$, sendo que a e b tem a mesma paridade. O traço é $\mathrm{tr}(\alpha) = a$. A norma é

$$\begin{aligned} N(\alpha) &= \frac{a}{2} + \frac{b}{2}\sqrt{d}\frac{a}{2} - \frac{b}{2}\sqrt{d} \\ &= \frac{a^2 - b^2 d}{4} \\ &= \frac{a^2 - b^2(4k+1)}{4} \\ &= \frac{a^2 - 4kb^2 - b^2}{4} \\ &= \frac{a^2 - b^2}{4} - kb^2 \\ &= \frac{(a+b)(a-b)}{4} = kb^2 \end{aligned}$$

como a e b tem a mesma paridade, então tanto $a + b$ como $a - b$ são pares, e $4 \mid (a+b)(a-b)$. Logo, $N(\alpha) \in \mathbb{Z}$.

($\Leftarrow$) Mostramos agora que qualquer inteiro quadrático deve ser de uma das duas formas.

Seja $\alpha = a + b\sqrt{d}$ um inteiro quadrático. Queremos mostrar que os coeficientes do polinômio característico de α são inteiros, ou seja, mostrar que a norma e o traço de α são inteiros.

O traço de α é $2a$, logo a pode ser um inteiro ou metade de um inteiro.

A norma de α é $a^2 - b^2 d$.

Suponha que x seja igual a $a/2$, com $a \in \mathbb{Z}$. Então

$$\left(\frac{a}{2}\right)^2 + y^2 d \in \mathbb{Z}$$
$$\frac{a^2}{4} + y^2 d \in \mathbb{Z}$$
$$a^2 + (4y^2)d \in 4\mathbb{Z}$$
$$a^2 + (2y)^2 \in 4\mathbb{Z}$$

Agora, sabemos que $a^2 \in \mathbb{Z}$, logo $(2y)^2 \in \mathbb{Z}$ também, o que significa que y pode ser inteiro ou metade de inteiro. Mas presumimos que a é ímpar, e se $y \in \mathbb{Z}$, a última equação seria uma contradição: $a^2 + (2y)^2$, ímpar, seria múltiplo de 4. Assim, $y = b/2$ para algum $b \in \mathbb{Z}$.

$$x^2 - dy^2 = \frac{a^2}{4} - \frac{b^2}{4}d = 4k$$

Logo,

$$\begin{aligned} a^2 &\equiv db^2 \pmod 4 \\ 1 &\equiv d(1) \pmod 4, \qquad \text{(quadrados ímpares são } 1 \pmod 4\text{)} \end{aligned}$$

e temos $d \equiv 1 \pmod 4$.

Agora, suponha que $d \not\equiv 1 \pmod 4$. Da discussão anterior, vemos que x não pode ser metade de um inteiro, portanto $x \in \mathbb{Z}$. Mas como $x^2 - dy^2 \in \mathbb{Z}$, então $dy^2 \in \mathbb{Z}$, e como d é livre de quadrados, pelo Lema 15.19 $y \in \mathbb{Z}$. □

Por conveniência, adotaremos uma forma unificada para denotar o conjunto de inteiros em um corpo quadrático. Observamos que se $x, b \in \mathbb{Z}$ tem a mesma paridade,

$$\begin{aligned} \frac{x + b\sqrt{d}}{2} &= \frac{x - b + b + b\sqrt{d}}{2} \\ &= \frac{x-b}{2} + b\left(\frac{1+\sqrt{d}}{2}\right) \\ &= a + b\left(\frac{1+\sqrt{d}}{2}\right). \qquad (x - b \text{ é par}) \end{aligned}$$

Seja

$$\omega = \begin{cases} \sqrt{d} & \text{se } d \equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{se } d \not\equiv 1 \pmod 4 \end{cases}$$

Denotaremos os inteiros em um corpo quadrático $F = \mathbb{Q}[\sqrt{d}]$ por

$$\mathcal{O}_F = \mathbb{Z}[\omega] = \{a + b\omega \ : \ a, b \in \mathbb{Z}\}.$$

Teorema 15.21. *Se α e β são inteiros em $\mathbb{Q}[\sqrt{d}]$, então $\overline{\alpha}$, $\alpha + \beta$ e $\alpha\beta$ também são.*

Não é difícil perceber, a partir do Teorema 15.21, que os inteiros em um corpo quadrático F formam um anel.

Definição 15.22 (anel de inteiros quadráticos)**.** O conjunto de inteiros quadráticos em um corpo quadrático F, com as operações usuais, é o **anel de inteiros quadráticos** de F, denotado por $\mathcal{O}_F$. ⧫

15.3 Divisibilidade

A noção de divisibilidade em $\mathbb{Z}$ se estende a inteiros quadráticos.

Definição 15.23 (divisibilidade para inteiros quadráticos)**.** Sejam $\alpha, \beta \in \mathcal{O}_F$. Dizemos que α **divide** β (denotamos $\alpha \mid \beta$) se existe $\gamma \in \mathcal{O}_F$ tal que $\alpha\gamma = \beta$. Quando α não divide β, denotamos $\alpha \nmid \beta$. ⧫

Teorema 15.24. *Sejam $a + b\omega \in \mathbb{Z}[\omega]$ e $n \in \mathbb{Z}$. Então $n \mid \alpha$ se e somente se $n \mid a$ e $n \mid b$*

Demonstração. Se $n \mid a$ e $n \mid b$, é evidente que $n \mid \alpha = a + b\omega$. Agora presuma que $n \mid \alpha = a + b\omega$ Então

$$\begin{aligned}(a + b\omega) &= n(x + y\omega)\\ a + b\omega &= nx + ny\omega\end{aligned}$$

e $a = nx$, $b = ny$, logo $n \mid a$ e $n \mid b$. □

Relembramos a definição de unidade, desta vez aplicada a inteiros quadráticos.

