Universidade Federal da Bahia
Instituto de Matemática
Departamento de Matemática

Inteiros e Introdução a teoria dos Números[1]

Professor: Carlos E. N. Bahiano
Primeiro semestre de 2005

[1]Esta apóstila ainda está em construção. Ao longo do curso muitos conceitos e exercícios serão incorporados ao texto. Sugestões e correções serão bem vindas.

Sumário

Capítulo 1

Equivalências e Ordens

Neste capítulo estuda-se a noção de equivalência e de ordem. A importância do conceito de relação de equivalência é evidenciada pelo teorema fundamental das relações de equivalência. Ao estudar objetos, estruturas e problemas matemáticos, todo matemático tenta agrupá-los em classes de elementos com as mesmas propriedades, de forma que em cada classe cada representante possua propriedades ou respostas equivalemtes, ou seja basta estudar um dos exemplos para saber como se comportam os outros daquela mesma classe. O estudo de espaços vetoriais de dimensão finita, por exemplo evidencia várias propriedades e conceitos comuns a todos os espaços vetoriais de dimensão finita. Basta estudar um deles para conhecer todos os outros espaços de mesma dimensão. Percebe-se portanto que a classificação de estruturas e objetos matemáticos apresenta-se como importante ferramenta para a evolução da Matemática enquanto Ciência. Classificar estruturas significa agrupar em classes de elementos com as mesmas propriedades. Uma boa classificação é aquela em que classes distintas não possuem elementos em comum e cada objeto ou estrutura pertence a alguma classe de tal maneira que estudar um objeto da classe fornece propriedades (com respeito à qual os objetos foram classificados) semelhantes para todos os outros elementos da classe.

Se relação de equivalência permite aos matemáticos classificar objetos e estruturas, a relação de ordem permite ordená-los em "filas", estabelecendo uma certa hierarquia entre os objetos. esta hierarquia pode ser estabelecida de forma global ou parcial.

1.0.1 Relação de equivalência

Definição 1.1. *Seja $\mathbb{E}$ um conjunto não vazio. Um subconjunto $\mathcal{R} \subseteq \mathbb{E} \times \mathbb{E}$ é dito ser uma relação de equivalência em $\mathbb{E}$ se satisfaz:*

1. $(x, x) \in \mathcal{R}, \qquad \forall x \in \mathbb{E}. \qquad (\mathcal{R}$ é reflexiva)

2. Se $(x, y) \in \mathcal{R}$ então $(y, x) \in \mathcal{R}$. ($\mathcal{R}$ é simétrica)

3. Se $(x, y), (y, z) \in \mathcal{R}$ então $(x, z) \in \mathcal{R}$. ($\mathcal{R}$ é transitiva.)

Teorema 1.2 (Teorema fundamental das Equivalências)**.** *Seja $\mathbb{E}$ um conjunto não vazio. Toda relação de equivalência não trivial, em $\mathbb{E}$, decompõe o conjunto $\mathbb{E}$ numa união, disjunta, de subconjuntos não vazios de $\mathbb{E}$.*

Demonstração. . Seja $\mathcal{R}$ uma relação de equivalência em $\mathbb{E}$. Defina para cada $x \in \mathbb{E}$, o conjunto $\mathcal{R}_x : \{y \in \mathbb{E}; (x, y) \in \mathcal{R}\}$. É fácil ver, em decorrência da transitividade de $\mathcal{R}$, que para quaisquer par de elementos $x, y \in \mathbb{E}$, tem-se:

$$\mathcal{R}_x \cap \mathcal{R}_y = \emptyset \quad \text{ou} \quad \mathcal{R}_x = \mathcal{R}_y.$$

Seja Λ o "maior"subconjunto de $\mathbb{E}$, com respeito a inclusão, com a seguinte propriedade:

$$x, y \in \Lambda \Rightarrow \mathcal{R}_x \neq \mathcal{R}_y$$

Afirmamos que: $\mathbb{E} = \bigsqcup_{x \in \Lambda} \mathcal{R}_x$. De fato, temos $x \in \mathcal{R}_x, \quad \forall x \in \mathbb{E}$. Se $x \notin \mathcal{R}_y, \quad \forall y \in \Lambda$, então o conjunto $\Omega = \Lambda \cap \{x\}$ conteria propriamente Λ, contradizendo sua maximalidade. Isto mostra que $\mathbb{E} = \bigsqcup_{x \in \Lambda} \mathcal{R}_x$. Pelo argumento exibido no primeiro parágrafo da demonstração concluimos que $x, y \in \Lambda$ com $x \neq y$ implica em $\mathcal{R}_x \cap \mathcal{R}_y = \emptyset$. □

Cada conjunto $\mathcal{R}_x$, descrito acima,é dito ser uma classe de equivalência. O conjunto $\{\mathcal{R}_x; x \in \mathbb{E}\}$ é chamado de conjunto quociente de $\mathbb{E}$ por $\mathcal{R}$, e escrevemos, exceto em alguns casos particulares, $\frac{\mathbb{E}}{\mathcal{R}}$ para representar este conjunto. O conjunto Λ, construído acima é dito ser *um sistema completo de resíduos módulo $\mathcal{R}$*. (s.c.r)

1.0.2 Exercícios

1. Mostre que as relações abaixo são relações de equivalência e determine um s.c.r para cada uma delas.
   (a) $\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}; n|(x - y)\}$
   (b) $\mathcal{R} = \{(\upsilon, \omega) \in \mathbb{R}^2 \times \mathbb{R}^2; \upsilon - \omega$ é paralelo ao eixo das abscissas.$\}$
   (c) Considere o subespaço vetorial $\Omega \subset \mathbb{R}^3$, gerado por $\{(1, 0, 0), (0, 1, 0)\}$. Seja $\mathcal{R} = \{(\upsilon, \omega) \in \mathbb{R}^3 \times \mathbb{R}^3; \upsilon - \omega \in \Omega\}$.
   (d) Seja $\mathbb{R}[x]$ o conjunto dos polinômios de coeficientes Reais e variável x. Seja $\mathcal{R} = \{(f(x), g(x)) \in \mathbb{R}[x] \times \mathbb{R}[x]; (x^2 + 1)|(f(x) - g(x))\}$
2. Encontre a classe dos elementos $2, (1, 1), (1, 1, 1), x^4 + x^3 + x + 1$, com respeito, respectivamente, as relações (a),(b),(c) e (d) acima.

3. Represente geometricamente as classes de equivalência das relações do exercício 1.

4. Por que as seguintes relações não são relações de equivalência? O que falha ?

   (a) $\mathcal{R} = \{(x, y) \in \mathbb{N} \times \mathbb{N}; y = x + 2\}$
   (b) $\mathcal{R} = \{(x, y) \in \mathbb{N} \times \mathbb{N}; y|x\}$
   (c) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R}; y|x\}$
   (d) $\mathcal{R} = \{(\upsilon, \omega) \in \mathbb{R}^3 \times \mathbb{R}^3; \upsilon \perp \omega\}$.

5. Considere um conjunto com 5 elementos e construa ao menos dois exemplos de relação de equivalência sobre o mesmo.

6. Seja $\mathcal{C}^0(\mathbb{R})$ o conjunto das funções contínuas definidas em $\mathbb{R}$ e com contra-domínio $\mathbb{R}$.

   (a) Determine para quais valores de $\alpha \in \mathbb{R}$ a relação

   $$\mathcal{R} := \{(f, g) \in \mathcal{C}^0(\mathbb{R}) \times \mathcal{C}^0(\mathbb{R}); \lim_{x \to 0}(f - g)(x) = \alpha.\}$$

   é uma relação de equivalência.
   (b) A relação $\mathcal{R} := \{(f, g) \in \mathcal{C}^0(\mathbb{R}) \times \mathcal{C}^0(\mathbb{R}); (f - g)$ é função par.$\}$ é uma relação de equivalência?
   (c) A relação $\mathcal{R} := \{(f, g) \in \mathcal{C}^0(\mathbb{R}) \times \mathcal{C}^0(\mathbb{R}); (f \circ g)$ é função par.$\}$ é uma relação de equivalência?
   (d) A relação $\mathcal{R} := \{(f, g) \in \mathcal{C}^0(\mathbb{R}) \times \mathcal{C}^0(\mathbb{R}); (f - g)$ é função constante.$\}$ é uma relação de equivalência?