Definição 15.25 (unidade)**.** Uma **unidade** em $\mathcal{O}_F$ é um elemento com inverso em $\mathcal{O}_F$ – ou seja, γ é unidade se e somente se existe δ tal que $\gamma\delta = 1$. ⧫

Teorema 15.26. *As unidades em um corpo quadrático são os elementos com norma igual a ± 1.*

Demonstração. Usamos a definição de unidade. γ é unidade se e somente se existe δ tal que

$$\begin{aligned}\gamma\delta &= 1\\ N(\gamma\delta) &= N(1)\\ N(\gamma)N(\delta) &= 1,\end{aligned}$$

portanto a norma de qualquer unidade é ± 1.

Agora, suponha que para algum $\alpha \in \mathbb{Q}[\sqrt{d}]$, $N(\alpha) = \pm 1$.

$$\alpha\overline{\alpha} = N(\alpha)$$
$$\alpha\overline{\alpha} = \pm 1,$$

e o inverso de α é $\mp\overline{\alpha}$. □

Teorema 15.27. *As unidades em um corpo quadrático formam um grupo com a operação de multiplicação.*

Demonstração. Segue naturalmente do Teorema 15.26. □

Denotamos o grupo de unidades em $\mathcal{O}_F$ por $\mathcal{O}_F^\times$.

Teorema 15.28. *Para qualquer corpo quadrático* F*,* $\mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$*, e consequentemente* $\mathcal{O}_F^\times \cap \mathbb{Q} = \{\pm 1\}$*.*

Demonstração. Se $\alpha \in \mathcal{O}_F \cap \mathbb{Q}$ então $\alpha = a + b\omega$, com $a, b \in \mathbb{Z}$ e $\alpha \in \mathbb{Q}$. Mas $\omega \notin \mathbb{Q}$, logo $b = 0$ e $\alpha = a \in \mathbb{Z}$.

A segunda parte do enunciado segue porque ± 1 são os únicos racionais com norma ± 1. □

Teorema 15.29. $\mathbb{Q}[\sqrt{d}]$ *tem infinitas unidades quando* $d > 0$*.*

Teorema 15.30. $\mathbb{Q}[\sqrt{-1}]$ *tem quatro unidades,* ± 1 *e* $\pm\sqrt{-1}$*;* $\mathbb{Q}[\sqrt{-3}]$ *tem seis unidades,* ± 1*,* $\pm(-1+\sqrt{-3})/2$ *e* $\pm(-1-\sqrt{-3})/2$*; para outros valores de* $d < 0$*,* $\mathbb{Q}[\sqrt{d}]$ *tem somente as duas unidades* ± 1*.*

Definição 15.31 (elementos irredutíveis, primos em corpo quadrático)**.** Seja $\alpha \in \mathcal{O}_F$. Se toda decomposição $\alpha = \beta\gamma$ com $\beta, \gamma \in \mathcal{O}$ implica que um dos fatores, β ou γ é uma unidade, então α é **irredutível** em $\mathcal{O}$.

Se, para todo elemento α não zero e não unidade, $\alpha \mid \beta\gamma$ sempre implica em $\alpha \mid \beta$ ou $\alpha \mid \gamma$, então α é **primo**. ♦

Enquanto primos e irredutíveis são noções equivalentes em $\mathbb{Z}$, são diferentes em anéis de inteiros quadráticos. Por exemplo, em $\mathbb{Q}[\sqrt{3}]$ o número 13 é irredutível: não existem α, β tais que $13 = \alpha\beta$. Mas 13 não é primo, já que

$$(4+\sqrt{3})(4-\sqrt{3}) = 13,$$

e 13 divide o produto no lado esquerdo da equação – mas não divide individualmente os fatores $4 \pm \sqrt{3}$.

Teorema 15.32. *Seja* $\alpha \in \mathcal{O}_F$*. Se* $|N(\alpha)|$ *é igual a um número primo em* $\mathbb{Z}$*, então* α *é irredutível em* $\mathcal{O}_F$*.*

Demonstração. Segue da multiplicatividade da norma. □

Teorema 15.33. *Um elemento em um anel de inteiros quadráticos que não é zero nem unidade pode ser decomposto em produto de irredutíveis.*

A fatoração a que se refere o Teorema 15.33 pode ou não ser única, dependendo do corpo quadrático.

Exercícios

Ex. 277 — Prove que se α é inteiro quadrático, então $\alpha^2 + (\overline{\alpha})^2 \in \mathbb{Z}$.

Ex. 278 — Prove que $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{3}]$ não são isomorfos.

Ex. 279 — Prove que $\mathbb{Q}[\sqrt{2}\sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, e que consequentemente, $\mathbb{Q}[\sqrt{2}\sqrt{3}]$ é extensão de $\mathbb{Q}[\sqrt{2}]$.

Ex. 280 — Determine $\left[\mathbb{Q}[\sqrt{3}\sqrt{5}] : \mathbb{Q}[\sqrt{5}]\right]$ e $\left[\mathbb{Q}[\sqrt{3}\sqrt{5}] : \mathbb{Q}\right]$.

Ex. 281 — Prove que há infinitos irredutíveis em $\mathcal{O}_F$, para qualquer corpo infinito F.

Ex. 282 — Prove que se $\left(a + b\sqrt{d}\right)/2$ pertence um corpo contido em $\mathbb{Q}$, então $\sqrt{d}$ pertence ao mesmo corpo.

Ex. 283 — Suponha que, ao invés da representação regular que apresentamos, usemos

$$\begin{pmatrix} a & bd & 0 \\ b & a & 0 \\ 0 & 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & bd & 0 \\ b & a & cd \\ 0 & c & a \end{pmatrix}.$$

Quais são as implicações? Estude traço, norma, os números representados pela matriz. Verifique como as demonstrações onde usamos traço e norma são afetadas.