1.0.3 Relação de Ordem

Definição 1.3. *dado um conjunto não vazio $\mathbb{E}$. Uma relação $\mathfrak{O} \subseteq \mathbb{E} \times \mathbb{E}$ é dito ser uma relação de ordem, em $\mathbb{E}$, se satisfaz:*

1. A relação $\mathfrak{O}$ é reflexiva. isto é, $(x, x) \in \mathfrak{O} \quad \forall x \in \mathbb{E}$.
2. A relação $\mathfrak{O}$ é anti-simétrica. isto é, Se $(x, y) \in \mathfrak{O}$ e $(y, x) \in \mathfrak{O}$, então $x = y$.
3. A relação $\mathfrak{O}$ é transitiva. Isto é, Se $(x, y), (y, z) \in \mathfrak{O}$, então $(x, z) \in \mathfrak{O}$.

Observação 1.4. *Observe que no ítem (2) da definição acima não exigimos que para $x, y \in E$ tenha-se $(x, y) \in \mathfrak{O}$ ou $(y, x) \in \mathfrak{O}$. Quando tal propriedade é verdadeira dizemos que a ordem é total, e o conjunto $\mathbb{E}$ é totalmente ordenado. Caso tal propriedade não ocorra, diremos que o conjunto $\mathbb{E}$ é parcialmente ordenado.*

1.0.4 Exercícios

1. Considere um conjunto com 5 elementos e construa um exemplo de relação de ordem parcial e de ordem total.

2. Mostre que as relações abaixo são relações de ordem em seus respectivos conjuntos,e determine quais conjuntos são parcialmente ordenado e quais são totalmente ordenado.

   (a) $\mathfrak{O}_1 = \{(x,y) \in \mathbb{N} \times \mathbb{N}$ tal que $x = y$ ou $y = x + n$ para algum $n \in \mathbb{N}.\}$ (Ordem menor ou igual: $x \leq y$)

   (b) $\mathfrak{O}_3 = \{(x,y) \in \mathbb{N} \times \mathbb{N}$ tal que $x = y$ ou $x = y + n$ para algum $n \in \mathbb{N}.\}$ (Ordem maior ou igual : $x \geq y$)

   (c) $\mathfrak{O} = \{(\mathbb{A}, \mathbb{B}) \in 2^{\mathbb{X}} \times 2^{\mathbb{X}}$ tal que $\mathbb{A} \subseteq B\}$, onde $2^{\mathbb{X}}$ representa o conjunto dos subconjuntos de um conjunto $\mathbb{X}$ não vazio.

   (d) Fixado $m \in \mathbb{N}$. Seja $\mathfrak{O}_4 = \{((\alpha_1, \ldots, \alpha_m), (\beta_1, \ldots, \beta_m)) \in \mathbb{N}^m \times \mathbb{N}^m$ tal que $\alpha_\imath \geq \beta_\imath \forall i \in \{1, \ldots, m\}$ ou $\alpha_\imath = \beta_\imath \forall \imath \in \{1, 2, \ldots, \jmath\}$ e $\alpha_{\jmath+1} > \beta_{\jmath+1}$ para algum $\jmath.\}$ (ordem lexicográfica)

3. Fixado um primo $p \in \mathbb{N}$, assuma $p^0 := 1$. A relação

   $$\mathcal{R} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \text{ tal que } p^r | x \text{ e } p^{r+1} \not| y, \text{ para algum } r \in \{0,1,2,3,\ldots\}\}$$

   é uma relação de ordem?

4. Mostre que as seguintes propriedades são verdadeiras. (Assuma $\mathbb{N} = \{1, 2, \ldots\}$.)

   (a) Se $x \leq y$ então, $x + z \leq y + z \quad \forall z \in \mathbb{N}$.

   (b) Sejam $x, y, z \in \mathbb{N}$. Se $x \leq y$ e $1 \leq z$ então, $x \cdot z \leq y \cdot z$.

   (c) Sejam $x, y, z, w \in \mathbb{N}$. Se $x \leq y$ e $1 \leq z \leq w$ então, $x \cdot z \leq y \cdot w$.

   (d) Sejam $x, y \in \mathbb{N}$. Se $x \cdot y = 1$ então, $x = 1$ e $y = 1$.

Capítulo 2

O conjunto dos Números inteiros

Neste capítulo estudaremos o conjunto dos números inteiros e sua construção a partir do conjuntos dos números naturais. Para tanto, discutiremos algumas questões a respeito dos números Naturais. Ao longo do texto introduziremos o conceito de relação de equivalência e de ordem. Os números inteiros serão então construídos segundo as idéais de Richard Dedekind, apresentado no livro: "Was sind und was sollen die Zahlen?,-- O que são e para que servem os números inteiros – publicado por volta de 1890.

2.1 O conjunto dos números Naturais

Certamente a noção de contagem é um fator comum a todos os seres que conseguem interagir com o ambiente à sua volta, de forma racional. Os animais contam, intuitivamente, suas crias, e esta forma rudimentar de matemática é um dos ingredientes indispensáveis á sobrevivência da espécie. Experiências com Golfinhos e Macacos mostram que estes animais conseguem racionalizar quantidades discretas; Em outras palavras, conseguem contar coisas e classificá-las segundo uma noção de quantidade. Não se sabe se estes animais concebem a noção de infinitude. Algumas espécies animais, não conseguem distiguir quantidades acima de 5 elementos, o que nos levar a questionar se esta limitação pode ocorrer ao Ser Humano. O que vc acha ? Será que você seria capaz de distinguir um conjunto com 1000 elementos, de outro com 999 ? Uma pessoa comum certamente dirá que visualmente é impossível distingui- los, mas que se efetuarmos a contagem saberemos distingui-los. Neste momento, justificamos a necessidade da aceitaçãoda existência dos números Naturais, sem o qual a distinção entre conjuntos com uma quantidade, muito grande, de elementos seria impossível ao Ser Humano.

O nome *Natural* é sem dúvida alguma muito bem empregado para representar esta primeira noção de uma sistema tização matemática para uma necessidade Hu-

mana. Natural significa: que existe sem intervenção Humana, que é produzido pela natureza, que é nato, institivo ou ainda que decorre normalmente da ordem das coisas. Embora esta noção tenha nascido com o Homem em sua fase racional, e tenha sido utilizada durante toda a História, apenas em 1889, foi apresentada uma construção, ou melhor formalizaçãoda noção de número natural, através dos Axiomas de Peano, exposto no livro "Arithmetice princípia novo methodo expositá´ – Novo mt́odo de exposição dos princípios da Aritmética– embalado pelo movimento de axiomatização da Matemática iniciado anos antes por Georg Cantor e seus trabalhos sobre teoria dos conjuntos. Este movimento e a redação inicial dos Axiomas de Peano receberam duras críticas de vários matemáticos famosos, entre eles Kronecker e Henri Poincaré. Segundo eles a teoria dos conjuntos permitia muitos paradoxos e portanto era evidente que a Matemática não poder-se -ia explicar apenas com as imposições da lógica. Sobre os Axiomas de Peano, Poinacaré declarou: " O Sistema de números Naturais é intuitivo mas, o princípio da indução matemática não se reduz a Lógica... Além disto as entidades Matemáticas precisam ser apresentadas numa seqüência que vai do particular para o geral." Para ele era inadmissível uma objeto matemático ser apresentado e elucidado por meio de uma classe ao qual o próprio objeto pertence. O ponto central da discussão a cerca dos Axiomas de Peano era que ao tentar definir os Naturais através deles, encontramos não apenas um conjunto, mais uma classe de conjuntos com as mesmas propriedades. Uma herança deste questionamento é a eterna dúvida que atormenta os alunos num primeiro curso de Álgebra – O Número zero é ou não é um número Natural ? Há evidências de que os Babilônios por volta de 2400AC já usavam a noção do número zero, embora não possuissem representação para o mesmo, porém tanto o símbolo quanto o objeto matemático só foram formalizados milhares de anos depois pelos matemáticos indianos por volta de 650DC. Alguns matemáticos aceitavam o conjunto dos números naturais sem a ocorrência do zero, entretanto com a evoluçãodos argumentos algébricos percebemos que o zero é um filho adotivo que se integrou muito bem à família e portanto deve ser considerado como um membro da mesma. Além disto se precisamos reconhecer sistema de números Naturais não apenas como um conjunto mas sim como uma estrutura algébrica que faz parte de uma classe maior (Semigrupo) , então considerar o zero como um número Natural é perfeitamente justificável. Vale salientar que tanto $\{1, 2, 3, ...\}$ quanto $\{0, 1, 2, 3, ...\}$ satisfazem os axiomas de Peano. A saber:

Axioma 2.1. *[Axiomas de Peano] Existe um conjunto* $\mathbb{N}$ *satisfazendo as seguintes propriedades*

1. O conjunto $\mathbb{N}$ é não vazio.
2. Existe uma função injetora $\mathfrak{S} : \mathbb{N} \to \mathbb{N}$ cuja imagem tem como complementar um conjunto unitário.

3. Para todo subconjunto de $\mathbb{P} \subset \mathbb{N}$ tal que $\mathbb{P}$ contém o complementar da imagem de $\mathfrak{S}$ e contém a imagem de cada elemento de $\mathbb{P}$, tem-se $\mathbb{P} = \mathbb{N}$.

A aplicação $\mathfrak{S}$ do segundo axioma é chamada de sucessão e a imagem de um elemento é chamada de sucessor deste elemento. O terceiro axioma é chamado de *Princípio da indução* e é utilizado pra mostrar que se uma proposição é válida para o primeiro dos Naturais e também é valida para o sucessor de cada um deles, então esta proposição é válida para todos os Naturais. Vamos utilizar a representação Indu-Arábica para os números Naturais, escrevendo-os numa lista, usando o sistema decimal de representação:

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ..., 20, 21, ...\}$$

Nesta lista cada elemento é o sucessor do anterior, exceto o símbolo "1". (Tente pensar, neste momento, os símbolos sem associá-los a quantidade de objetos!!!).

A natureza histórica dos números Naturais exige da mente Humana que associe a cada número natural um conjunto com uma certa quantidade de elementos e seu sucessor é um conjunto com um elemento " a mais". Desta forma, podemos definir de maneira natural a operação de soma de números naturais e associá-la a noçãode união de conjuntos, fazendo-a intimamente dependente da sucessão.

Definição 2.2 (Soma)**.** *Seja $\mathbb{N}$ o conjunto dos números Naturais, representado com acima. Definamos a soma de números naturais como se segue:*

$$\begin{array}{rcccl} + & : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (1, x) & \mapsto & \mathfrak{S}(x) \\ & & (x, 1) & \mapsto & \mathfrak{S}(x) \\ & & (\mathfrak{S}(x), y) & \mapsto & \mathfrak{S}(x + y) \\ & & (x, \mathfrak{S}(y)) & \mapsto & \mathfrak{S}(x + y) \end{array}$$

, ou equivalentemente,(para uma notação mais curta)

$$1{+}x = x{+}1 := \mathfrak{S}(x) \qquad \text{e} \qquad \mathfrak{S}(x){+}y := \mathfrak{S}(x{+}y) \qquad x{+}\mathfrak{S}(y) := \mathfrak{S}(x{+}y) \quad \forall x, y \in \mathbb{N}.$$

A segunda igualdade nos diz que se sabemos somar x com y então sabemos somar o sucessor de x com y. Assim temos

$$1 + 1 := \mathfrak{S}(1) = 2 \qquad 2 + 1 = \mathfrak{S}(1) + 1 := \mathfrak{S}(1 + 1) = \mathfrak{S}(2) = 3$$

e assim por diante.

Definição 2.3. *Seja $\mathbb{N}$ o conjunto dos números Naturais, representado com acima. Definamos o produto de números naturais como se segue:*

$$\begin{array}{rccl} \cdot & : & \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (1,x) & \mapsto & x \\ & & (x,1) & \mapsto & x \\ & & (\mathfrak{S}(x),y) & \mapsto & (x\cdot y)+y \\ & & (y,\mathfrak{S}(x)) & \mapsto & (x\cdot y)+y \end{array}$$

ou equivalentemente,(para uma notação mais curta)

$$1\cdot x = x\cdot 1 := x \qquad \text{e} \qquad \mathfrak{S}(x)\cdot y = y\cdot\mathfrak{S}(x) := x\cdot y + y \quad \forall x,y\in\mathbb{N}.$$

Um raciocínio análogo ao feito para soma, nos fornece:

$$1\cdot 1 := 1 \quad , 2\cdot 3 = \mathfrak{S}(1)\cdot 3 := 1\cdot 3+3 := \mathfrak{S}(2+3) = 6.$$

2.1.1 Exercícios

1. Mostre que com as definições acima, as afirmações abaixo são verdadeiras.
   (a) As operações de soma e o produto de números Naturais são comutativas.
   (b) As operações de soma e o produto de números Naturais são associativas.
   (c) Se $n \neq 1$, então $n+1 = \mathfrak{S}^n(1)$ em que $\mathfrak{S}^n$ representa a composição de n funções iguais a $\mathfrak{S}$.
   (d) Vale a distributividade, isto é, $x(y+z) = xy+xz \quad \forall x,y,z\in\mathbb{N}$.
   (e) Valem as leis do cancelamento:
      i. Se $x+y = x+z$ então $y = z$.
      ii. Se $xy = xz$ então $y = z$.
2. Mostre que $\mathcal{O} := \{(x,y)\in\mathbb{N}\times\mathbb{N}; x = y \text{ ou } x = \mathfrak{S}^r(y) \text{ para algum } r\in\mathbb{N}\}$ é uma relação de ordem total.
3. Todo subconjunto, não vazio, de $\mathbb{N}$, tem um menor elemento com respeito a ordem enunciada acima . **(Princípio da boa ordem)**
4. Se somar dois valores representa a cardinalidade de um conjunto obtido pela união de conjuntos cujas cardinalidades são os valores somados, o que significa a multiplicação em termos de conjuntos ?
5. Definina o significado de x^y por meio das operações de soma e produto e prove que $x^y\cdot x^z = x^{y+z}$. Interprete esta operação em termos de conjuntos.
6. Mostre que todo subconjunto de $\mathbb{M}\subseteq\mathbb{N}$ possui um elemento que não é sucessor de nenhum outro lemento de $\mathbb{M}$.

7. Prove por indução as seguintes proposiçõessobre números naturais:

   (a) $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

   (b) $1 + 3 + 5 + \cdots + (2n + 1) = (n + 1)^2$

   (c) $n < 2^n \quad \forall n \in \mathbb{N}$

   (d) $2^n < n! \quad \forall n \geq 4.$

   (e) $1 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}(n(n + 1))^2.$

   (f) $\displaystyle\sum_{r=1}^{n} 2r = n(n + 1) \quad \forall n \geq 1$

   (g) $1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1 \quad \forall n > 1$

   (h) $\displaystyle\sum_{r=1}^{n} r^2 = \frac{1}{6}n(n + 1)(2n + 1) \quad \forall n \geq 1$

   (i) $4^n - 1$ e $2^{2n+1} + 1$ são divisíveis por 3 $\qquad \forall n \geq 1.$

   (j) 4 divide $7^n - 3^n \quad \forall n \geq 1.$ (*dica: some e subtraia* $7 \cdot 3^n$ *a expressão obtida para* $n + 1$.)