Capítulo 16

Régua e compasso: o corpo dos números construtíveis

As regras para construções com régua e compasso estão intimamente relacionadas aos postulados da Geometria Euclideana – em particular, os dois primeiros, que não tratam de angulos.

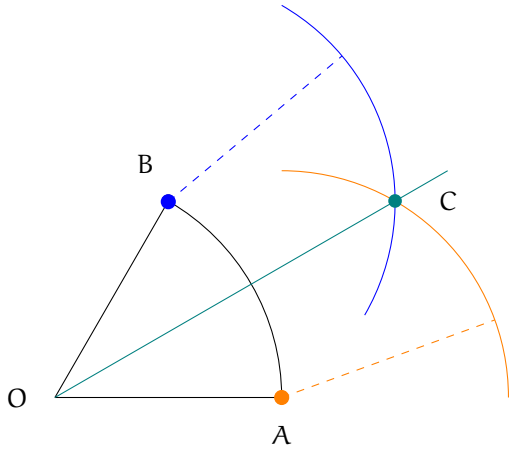
Definição 16.1 (construção com régua e compasso)**.** Uma **construção clássica com régua e compasso** deve ser realizada a partir de dois pontos iniciais distintos, e usando apenas as operações a seguir, com uma régua e um compasso.

- com a régua, retas podem ser traçadas passando por dois pontos;
- dado um ponto e uma distância, um círculo pode ser traçado com o compasso;
- a partir de duas retas, ou dois círculos, ou uma reta e um círculo, é possível indentificar os pontos de interseção, e portanto aumentar o conjunto de pontos.

Podem ser arbitrariamente grandes o comprimento da régua e a abertura do compasso, e a régua não pode ter marcações. ⧫

Os gregos conseguiram determinar como, usando apenas régua e compasso, realizar as quatro operações aritméticas básicas, além de diversas outras operações – extrair raízes quadradas, obter a bisecção de ângulos, criar um quadrado com o dobro de uma dada área, criar um quadrado com o mesmo volume de um polígono dado, e construir polígonos com alguns números específicos de lados. Havia, no entanto, construções que os gregos não conseguiam realizar, e cujas demonstrações de impossibilidade só foram obtidas muito mais tarde.

Para um exemplo simples de construção com régua e compasso, examinamos a bisecção de um ângulo. São dadas duas retas não paralelas que se interceptam em um ponto O. Marcamos dois pontos, um em cada reta, e a uma mesma distancia de O. Nomeamos os pontos A e B. Desenhamos dois círculos, um com centro em A, e um com centro em B; o raio deve ser maior que a distância de A até B. Estes dois círculos se interceptam em dois pontos; tomamos um deles, C, e a reta OC é a bissetriz do ângulo dado.



16.1 Números construtíveis

Embora seja possível trabalhar com "pontos" construtíveis no plano, podemos usar, como já fizemos anteriormente, o plano complexo. Assim, o ponto (a, b) corresponde ao número complexo $a + bi$.

Definimos, portanto, número construtível. Partimos da existencia de dois pontos diferentes, e construímos outros a partir deles. É necessário agora formalizar o que consideramos "construção com récua e compasso":

Definição 16.2 (número construtível)**.**

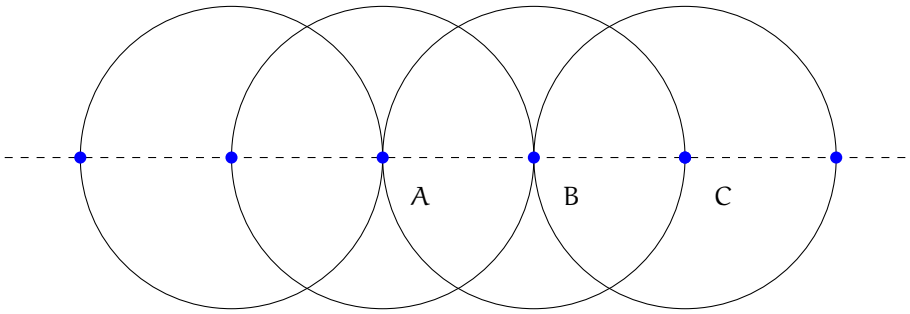
- Os pontos $(0, 0)$ e $(1, 0)$ são construtíveis.
- Se P e Q são dois pontos construtíveis, então a reta passando por P e Q também é (e evidentemente, o segmento indo de P até Q também).
- Se P e Q são construtíveis, então a circunferência com centro em P e raio PQ é construtível (porque podemos posicionar a ponta seca do compasso em P e a outra ponta em Q).
- Os pontos de interseção de dois objetos construtíveis. são construtíveis. ♦

Determinaremos agora quais números são construtíveis. Gradualmente identificaremos conjuntos numéricos. O primeiro conjunto de números construtíveis será o dos inteiros ($\mathbb{Z}$) – os pontos inteiros no eixo real.

Assim, verificamos a seguir que podemos identificar os eixos real e imaginário, e construir todos os pontos inteiros nesses eixos.