   (k) $(x + y)^n = x^n + \displaystyle\sum_{r=1}^{n} \binom{n}{r} x^{n-r}y^r \quad \forall n \geq 2.$

   (l) $\displaystyle\sum_{r=1}^{n}(r^5 + r^7) = 2[\frac{1}{2}n(n + 1)]^4 \quad \forall n \geq 1$

   (m) $\displaystyle\sum_{r=1}^{n} \frac{1}{r(r + 1)} = \frac{n}{n + 1} \quad \forall n \geq 1$

   (n) A soma das medidas dos ângulos internos de um polígono de n lados, $n \geq 3$, é $\pi(n - 2)$.

8. Seja $\mathbb{B}$ um conjunto com n elementos. Mostre que existem 2^n subconjuntos, distintos, contidos em $\mathbb{B}$ — (incluindo o conjunto vazio).

9. Seja $\mathbb{B}$ um conjunto com n elementos.

   (a) Se $n \geq 2$, prove por indução que a quantidade de subconjuntos de $\mathbb{B}$, distintos, com dois elementos é igual a $\frac{n(n-1)}{2}$

   (b) Se $n \geq 3$, prove por indução que a quantidade de subconjuntos de $\mathbb{B}$, distintos, com três elementos é igual a $\frac{n(n-1)(n-2)}{3!}$

   (c) Enuncie uma conjectura, com resultado similar aos enunciados acima, para o caso $n \geq r$

(d) Conclua que a quantidade de subconjuntos, distintos, contidos em $\mathbb{B}$ é $\sum_{r=0}^{n} \binom{n}{r}$

10. Seja $\mathbb{B}$ um conjunto com n elementos. Mostre que o número de funções injetoras, distintas, de $\mathbb{B}$ em $\mathbb{B}$ é $n!$.

11. Seja $x \in \mathbb{R}$ tal que $x > -1$. Mostre que para todo número natural n tem-se $(1+x)^n \geq 1 + nx$.

12. Considere o problema das torres de Hanói com n discos, $n \geq 3$. Mostre que a solução com o menor número de movimentos possível é obtida com $2^n - 1$ movimentos. (*Se não conheces o problema visite o laboratório de matemática*)

13. Mostre que para cada função sucessão, existe uma única função de soma e de produto definida como acima.

14. Considere o zero como número Natural e defina uma sucessão, uma soma e um produto que preserve a noção atual de soma e produtos de números Naturais. Mostre que assumir o terceiro axioma de Peano em um dos dois casos –zero é Natural ou zero não é Natural – implica na validade deste mesmo axioma para o outro.

2.2 Os Números Inteiros segundo Dedekind

A seguir apresentaremos os Números inteiros como um conjunto de classes de equivalência de uma relação definida sobre o conjunto dos números Naturais. Uma característica bastante peculiar desta construção é a obtençãodo elemento zero (elemento neutro da soma de números inteiros), como número inteiro, mesmo que não admitamos a ocorrência deste elemento neutro no conjunto dos números naturais.

2.2.1 A construção dos Inteiros

Considere a relação de equivalência, $\mathcal{R}$, de $\mathbb{N} \times \mathbb{N}$, dada por

$$\mathcal{R} := \{((a,b),(c,d)) \in \mathbb{N}^2 \times \mathbb{N}^2; a + d = b + c\}. \tag{2.1}$$

Representemos por $\mathcal{R}_{(a,b)}$ a classe do elemento $(a,b) \in \mathbb{N} \times \mathbb{N}$. Isto é,

$$\mathcal{R}_{(a,b)} := \{(x,y) \in \mathbb{N} \times \mathbb{N}; a + y = b + x\}$$

e seja $\mathbb{Z} := \{\mathcal{R}_{(a,b)}; (a,b) \in \mathbb{N} \times \mathbb{N}\}$ o conjuto quociente de $\mathbb{N}^2$ pela relação $\mathcal{R}$ dada em 2.1.

Definição 2.4 (conjunto dos Inteiros)**.** *O conjunto $\mathbb{Z}$ definido acima, é dito ser o conjunto dos Números Inteiros, e cada elemento deste conjunto é dito ser um número inteiro.*

No conjunto dos Números inteiros é possível definir duas operações chamadas de soma e produto, que herda a comutatividade, associatividade, e a leis de cancelamento, presentes no conjunto dos Números Naturais. Além disto o conjunto dos números inteiros sempre possui um elemento neutro para a soma, este número, chamado de zero, independe de considerar-mos ou não a existência do zero como um número Natural.

Definição 2.5 (Soma de Inteiros)**.** *Seja $\mathbb{Z} = \{\mathcal{R}_{(a,b)}; (a,b) \in \mathbb{N} \times \mathbb{N}\}$ o conjunto quociente pela relação $\mathcal{R}$ dada em 2.1. A aplicação definida por:*

$$\begin{array}{rccc} + & : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & (\mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)}) & \mapsto & \mathcal{R}_{(a+x,b+y)} \end{array}$$

é dita ser a *operação de soma* de números inteiros. Escreveremos, por motivo de simplicidade, $\mathcal{R}_{(a,b)} + \mathcal{R}_{(x,y)}$, em lugar de $+(\mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)})$. Observe que a aplicação de soma definida acima não depende da escolha dos representantes. De fato, se $\mathcal{R}_{(a,b)} = \mathcal{R}_{(c,d)}$ e $\mathcal{R}_{(x,y)} = \mathcal{R}_{(u,w)}$, então $a + d = b + c$ e $x + w = y + u$. Portanto,

$$(a+d)+(x+w) = (a+x)+(d+w) \quad = \quad (b+c)+(y+u) = (b+y)+(c+u)$$

, ou equivalentemente $\mathcal{R}_{(a+x,b+y)} = \mathcal{R}_{(c+u,d+w)}$.

Proposição 2.6. *A aplicação de soma $+ : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ tem as seguintes propriedades:*

1. A soma é comutativa. Isto é,

$$\mathcal{R}_{(a,b)} + \mathcal{R}_{(x,y)} = \mathcal{R}_{(x,y)} + \mathcal{R}_{(a,b)}. \quad \forall \mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)} \in \mathbb{Z}.$$

2. A soma é Associativa. Isto é,

$$(\mathcal{R}_{(x,y)} + \mathcal{R}_{(a,b)}) + \mathcal{R}_{(c,d)} = \mathcal{R}_{(x,y)} + (\mathcal{R}_{(a,b)} + \mathcal{R}_{(c,d)}) \quad \forall \mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)}, \mathcal{R}_{(c,d)} \in \mathbb{Z}.$$

3. Existe elemento neutro para a Soma, chamado de zero.

4. Cada elemento tem um oposto aditivo. Isto é, para cada elemento $\mathcal{R}_{(a,b)} \in \mathbb{Z}$, existe elemento $\mathcal{R}_{(x,y)}$ tal que $\mathcal{R}_{(a,b)} + \mathcal{R}_{(x,y)}$ é o elemento neutro da soma.

Demonstração. Deixamos os itens (1) e (2) como exercício. Para mostrar a existência do elemento neutro , basta observar que a classe $\mathcal{R}_{(x,x)}$ satisfaz:

$$\mathcal{R}_{(x,x)} + \mathcal{R}_{(a,b)} = \mathcal{R}_{(x+a,x+b)}.$$

Como $b + (x + a) = a + (x + b)$, concluimos que $(a, b) \in \mathcal{R}_{(x+a,x+b)}$. Portanto pelo teorema 1.2, temos que $\mathcal{R}_{(a,b)} = \mathcal{R}_{(x+a,x+b)}$. Isto é,

$$\mathcal{R}_{(x,x)} + \mathcal{R}_{(a,b)} = \mathcal{R}_{(a,b)} \quad \forall x \in \mathbb{N}, \mathcal{R}_{(a,b)} \in \mathbb{Z}.$$

Para mostrar que todo elemento tem um elemento oposto, basta observar que

$$\mathcal{R}_{(a,b)} + \mathcal{R}_{(b,a)} = \mathcal{R}_{(a+b,b+a)} = \mathcal{R}_{(a+b,a+b)} = \mathcal{R}_{(x,x)} \quad \forall x, a, b \in \mathbb{N}.$$

□

Definição 2.7 (Produto de Inteiros)**.** *Seja* $\mathbb{Z} = \{\mathcal{R}_{(a,b)}; (a, b) \in \mathbb{N} \times \mathbb{N}\}$ *o conjunto quociente pela relação* $\mathcal{R}$ *dada em 2.1. A aplicação definida por:*

$$\begin{array}{rccc} \cdot & : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & (\mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)}) & \mapsto & \mathcal{R}_{(ax+by,ay+bx)} \end{array}$$

é dita ser a *operação produto* de números inteiros. Escreveremos, por motivo de simplicidade, $\mathcal{R}_{(a,b)} \cdot \mathcal{R}_{(x,y)}$, em lugar de $\cdot(\mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)})$.