Lema 16.3. *O conjunto $\mathbb{Z}$ é construtível.*

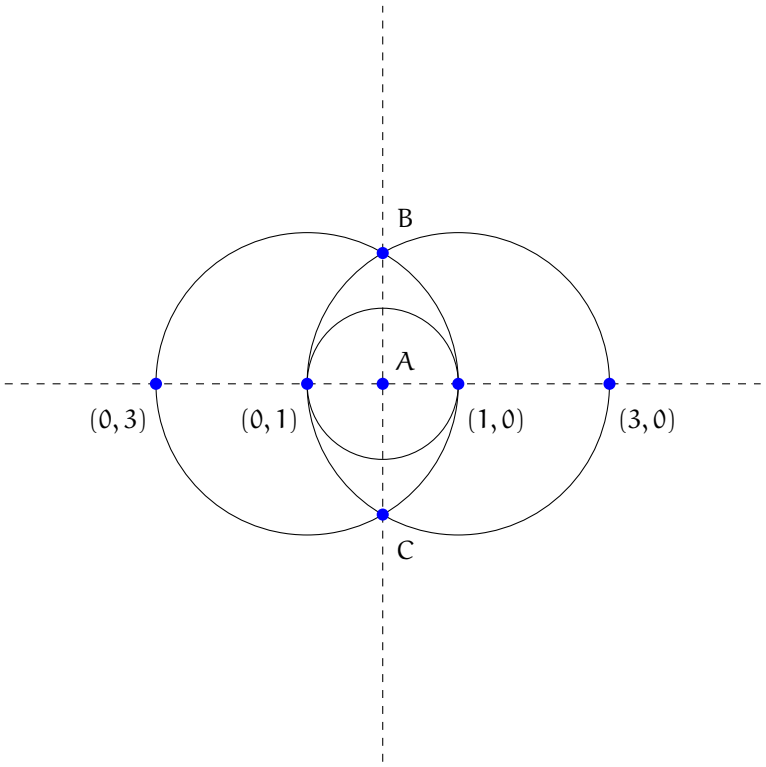
Demonstração. Podemos construir pontos equidistantes no eixo real tendo dois pontos iniciais A e B; escolhemos A como origem. Criamos inicialmente um círculo com centro em A e raio igual a d, a distancia entre A e B. Depois, criamos outro círculo com centro em B, e raio d. Agora, os pontos A e B determinam uma reta, que será o eixo real. Os outros pontos podem ser obtidos facilmente – por exemplo, C é a interseção do círculo com centro em B com a reta AB.



Com isso provamos que os números da forma $(k, 0)$, com $k \in \mathbb{Z}$, são construtíveis (e portanto $\mathbb{Z}$ é construtível). □

Teorema 16.4. *Os números da forma $(0, k)$, com $k \in \mathbb{Z}$ são construtíveis.*

Demonstração. Para traçar o eixo imaginário, traçamos uma reta perpendicular a AB, passando por A. Para isso, desenhamos um círculo com centro em A e raio 1. Depois, traçamos dous círculos, com centro em $(1, 0)$ e $(-1, 0)$, com raio 2. As interseções destes círculos, nos pontos B e C, determinam uma reta perpendicular a AB.

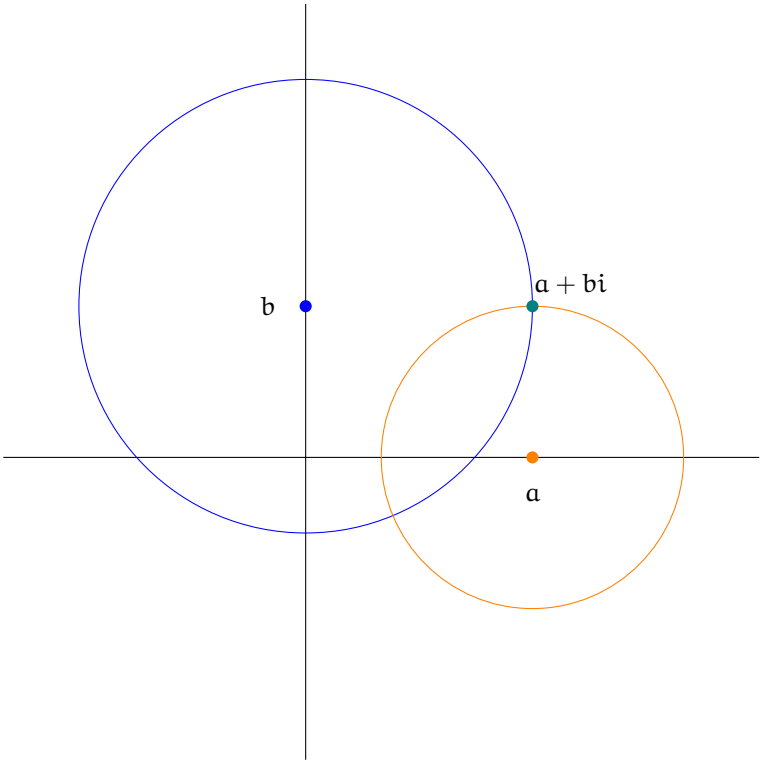


Tendo a origem, o eixo imaginário, e número $1 + 0i$ (que é o ponto $(1, 0)$) é possível construir os pontos $(0, y)$, com $y \in \mathbb{Z}$. □

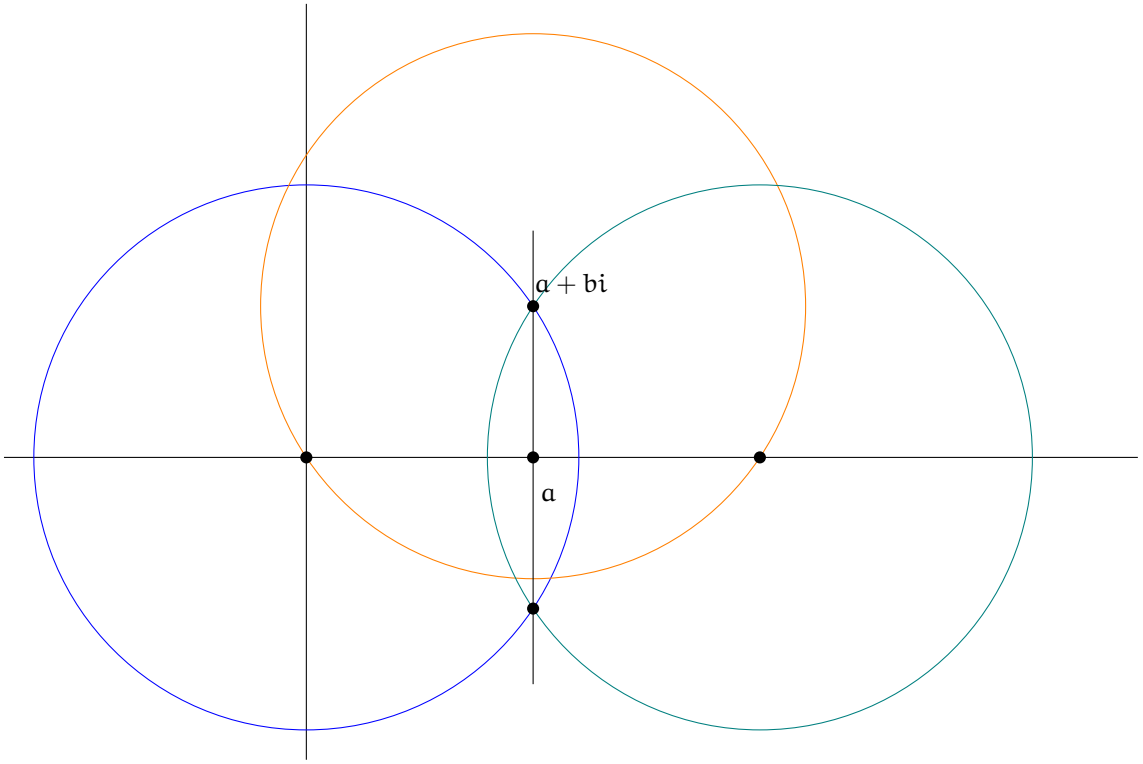
Naturalmente, o próximo passo é mostrar como combinar os números que já temos, a fim de obter $a + bi$ a partir de a e de bi.

Lema 16.5. $a+bi$ *e* $a-bi$ *podem ser construídos se e somente se os pontos* a *e* bi *podem ser construídos.*

Demonstração. Se $a+0i$ e $0+bi$ são construtíveis, então podemos criar dois círculos, um com raio b no ponto a e um com raio a no ponto bi. Um dos dois pontos onde estes círculos se encontram é $a + bi$.



A partir do ponto $a + bi$, podemos baixar perpendiculares nos dois eixos. A figura a seguir ilustra a obtenção de a a partir de $a + bi$.



Primeiro, desenha-se o círculo com centro em $a+bi$ e passando pela origem. Depois, com o mesmo raio, desenham-se dois círculos, nos dois pontos em que o primeiro círculo intercepta o eixo real. Basta agora traçar a perpendicular, que passa pelasinterseções dos dois últimos círculos.

Notamos que esta construção também nos dá $a - bi$. □

A técnica usada é útil para obter o conjugado de um número.

Corolário 16.6. *Se z é construtível, $\bar{z}$ também é.*

Demonstração. Se $z = a + bi$, basta baixar perpendiculares para obter os pontos $(a, 0)$ e $(0, b)$, e assim construir $a - bi$. □

Finalmente, tratamos das operações de soma e multiplicação, com suas inversas. Começamos pela soma.

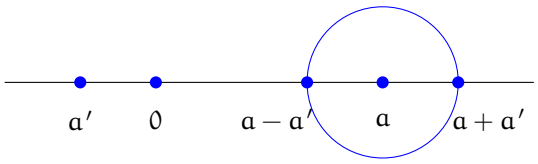
Lema 16.7. *Dados dois complexos x e y, é possível construir $x + y$ e $x - y$ (o que implica que os inteiros Gaussianos são construtíveis).*

Demonstração. Queremos somar dois complexos, $x = a + bi$ e $y = a' + b'i$.

Mostramos que o enunciado vale no eixo dos reais – o que significa que também vale no eixo imaginário, e como a soma de complexos se dá comando os componentes real e imaginário separadamente, isto bastará.

Geometricamente, se pudermos somar as coordenadas separadamente nos dois eixos, $a + a'$ e $b + b'$, o Lema 16.5 garante que a partir dessas novas coordenadas podemos construir $(a + a') + (b + b')i$.

Dados a e a' no eixo real, temos a distância da origem até a'. Criamos um círculo centrado em a com raio igual a essa distância, e um dos pontos de interseção do círculo com o eixo é $a + a'$; o outro é $a - a'$.

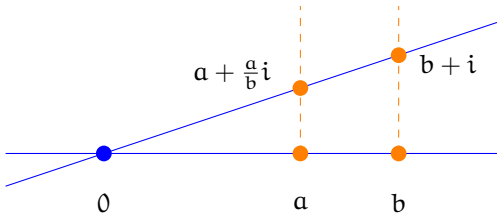


□

Passamos à multiplicação.

Lema 16.8. *Dados dois complexos x e y, é possível construir xy e, quando $y \neq 0$, x/y.*

Demonstração. Tendo a e a' no eixo real, é possível construir $b + i$. Traçamos uma reta da origem até $a' + i$; depois, traçamos uma reta perpendicular a a, e marcamos o ponto onde ela se intercepta com a reta traçada anteriormente.



O ponto obtido é $a + (a/b)i$, e pelo Lema 16.5, é possível obter $(a/b)i$ e a/b. O procedimento inverso pode ser usado para obter ab a partir de a e b. □

Teorema 16.9. *Os números construtíveis formam um corpo.*

Demonstração. Segue dos lemas anteriores. As quatro operações podem ser realizadas, e valem associatividade, comutatividade e distributividade como usualmente. Há elemento neutro para adição (a origem); e elemento neutro para multiplicação: $(1, 0)$, ou $1 + 0i$. □

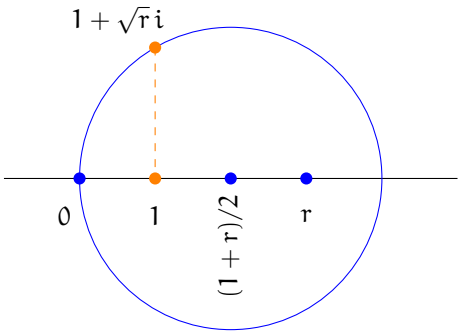
Corolário 16.10. *$\mathbb{Q}$ e $\mathbb{Q}[i]$ são construtíveis.*

O conjunto $\mathcal{C}$, além de ser um corpo, tem outra propriedade – é fechado para a extração de raízes quadradas.