Proposição 2.8. *A aplicação produto* $\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ *tem as seguintes propriedades:*

1. O produto é comutativo. Isto é,
   $\mathcal{R}_{(a,b)} \cdot \mathcal{R}_{(x,y)} = \mathcal{R}_{(x,y)} \cdot \mathcal{R}_{(a,b)}. \quad \forall \mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)} \in \mathbb{Z}.$
2. O produto é Associativo. Isto é,
   $(\mathcal{R}_{(x,y)} \cdot \mathcal{R}_{(a,b)}) \cdot \mathcal{R}_{(c,d)} = \mathcal{R}_{(x,y)} \cdot (\mathcal{R}_{(a,b)} \cdot \mathcal{R}_{(c,d)}) \quad \forall \mathcal{R}_{(a,b)}, \mathcal{R}_{(x,y)}, \mathcal{R}_{(c,d)} \in \mathbb{Z}.$
3. Existe elemento neutro para o produto, chamado de Hum.

Demonstração. Deixamos os itens (1) e (2) como exercícios. Para mostrar a existência do elemento neutro, basta observar que para todo $x \in \mathbb{N}$ tem-se:

$$\mathcal{R}_{(x+1,x)} \cdot \mathcal{R}_{(a,b)} = \mathcal{R}_{((x+1)a+xb,xa+(x+1)b)} = \mathcal{R}_{(xa+a+xb,xa+bx+b)},$$

e que por outro lado, $a + (xa + bx + b) = b + (xa + a + xb)$ o que significa dizer que $(a, b) \in \mathcal{R}_{(xa+a+xb,xa+bx+b)}$. Portanto

$$\mathcal{R}_{(x+1,x)} \cdot \mathcal{R}_{(a,b)} = \mathcal{R}_{((x+1)a+xb,xa+(x+1)b)} = \mathcal{R}_{(a,b)}.$$

□

Observação 2.9. *Alguns autores, simplesmente citam a classe* $\mathcal{R}_{(1,0)}$ *como representante do número inteiro Hum . Entretanto tal afirmação pressupõe a aceitação do zero como número Natural, fato absolutamente desnecessário para a construção dos inteiros.Assim a classe* $\mathcal{R}_{(2,1)}$ *é muito mais elegante como representante do número Hum.*

2.2.2 Ordem nos Inteiros

Nesta seção mostraremos que o conjunto dos Naturais é um conjunto totalmente ordenado pela sucessão e que a ordem dos Naturais é herdada pelo conjunto dos números inteiros. Uma conseqüência natural do conceito de ordem total é a trisecção do conjunto em subconjuntos disjuntos dois-a-dois. Em razão desta propriedade,poderemos triseccionar o conjunto dos números inteiros na união dos conjuntos dos inteiros estritamente negativos, com o conjunto unitário composto pelo zero, e com os inteiros estritamente positivos. Além disto, mostraremos que o conjunto do números inteiros possui um subconjunto que é uma cópia do conjunto dos numeros naturais.

Considerando a ordem $\mathfrak{O}_{\mathbb{N}} = \{(x, y) \in \mathbb{N} \times \mathbb{N}; x = y \text{ ou } y = x + n \text{ para algum } n \in \mathbb{N}\}$, escreveremos $x \leq y$ sempre que $(x, y) \in \mathfrak{O}_{\mathbb{N}}$, e diremos que x é menor ou igual a y. Usaremos a expressão $x < y$ para indicar que $x \leq y$ e $x \neq y$, e neste caso, diremos que x é menor, ou estritamente menor, que y. Com a notação acima, podemos então definir uma ordem, chamada de *" menor ou igual ´ ´*, no conjunto dos números inteiros, dada no teorema abaixo, que herda todas as propriedades da ordem de números naturais, comforme listada nos Exercícios 2.2.3.

Teorema 2.10. *A relação*

$$\mathfrak{O}_{\mathbb{Z}} := \{(\mathcal{R}_{(x,y)}, \mathcal{R}_{(a,b)}) \in \mathbb{Z} \times \mathbb{Z}; x + b \leq y + a\}$$

é uma ordem total em $\mathbb{Z}$.

Demonstração. Escrevamos $\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(a,b)}$ para indicar que $(\mathcal{R}_{(x,y)}, \mathcal{R}_{(a,b)} \in \mathfrak{O}_{\mathbb{Z}}$. Antes de mostrar que que $\mathfrak{O}_{\mathbb{Z}}$ é de fato uma ordem, mostremos que a condição $\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(a,b)}$ não depende da escolha dos representantes das classes $\mathcal{R}_{(x,y)}$ e $\mathcal{R}_{(a,b)}$. De fato, se $\mathcal{R}_{(x,y)} = \mathcal{R}_{(u,w)}$ e $\mathcal{R}_{(a,b)} = \mathcal{R}_{(c,d)}$ então,

$$x + w = y + u \text{ e } a + d = b + c. \tag{2.2}$$

Portanto se, $x + b \leq y + a$ então:

$$(u + b) + (x + y) = (x + b) + (y + u) \leq (y + a) + (x + w) = (w + a) + (x + y) \tag{2.3}$$

Pela lei do cancelamento, da ordem dos naturais, temos:

$$u + b \leq w + a.$$

Portanto pela definição de $\mathfrak{O}_{\mathbb{Z}}$, temos $\mathcal{R}_{(u,w)} \leq \mathcal{R}_{(a,b)}$. Em outras palavras, estar ou não na relação $\mathfrak{O}_{\mathbb{Z}}$ não depende dos representantes escolhidos. Prossigamos para mostrar que $\mathfrak{O}_{\mathbb{Z}}$ é reflexiva, anti-simétrica, transitiva.

1. $\mathfrak{O}_{\mathbb{Z}}$ é reflexiva. Pois para todo elemento $\mathcal{R}_{(x,y)} \in \mathbb{Z}$ temos: $x + y = y + x$. Logo $\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(x,y)}$.

2. $\mathfrak{O}_{\mathbb{Z}}$ é anti-simétrica. Suponha $\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(a,b)}$. e $\mathcal{R}_{(a,b)} \leq \mathcal{R}_{(x,y)}$. Neste caso, de acordo com a definição de $\mathfrak{O}_{\mathbb{Z}}$, temos:

$$x + b \leq y + a \text{ e } a + y \leq b + x \quad \text{ com } x, y, a, b \in \mathbb{N}. \tag{2.4}$$

Portanto, $x+b = y+a$, e pela construção do conjunto dos inteiros , isto significa que $(a, b) \in \mathcal{R}_{(x,y)}$, ou seja $\mathcal{R}_{(x,y)} = \mathcal{R}_{(a,b)}$.

3. $\mathfrak{O}_{\mathbb{Z}}$ é transitiva. Suponha $\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(a,b)}$, e $\mathcal{R}_{(a,b)} \leq \mathcal{R}_{(c,d)}$. Neste caso temos,

$$x + b \leq y + a \text{ e } a + d \leq b + c.$$

Portanto,

$$(x + d) + (b + a) = (x + b) + (a + d) \leq (y + a) + (b + c) = (y + c) + (b + a).$$

Aplicando-se a lei do cancelamento, da ordem dos naturais, temos que $x + d \leq y+c$, e de acordo com a definição de $\mathfrak{O}_{\mathbb{Z}}$ concluimos que $\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(c,d)}$. Portanto $\mathfrak{O}_{\mathbb{Z}}$ é transitiva.