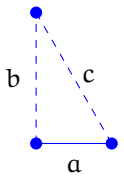
Teorema 16.11. *Se $x^2 \in \mathcal{C}$, então $x \in \mathcal{C}$.*

Demonstração. Provamos que, se $r \in \mathcal{C}$, então $\sqrt{r} \in \mathcal{C}$.

Trace um círculo com centro em $(1+r)/2$, e raio também $(1+r)/2$.



Agora trace uma perpendicular ao eixo real, passando pelo um. Ela interceptará o círculo nos pontos $1 \pm \sqrt{r}\,i$. Isto pode ser facilmente verificado usando o Teorema de Pitágoras.



$$a = \frac{r}{2} + \frac{1}{2}$$
$$c = \frac{1+r}{2}$$

e $b = \sqrt{c^2 - a^2}$ resulta em $\sqrt{r}$. □

É interessante que, sendo possível calcular $\sqrt{x}$, pode-se calcular $\sqrt[2^k]{x}$, para todo $k \in \mathbb{N}$, já que

$$\sqrt[2^k]{x} = \sqrt{\sqrt[2^{k-1}]{x}}.$$

O fato de podermos extrair raízes quadradas implica que $\mathcal{C}$ é superconjunto *estrito* de $\mathbb{Q}[i]$. E, como os números construídos são todos complexos,

$$\mathbb{Q}[i] \subset \mathcal{C} \subseteq \mathbb{C}.$$

Os números que conseguimos construir são, portanto, da forma $a + bi$, onde a e b são da forma $r\sqrt[2^k]{s}$, com $r, s \in \mathbb{Q}$ e $k \in \mathbb{N}$.

Na próxima seção mostraremos que a segunda inclusão também é estrita ($\mathcal{C} \subset \mathbb{C}$).

16.2 Todos os números construtíveis

As construções na Seção anterior são interessantes e contribuem para o desenvolvimento de uma intuição relacionada aos números construtíveis. No entanto, da maneira como foram colocadas, elas não permitiram determinar o que *não* pode ser construído com régua e compasso. O Teorema 16.12 determina exatamente quais números podem ser construídos.

Teorema 16.12. *Seja* K *o conjunto dos números da forma* $a + bi$*, onde* a *e* b *são da forma* $r\sqrt[2^q]{s}$*, com* $r, s \in \mathbb{Q}$ *e* $q \in \mathbb{N}$*.*

Os únicos números possíveis construtíveis são da forma $\frac{a}{b} + \frac{c}{d}i$*, onde* a, b, c, d *estão em* K*.*

Demonstração. O conjunto $\mathcal{C}$ contém, além de 1 e i, interseções entre objetos, que são sempre retas ou circunferências.

A interseção de duas retas passando por pontos em K resulta de um sistema com duas equações lineares, ambas com coeficientes em K, e portanto é obtido usando as quatro operações básicas, para as quais K é fechado.

Consideramos agora a interseção de duas circunferências construídas com régua e compasso. Para cada uma. o centro é um número construtível, e um ponto da borda (um dos pontos por onde o compasso passou) é também construtível. O raio, que é subtração de dois números da forma $a + bi$, com coeficientes em K, também o será.

As interseções entre as duas circunferências serão o resultado do sistema

$$\begin{aligned}(x-a)^2 + (y-b)^2 &= e\\ (x-c)^2 + (y-d)^2 &= f,\end{aligned}$$

com todos os coeficientes e termos constantes em K. Se expandirmos os termos elevados ao quadradoe subtrairmos a segunda equação da primeira, teremos

$$2(c-a)x + 2(d-b)y = e - f - a^2 - b^2 + c^2 + d^2,$$

que é a equação de uma reta com todos os coeficientes em K. Assim, o caso de duas circunferências é o mesmo caso de uma circunferência com uma reta.

Finalmente, o caso da interseção de uma reta com uma circunferência é simples: o resultado será a solução de um sistema da forma

$$\begin{aligned}ax + by &= e,\\ (x-c)^2 + (y-d)^2 &= f,\end{aligned}$$

e o resultado será obtido usando as quatro operações elementares e raiz

quadrada – todas operações para as quais K é fechado.

Assim, $\mathcal{C} = \mathrm{K}$. □

Corolário 16.13. *Raízes cúbicas, quintas, de grau ímpar ou, de maneira geral, com grau diferente de potência de dois não são construtíveis, e* $\mathcal{C} \subset \mathbb{C}$ *(inclusão estrita: os conjuntos não são iguais).*

16.3 Alguns problemas impossíveis

Algumas construções geométricas dependem do uso de comprimentos dados por números não construtíveis, por isso não são possíveis de realizar com régua e compasso, *usando as regrasque determinamos no início do Capítulo*.

- **Duplicação do volume de um cubo**

  A partir de um cubo, o objetivo é construir outro, com o dobro do volume.

  Considere um cubo com lado unitário. O cubo com o dobro do volume teria que ser construído de forma que seu volume seja 2, e portanto com lado de comprimento $\sqrt[3]{2}$, que não é construtível.

- **Trisecção de um ângulo**

  A trisecção de um ângulo α com régua e compasso consiste em obter pontos que determinem duas retas formando um ângulo $\alpha/3$.

  Seja α igual a 60^o, ou $\pi/3$. A trisecção deste angulo nos daria ângulos de 20^o, ou $\pi/9$. Mas se este ângulo pudesse ser construído, a distância dad pelo seu cosseno também o seria (pela definição de cosseno, basta baixar um aperpendicular). No entanto, $\cos \pi/9$ é raiz de

  $$8x^3 - 6x - 1,$$

  e não há[1] polinômio de menor grau, com coeficientes racionais, do qual ele seja raiz.

- **Quadratura do círculo**

  Obter a "quadratura de um círculo" é, dado um círculo, construir um quadrado com a mesma área.

  Considere um círculo com raio unitário: sua área é π. Um quadrado com área π precisaria ter lado com comprimento igual a $\sqrt{\pi}$, que não é construtível.

[1] Não estamos demonstrando, apenas comentando. Para um argumento com rigor, teríamos que provar que de fato este polinômio não é redutível em $\mathbb{Q}$ – o que fica fora do escopo deste texto.

Exercícios

Ex. 284 — Dados dois pontos A e B, mostre como construir um quadrado tendo como um dos lados o segmento AB.

Ex. 285 — Dados dois pontos A e B, mostre como construir um triângulo equilátero tendo como um dos lados o segmento AB.

Ex. 286 — Prove que há infinitos números construtíveis

a) na borda de uma circunferência construtível, e

b) no interior de uma circunferência construtível.

Ex. 287 — Números algébricos são raizes de equações polinomiais com coeficientes racionais. Por exemplo, $1 + 2i$ é algébrico, porque é raiz da equação $x^4 - 4x^3 + 10x^2 - 12x + 5 = 0$; A razão áurea é um número algébrico, porque é raiz da equação $x^2 - x - 1 = 0$; já π não é algébrico, porque não é raiz de qualquer equação linear com coeficientes racionais. Denote o conjunto dos números algébricos por $\mathcal{A}$. Qual a relação entre $\mathcal{A}$ e $\mathcal{C}$? Um está contido no outro?

Ex. 288 — Dados os pontos $0+0i$ e $1+0i$, como é possível construir o ponto $\cos(\pi/6) + \sin(\pi/6)i$?

Ex. 289 — Se for possível usar uma régua com dois pontos diferentes marcados, as construções realizadas não são mais as clássicas construções Euclideanas com régua e compasso. Mostre que, com uma régua dessas, é possível realizar a trisecção de qualquer ângulo.

Apêndices

Apêndice A

Dicas e Respostas

Resp. (Ex. 8) — Em (a), $k = 3$, e em (b), $k = 4$.

Resp. (Ex. 13) — Duas matrizes invertíveis podem ser somadas resultando em uma singular. O conjunto não seria fechado para soma.

Resp. (Ex. 15) — Só haverá um símbolo a usar, e a quantidade dele é a quantidade representada (diferente do esquema apresentado no texto!) Note que, usando somente o dígito 1, ainda vale

$$n = \sum_{i=0}^{k} d_k 1^k.$$

Por exemplo, 111 é a representação de 3, porque

$$\begin{aligned} n &= 1 \cdot 1^2 + 1 \cdot 1^1 + 1 \cdot 1^0 \\ &= 1 + 1 + 1 \\ &= 3. \end{aligned}$$

Resp. (Ex. 18) — Veja o Exercício 17.

Resp. (Ex. 31) — Escreva $n = 7q + r$, com $q \in \mathbb{Z}$ e $r < 7$. Depois escreva $7(4q^2) = 7k$; $7(7q^2 + 2q) + 1 = 7k + 1$; $7(7q^2 + 4q) + 1 = 7k + 4$, e observe que o resto de um quadrado dividido por 7 só pode ser $0, 1, 2$ ou 4...

Resp. (Ex. 35) — (Dica) Seja $n \in \mathbb{N}$. Considere os números 1, 11, ..., 111...1 (n números) Divida cada um por n.

Resp. (Ex. 39) — Descida infinita.

Resp. (Ex. 46) — Uma possível demonstração:
Por indução em n.
A base é trivial, com $n = 1$: $u_m \mid u_{m\cdot 1}$, que é o mesmo que dizer que $u_m \mid u_m$.
Para a hipótese, presuma que, para todo m, $u_m \mid u_{mj}$ para todo número menor j que n.
Agora, observando que o Lema 4.34 afirma que $u_{m(n+1)} = u_{mn+m}$,

$$u_{m(n+1)} = u_{m(n-1)}u_m + u_{mn}u_{m+1}.$$

Como $u_m \mid u_{mn}$, o lado direito é divisível por u_m, e $u_m \mid u_{m(n+1)}$.

Resp. (Ex. 48) — Lema de Honsberger não, e conseguentemente o Teorema 4.40 não. O Lema 4.37 vale desde que os dois valores iniciais sejam coprimos.

Resp. (Ex. 57) — Use o Teorema 4.30.

Resp. (Ex. 61) — Fatore. Nenhum deles tem mais que três divisores primos distintos.

Resp. (Ex. 70) — Como $d' \mid a$, $d' \mid b$, então $d \mid d'$, portanto deve haver $k \in X$ tal que $kd' = d$. Mas então

$$\lambda(d') \leq \lambda(kd') = \lambda(d).$$

Se d' também é máximo divisor comum, então $d' \mid d$, e pelo mesmo argumento, chega-se a $\lambda(d') = \lambda(d)$.

Resp. (Ex. 71) — Observe que as matrizes dessa forma comutam. A função de valoração pode ser o determinante. Para obter Q e R, comece invertendo B e note que $Q = (A - R)B^{-1}$. O lado direito deve ser uma matriz com entradas inteiras. Disso se obtém uma equação diofantina cujas incógnitas são os dois valores em R – o que significa que sempre é possível encontrar R, e consequentemente, Q.

Resp. (Ex. 72) — O algoritmo estendido de Euclides, usado para obter os coeficientes de Bézout, funciona em qualquer domínio Euclideano.

Resp. (Ex. 74) — $n^3 - 1 = (n-1)(n^2+n+1)$, e este produto é primo.

Resp. (Ex. 75) — Considere os casos $n = 3k+1$, $n = 3k+2$, e conclua que n só pode ser $3k$.

Resp. (Ex. 77) — Presuma $\sqrt[k]{n} = a/b$, com $\operatorname{mdc}(a,b) = 1$. O que acontece se $b > 1$?