Desta forma conluimos que $\mathfrak{O}_{\mathbb{Z}}$ é uma ordem em $\mathbb{Z}$. Resta mostrar que é uma ordem total. De fato, dados $\mathcal{R}_{(x,y)}, \mathcal{R}_{(a,b)} \in \mathbb{Z}$, como a ordem "menor ou igual"é uma ordem total nos Naturais, temos que

$$x + b \leq y + a \text{ ou } y + a \leq x + b.$$

Esta afirmação por sua vez, é eqivalente a dizer que:

$$\mathcal{R}_{(x,y)} \leq \mathcal{R}_{(a,b)} \text{ ou } \mathcal{R}_{(a,b)} \leq \mathcal{R}_{(x,y)}.$$

Portanto a ordem $\mathfrak{O}_{\mathbb{Z}}$ é uma ordem total. □

Proposição 2.11. *Seja $\omega = \mathcal{R}_{(x,y)} \in \mathbb{Z}$. Representemos pelo símbolo* "0" *a classe do elemento neutro para a soma em $\mathbb{Z}$. Considerando a ordem $\mathfrak{O}_{\mathbb{Z}}$ acima, temos:*

1. $0 \leq \omega$ se, e somente se, $y \leq x$.
2. $\omega \leq 0$ se, e somente se, $x \leq y$.

Demonstração. Lembremos que o elemento neutro da soma em $\mathbb{Z}$ é dado pela classe $\mathcal{R}_{(z,z)}$, com $z \in \mathbb{N}$. Portanto, para mostrar o ítem (1) basta observar que:

$$\mathcal{R}_{(z,z)} \leq \mathcal{R}_{(x,y)} \Longrightarrow z + y \leq z + x \Longrightarrow y \leq x.$$

A demonstração do ítem (2) ́feita de forma análoga. □

Definição 2.12. *Considere o conjunto dos números inteiros, munido da ordem total* $\mathfrak{O}_{\mathbb{Z}}$ *dada acima. Os conjuntos, descritos abaixo, são chamados, respectivamente de conjunto dos inteiros positivos e conjuto dos inteiros negativos*

$$\mathbb{Z}_+ := \{\omega \in \mathbb{Z}; 0 \leq \omega \ e \ \omega \neq 0\} = \{\mathcal{R}_{(x,y)}; y < x\}$$

$$\mathbb{Z}_- := \{\omega \in \mathbb{Z}; \omega \leq 0 \ e \ \omega \neq 0\} = \{\mathcal{R}_{(x,y)}; x < y\}$$

O corolário a seguir é uma conseqüência imediata da proposição 2.11 e da definição acima. Ela afirma que um número inteiro é positivo, negativo ou zero.

Corolário 2.13. *A ordem* $\mathfrak{O}_{\mathbb{Z}}$ *particiona o conjunto* $\mathbb{Z}$ *em três subconjuntos mutuamente disjuntos.*

De fato, temos $\mathbb{Z} = \mathbb{Z}_- \sqcup \{0\} \sqcup \mathbb{Z}_+$. □

O Teorema a seguir caracteriza os números inteiros positivos e negativos, e nos permite pensar os números naturais como subconjunto do conjunto dos números inteiros.

Teorema 2.14. *Considere os conjuntos dos números naturais,*$\mathbb{N} := \{1, 2, 3 \ldots\}$*, e dos inteiros, munidos com as respectivas ordens "menor ou igual´´ . Então:*

1. $\mathbb{Z}_+ = \{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\}$
2. $\mathbb{Z}_- = \{\mathcal{R}_{(1,x)}; x \in \mathbb{N} \text{ e } 1 < x\}$

Demonstração. Observemos que se $x \in \mathbb{N}$ e $1 < x$ então, $z + 1 \leq z + x \quad \forall z \in \mathbb{N}$. Por outro lado, se $x \in \mathbb{N}$ e $x < 1$ então, $z + x \leq z + 1 \quad \forall z \in \mathbb{N}$. Portanto, de acordo com a definição 2.12 temos

$$\{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\} \subseteq \mathbb{Z}_+$$

$$\{\mathcal{R}_{(1,x)}; x \in \mathbb{N} \text{ e } 1 < x\} \subseteq \mathbb{Z}_-$$

Para mostrar as inclusões reversas, procedamos como se segue: Suponha $\mathcal{R}_{(a,b)} \in \mathbb{Z}_+$. Neste caso, pela definição de $\mathbb{Z}_+$, temos que $b < a$, com $a, b \in \mathbb{N}$. Pela definição da ordem "menor ou igual´´ dos números naturais, segue que existe $p \in \mathbb{N}, (1 \leq p)$ tal que $a = b + p$. Portanto $a + 1 = b + p + 1$, o que significa $(a, b) \in \mathcal{R}_{(p+1,1)}$ ou equivalentemente, $\mathcal{R}_{(a,b)} = \mathcal{R}_{(p+1,1)}$. Isto mostra que $\mathbb{Z}_+ \subseteq \{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\}$. Logo $\mathbb{Z}_+ = \{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\}$. De forma análoga: Suponha $\mathcal{R}_{(a,b)} \in \mathbb{Z}_-$. Neste caso, pela definição de $\mathbb{Z}_-$, temos que $a < b$, com $a, b \in \mathbb{N}$. Pela definição da ordem "menor ou igual´´ dos números naturais, segue que existe $p \in \mathbb{N}, (1 \leq p)$ tal que $b = a + p$. Portanto $b + 1 = a + p + 1$. Isto, por sua vez, significa que $(a, b) \in \mathcal{R}_{(1,p+1)}$ ou equivalentemente, $\mathcal{R}_{(a,b)} = \mathcal{R}_{(1,p+1)}$. Isto mostra que $\mathbb{Z}_- \subseteq \{\mathcal{R}_{(1,x)}; x \in \mathbb{N} \text{ e } 1 < x\}$. Logo $\mathbb{Z}_+ = \{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\}$. □

Corolário 2.15. *Se $\mathcal{R}_{(a,b)} = \mathcal{R}_{(x,1)}$ então o oposto(aditivo) de $\mathcal{R}_{(a,b)}$, representado por $-\mathcal{R}_{(a,b)}$ é $\mathcal{R}_{(1,x)} = \mathcal{R}_{(b,a)}$.*

A demonstração é imediata. □

Corolário 2.16. *O conjunto $\mathbb{Z}_+ = \{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\}$ satisfaz os axiomas de Peano.*

Basta mostrar que existe uma bijeção que preserva a a soma (e portanto a sucessão e a ordem), entre o conjunto $\mathbb{N} = \{1, 2, 3, \ldots\}$ e o conjunto $\{\mathcal{R}_{(x,1)}; x \in \mathbb{N} \text{ e } 1 < x\}$. Seja, $\varphi : \mathbb{N} \to \mathbb{Z}_+$ dada por $\varphi(n) = \mathcal{R}_{(n+1,1)}$. Temos:

$$\varphi(n) + \varphi(m) = \mathcal{R}_{(n+1,1)} + \mathcal{R}_{(m+1,1)} = \mathcal{R}_{(n+m+2,2)}$$

Por outro lado, como $(n+m+1)+2 = (n+m+2)+1$ temos $\mathcal{R}_{(n+m+2,2)} = \mathcal{R}_{(n+m+1,1)}$. Portanto,

$$\varphi(n) + \varphi(m) = \varphi(m+n).$$

Além disto, se $\varphi(n) = \varphi(m)$ então $\mathcal{R}_{(n+1,1)} = \mathcal{R}_{(m+1,1)}$, e conseqüentemente temos:$(n+1)+1 = (m+1)+1$, ou seja, $n = m$. Concluimos,portanto, que φ é uma função injetora que preserva a soma, consequentemente preserva a sucessão e a ordem. O teorema 2.14 nos mostra que φ é sobrejetora. □

Observação 2.17. *O que o teorema acima nos garante é que o conjunto $\mathbb{Z}_+$ é um representante legítimo do conjunto dos números Naturais, e que portanto toda propriedade válida para números Naturais, também é válida para os elementos de $\mathbb{Z}_+$, e vice-versa.*

2.2.3 Exercícios

1. Mostre, usando a caracterização dos inteiros como classes de equivalência, que as seguintes afirmações são verdadeiras:
   (a) Se $x \leq y$ então, $x + z \leq y + z \quad \forall z \in \mathbb{Z}$. Em particular, $x - z \leq y - z$.
   (b) Sejam $x, y, z \in \mathbb{Z}$. Se $x \leq y$ e $0 \leq z$ então, $x \cdot z \leq y \cdot z$.
   (c) Sejam $x, y, z \in \mathbb{Z}$. Se $x \leq y$ e $z \leq 0$ então, $y \cdot z \leq x \cdot z$.
   (d) Sejam $x, y, z, w \in \mathbb{Z}$. Se $0 \leq x \leq y$ e $0 \leq z \leq w$ então, $x \cdot z \leq y \cdot w$.
   (e) Sejam $x, y \in \mathbb{Z}$. Se $0 \leq x \leq y$ então, $0 \leq y - x$.
   (f) Sejam $x, y \in \mathbb{Z}$. Se $x \cdot y = 0$ então, $x = 0$ ou $y = 0$.
   (g) Sejam $x, y, z \in \mathbb{Z}$. Se $x \cdot y = 1$ então, $x = y = -1$ ou $x = y = 1$.
   (h) Sejam $x, y \in \mathbb{Z}$. Se $x \leq 0$ e $y \leq 0$ então, $x \cdot y \geq 0$.

(i) Sejam $x, y \in \mathbb{Z}$. Se $x \leq 0$ e $y \geq 0$ então, $x \cdot y \leq 0$.

(j) Sejam $x, y \in \mathbb{Z}$. Se $x \geq 0$ e $y \geq 0$ então, $x \cdot y \geq 0$.

2. Seja $\mathbb{S}$ um conjunto não vazio e totalmente ordenado. Mostre que se existe uma bijeção $\varphi : \mathbb{N} \to \mathbb{S}$ tal que φ preserva a ordem então, $\mathbb{S}$ satisfaz os axiomas de Peano.

2.3 Princípio da Indução sobre os Inteiros

Assumiremos para esta seção que o leitor demonstrou o **princípio do menor Natural**, recomendado enunciado no exercício **3**.

Definição 2.18. *Dizemos que um subconjunto $\mathbb{L} \subseteq Z$ é limitado inferiormente se existe $\omega \in \mathbb{Z}$ tal que $\omega \leq \lambda \quad \forall \lambda \in \mathbb{L}$.*

Teorema 2.19 (Princípio do menor inteiro)**.** *Todo subconjunto $\mathbb{L} \subseteq Z$ limitado inferiormente posui um menor elemento. Isto é, existe $\omega \in \mathbb{L}$ tal que $\omega \leq \lambda \quad \forall \lambda \in \mathbb{L}$.*

Demonstração. Seja $\mathbb{L} \subseteq \mathbb{Z}$ um subconjunto, não vazio, limitado inferiormente. Neste caso, seja $\gamma \in \mathbb{Z}$ tal que $\gamma \leq \lambda \quad \forall \lambda \in \mathbb{L}$. Se $\gamma \in \mathbb{L}$, então γ é o menor elemento de $\mathbb{L}$. Caso contrário, considere o conjunto $\mathbb{V} = \{\lambda + (-\gamma); \lambda \in \mathbb{L}\}$. De acordo com as propriedades da ordem "menor ou igual ´´ temos que $\mathbb{V} \subseteq \mathbb{Z}_+$. Logo,pela observação 2.17, temos que $\mathbb{V}$ possui um menor elemento, digamos: $\omega - \gamma$, com $\omega \in \mathbb{L}$. Este elemento , portanto, satisfaz:

$$\omega - \gamma \leq \lambda - \gamma \quad \forall \lambda \in \mathbb{L}.$$

Portanto,

$$\omega \leq \lambda \quad \forall \lambda \in \mathbb{L}.$$

□.

Teorema 2.20 (Princípio da Indução sobre os Inteiros)**.** *Fixado $\omega \in \mathbb{Z}$. Seja $\mathbb{L} = \{\lambda \in \mathbb{Z}; \omega \leq \lambda\}$. Seja $\mathcal{P}$ uma proposição enunciada para os elementos de $\mathbb{L}$. Tal que $\mathcal{P}$ satisfaz:*

1. $\mathcal{P}$ é válida para ω.
2. Se $\mathcal{P}$ é válida para $\lambda \in \mathbb{L}$, então $\mathcal{P}$ é válida para $\lambda + 1$.

Então $\mathcal{P}$ é válida para todos os elementos de $\mathbb{L}$.

Demonstração. Seja $\mathbb{S}$ o conjunto dos elementos de $\mathbb{L}$ para os quais a afirmação não é válida. Isto é, $\mathbb{S} = \{\gamma \in \mathbb{L}; \mathcal{P}(\gamma)$ não é válida $\}$. Suponha que $\mathbb{S}$ seja não vazio.

Neste caso, $\mathbb{S}$ um subconjunto de $\mathbb{Z}$, limitado inferiormente e, portanto, de acordo com o teorema 2.19, existe um menor elemento $\eta \in \mathbb{S}$. Uma vez que ω é o menor elemento de $\mathbb{L}$ temos $\omega \leq \eta$. Por outro lado, por hipótese,$\mathcal{P}$ é válida para ω. Portanto, $\omega \neq \eta$. Segue-se que, $\omega \leq \eta - 1 < \eta$. Como η é o menor elemento de $\mathbb{L}$ para o qual a proposição $\mathcal{P}$ não é válida, temos que $\mathcal{P}$ é válida para $\eta - 1$, e conseqüentemente, por hipótese, $\mathcal{P}$ é válida para $(\eta - 1) + 1 = \eta$. Chegamos portanto a uma contradição o que nos leva a concluir que $\mathbb{S}$ deve ser vazio. Isto é, a proposição $\mathcal{P}$ é válida para todos os elementos de $\mathbb{L}$.

2.3.1 Exercícios

1. Mostre que todo subconjunto, não vazio, do conjunto dos números inteiros, limitado superiormente, tem um maior elemento.
2. Fixado $\omega \in \mathbb{Z}$. Seja $\mathbb{L} = \{\lambda \in \mathbb{Z}; \lambda \leq \omega\}$. Seja $\mathcal{P}$ uma proposição enunciada para os elementos de $\mathbb{L}$. Tal que $\mathcal{P}$ satisfaz:
   (a) $\mathcal{P}$ é válida para ω.
   (b) Se $\mathcal{P}$ é válida para λ, então $\mathcal{P}$ é válida para $\lambda - 1$.

   Nestas condições , mostre que $\mathcal{P}$ é válida para todos os elementos de $\mathbb{L}$.
3. Prove por indução as seguintes afirmações :
   (a) $n^3 + 2n$ é um múltiplo de 3, para todo $n \geq 1$.
   (b) Fixado uma incógnita x. Tem-se que $1 + x + x^2 + x^3 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}$. (Assuma $x^0 := 1$.)
   (c) Fixado duas incógnitas x, y. Tem-se que $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}$. (Assuma $0! = 1$.)
   (d) 3 divide $x^3 - x \qquad x \in \mathbb{N}$.

2.4 Propriedades Aritméticas dos Inteiros

2.4.1 Divisibilidade

Definição 2.21. *Dados números inteiros $x, y \in \mathbb{Z}$, dizemos que x divide y, se existe $z \in \mathbb{Z}$, tal que $y = x \cdot z$. Neste caso, dizemos que y é um múltiplo de x e o inteiro x é dito ser um divisor de y. Escreveremos $x|y$ para indicar que x divide y.*

As seguintes propriedades seguem imediatamente da definição de divisão.