Resp. (Ex. 79) — Suponha que $p < q$ são primos consecutivos, e que $p + q = 2t$. Então $t = (p+q/2)$, e claramente, $p < t < q$. Mas t, estando entre p e q, não pode ser primo, porque p e q são primos consecutivos.

Resp. (Ex. 80) —

$$\begin{aligned}
\operatorname{mdc}\left(\frac{p+1}{2}, \frac{p\text{-}1}{2}\right) &= 2\operatorname{mdc}(p+1, p\text{-}1) \\
&= 2\operatorname{mdc}(p+1\text{-}(p\text{-}1), p\text{-}1) \\
&= 2\operatorname{mdc}(2, p\text{-}1) \\
&= \operatorname{mdc}\left(1, \frac{p\text{-}1}{2}\right) \\
&= 1.
\end{aligned}$$

Resp. (Ex. 81) — Todo F_n deixa resto dois quanto dividido por 5, e são todos ímpares.

Resp. (Ex. 82) — Para F_0 e F_1 é evidente. Para outros, como terminam com dígito 7, não são quadrados (veja o Exercícios 17).

Resp. (Ex. 83) — Indução em n.

Resp. (Ex. 89) — (Dica) $s + t$ tem um fator que não está dentre os fatores de A.

Resp. (Ex. 90) — mas não ambos. Logo, nenhum primo divide $s+t$, e $s+t > 1$ seria um novo primo, não listado antes.

Resp. (Ex. 91) — (Dica) Se $3 \mid a$, então $9 \mid a^2$.

Resp. (Ex. 98) — Ache o expoente de 2 na fatoração de $\binom{100}{n}$.

Resp. (Ex. 100) — Semelhante à demonstração da infinitude dos primos $4k+3$.

Resp. (Ex. 105) — $6/pi^2$.
Para resolver: comece olhando para a probabilidadede um inteiro qualquer k dividir os dois números; a de um número ser o MDC de ambos; e a desse último número ser 1.

Resp. (Ex. 118) — A equação diofantina tem soluções, mas nenhuma com x e y positivos:

$$-22(30) + 44(18) = 132$$

A forma geral da solução é

$$30(-22 + 18k) + 18(44 - 30k) = 132$$

Mas precisamos então de

$$\begin{aligned} -22 + 18k &> 0 \\ 44 - 30k &> 0 \end{aligned}$$

Ou seja,

$$\begin{aligned} k &> \frac{22}{18} \approx 1.222 \\ k &< \frac{44}{30} \approx 1.466, \end{aligned}$$

e não existe $k \in \mathbb{Z}$ que possamos usar.

Resp. (Ex. 119) — $k > -30.75$, e como k deve ser inteiro, $k \geq -30$.

Resp. (Ex. 142) — ϕ é multiplicativa; $\text{mdc}\,(()\,2, k) = 1$ se k é ímpar...

Resp. (Ex. 149) — É um par de Moebius.

Resp. (Ex. 153) — $n \leq 2^{\pi(n)}\sqrt{n}$, e depois chegue a $2^{\pi n} \geq \sqrt{n}$, e $\pi(n) \geq \log\sqrt{n}$.

Resp. (Ex. 158) — (a) $a = 3, b = 2$. (b) 17 é primo...

Resp. (Ex. 165) — 15 (use de Polignac-Legendre).

Resp. (Ex. 166) — 9 (use de Polignac-Legendre).

Resp. (Ex. 175) — $\{-13, -11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11\}$.

Resp. (Ex. 180) — $p \mid k^2 - 1 = (c-1)(c+1)$, logo pelo Lema de Euclides, $p \mid c+1$ ou $p \mid k-1$

Resp. (Ex. 185) — Não é um grupo. Na tabela,

$$ab = c$$
$$ac = d$$

Então

$$a\underline{a}b = ac = d,$$

mas

$$\underline{a}ab = eb = b,$$

e como a operação não é associativa – $a(bb) \neq (aa)b$ – teríamos $b = d$.

Resp. (Ex. 186) — Não – mostre que não são incongruentes $\pmod m$.

Resp. (Ex. 188) — ϕ é multiplicativa; $g^{2p^k} - 1$ é par ou ímpar? O que significa $g^{2p^k} \pmod{2p^k}$?

Resp. (Ex. 189) — Qual é a ordem de $a^m - 1$ módulo m?

Resp. (Ex. 201) — $(x, y) \odot (a, b) = (ax - by, ay + bx)$

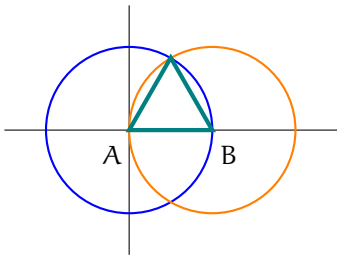
Resp. (Ex. 211) — Observe os divisores de $5(n!)^2 - 1$. Há um divisor $p > n$ que não é $5k + 1$.

Resp. (Ex. 226) — É consequência do Teorema 10.6.

Resp. (Ex. 235) — Não e não.

Resp. (Ex. 272) — Expresse as extremidades do intervalo como frações contínuas. Encontre o primeiro termo em que diferem e adicione 1 ao menor deles, a não ser que seja o último. Descarte os termos à direita. O que resta?

Resp. (Ex. 285) —



Resp. (Ex. 287) — Claramente, $\sqrt[3]{2} \notin \mathcal{C}$, mas $\sqrt[3]{2} \in \mathcal{A}$. Além disso, da demonstração do Teorema 16.12, todo número construtível é algébrico. Portanto,

$$\mathcal{C} \subset \mathcal{A}$$

Ficha Técnica

Este texto foi produzido inteiramente em LaTeX em sistema Debian GNU/Linux. Os diagramas foram criados sem editor gráfico, usando diretamente o pacote Ti*k*Z. O ambiente Emacs foi usado para edição do texto LaTeX.

Índice Remissivo