Proposição 2.22 (Propriedades da divisão)**.** *As seguinte afirmações sobre números inteiros, são verdadeiras.*

1. Sejam $x, y, z \in \mathbb{Z}$. Se $x|y$ e $y|z$ então, $x|z$.
2. Se $x|y$ então $xz|yz$.
3. Se $z \neq 0$ e $xz|yz$ então $x|y$.
4. Se $x|1$ então $x = 1$ ou $x = -1$.
5. Se $x, y \in \mathbb{Z}_+$ e $x|y$ então $x \leq y$.
6. Se $x|y$ então $|x| \leq |y|$. Onde $|z| = \begin{cases} z, & \text{se } 0 \leq z \\ -z, & \text{se } z \leq 0 \end{cases}$
7. Se $x|y$ então $x \leq |y|$.
8. Se $x|y$ e $y|x$ então $|x| = |y|$.
9. Se $x|y$ e $x|z$ então, $x|ay + bz$. $\quad \forall a, b \in \mathbb{Z}$

Demonstração. A demonstração é deixada como exercício.

Definição 2.23. *Um número inteiro $x \in \mathbb{Z}$, é dito ser composto se o conjunto dos divisores de x tem mais que quatro elementos. Isto é, se $x = yz$ com y e z não pertencentes a$\{1, -1, x, -x\}$.*

Definição 2.24. *Um número $x \in \mathbb{Z}$ é dito ser primo se o conjunto dos divisores positivos tem exatamente 2 elementos $\{1, |x|\}$.*

O conjunto dos divisores de um número inteiro, não nulo, tem um número finito de elementos. Isto decorre da propriedade 5 enunciada na proposição 2.22. Podemos concluir que dados dois inteiros $x, y \in \mathbb{Z}$, não simultaneamente nulos, o conjunto dos divisores comuns a x e a y, isto é, o conjunto $\{z \in \mathbb{Z}; z|x \text{ e } z|y\}$, tem um número finito de elementos e, portanto, considerando a ordem "menor ou igual,´´ tem um maior divisor comum. Isto motiva a seguinte definição .

Definição 2.25. *Dados $x, y \in \mathbb{Z}$, não simultaneamente nulos, o Maior Divisor Comum de x ey é o maior inteiro positivo que divide simultaneamente x e y.*

Escreveremos $\mathbf{MDC}(x, y)$ para indicar o maior divisor comum de x e y. A proposição a seguir nos dar a propriedade fundamental do maior divisor comum de dois inteiros, e é utilizada como definição por muitos autores. A razão pela qual eles escolhem definir o MDC pela propriedade universal,é poder estender o conceito de MDC para outros ambientes matemáticos, como por exemplo para o conjunto dos polinômios em uma variável com coeficientes reais.

Teorema 2.26 (Euclides)**.** *Dado um número inteiro $x \notin \{-1, 0, 1\}$ tem-se que x é um número primo ou x é um produto finito de números primos.*

Demonstração. Basta Como $-x = (-1)x$, basta mostrar que todo inteiro positivo maior que 1 ou é primo ou um produto de um número finito de primos.

Para demostrar esta afirmação usaremos o princípio da indução em sua segunda forma. Considere o conjunto $\mathbb{B} = \{z \in \mathbb{Z}; z > 1 \text{ e } z \text{ ou é primo ou produto finito de primos}\}$. Temos que $2 \in \mathbb{Z}$. Dado $x > 2$, suponha que a tese seja válida para todo $y \in \mathbb{Z}$ satisfazendo $2 \leq y < x$. Neste caso, se x for primo teremos $x \in \mathbb{B}$. Caso contário, existem $a, b \notin \{0, 1\}$ ambos positivos e satisfazendo $x = ab$. Decorre da definição de ordem nos inteiros que $x > a \geq 2$ e $x > b \geq 2$. portanto, pela hipótese de indução a e b ou são primos ou produtos de um número finito de primos. Em qualquer dos casos x é um produto de um número finito de primos e $x \in \mathbb{B}$. Pelo princípio da indução, segue que todo número inteiro, maior ou igual a 2, ou é primo ou um produto finito de primos, e consequentemente todo inteiro x tal que $|x| \geq 2$ ou é primo ou produto finito de primos. □

Teorema 2.27. *Existem infinitos primos positivos.*

Demonstração. Suponha que a quantidade de números primos positivos é finita e que $\wp_1 < \wp_2 < \wp_3 < \cdots < \wp_n$ sejam todos os primos positivos listados em ordem crescente. Considere o inteiro positivo $x = \wp_1 \cdot \wp_2 \cdots \wp_n + 1$. Como x é extritamente maior que cada um dos primos $\wp_i$ devemos ter obrigatoriamente, pelo teorema 2.26 que x é um produto de primos e neste caso deve existir $\wp \in \{\wp_1, \ldots, \wp_n\}$ e um inteiro positivo y tais que $x = \wp \cdot y$. Desta forma $\wp$ obrigatoriamente satisfaz $\wp | x$ e $\wp | (\wp_1 \cdot \wp_2 \cdots \wp_n)$. Conseqüentemente tem-se que $\wp | (x - \wp_1 \cdot \wp_2 \cdots \wp_n)$, isto é, $\wp | 1$. O que nos leva a contradizer o fato de $\wp$ ser primo.

Portanto assumir que a quantidade de primos positivo é finita, nos leva a uma contradição da definição de número primo. Logo a quantidade de números primos positivos é infinita. □

2.4.2 Divisão Euclidiana

Teorema 2.28. *Dados $x, y \in \mathbb{Z}$, com $y \neq 0$, existem únicos inteiros q, r, chamados respectivamente de quociente e resto da divisão, tais que:*

$$x = qy + r \qquad com\ 0 \leq r < |y|.$$

Dividiremos a demonstração deste teorema em dois casos: $y > 0$ e $y < 0$.

Se $y > 0$ então $|y| = y$. Neste caso, considere o conjunto $\mathbb{B} = \{x - ay; a \in mathbbZ \text{ e } x - ay \geq 0\}$. O conjunto $\mathbb{B}$ é não vazio e limitado inferiormente pelo zero. Para comprovar este fato, basta observar que $x - (-|x|)y = x + |x|y \geq x + |x| \geq 0$.

Desta forma, existe $r \in \mathbb{B}$ tal que $0 \leq r$ e r é o menor elemento em $\mathbb{B}$. Ou seja, existe $q \in mathbbZ$ tal que $r = x - qy \geq 0$. Para mostrar que $r < |y|$, observamos que se fosse $r > y$ então existiria $\sigma \in \mathbb{N}^*$ satisfazendo $r = y + \sigma$ e $0 < \sigma < r$. Conseqüentemente, teríamos

$$\begin{aligned} y + \sigma &= x - qy \\ \sigma &= x - (q+1)y \in \mathbb{B} \end{aligned}$$

contradizendo a minimalidade de r. Portanto

$$x = qy + r \qquad \text{com } 0 \leq r < |y|.$$

Resta mostrar que q r descritos acima são únicamente determinados por x e y.

Suponha que existam $q, r, b, u \in \mathbb{Z}$ tais que $x = qy + r$ e $x = by + u$ com $0 \leq r < y$ e $0 \leq u < y$. Neste caso, temos $0 \leq |r - u| < y$. Por outro lado,

$$\begin{aligned} by + u &= qy + r \quad \therefore \\ (b-q)y = r - u \quad &\therefore \\ |b-q|y &= |r-u| \end{aligned}$$

Logo, se $r \neq u$ devemos ter $|b - q| \geq 1$ e consequentemente

$$y \leq |b-q|y = |r-u| < y \qquad \text{um absurdo!}$$

Logo $r = u$ e consequentemente $q = b$.

Para o caso em que $y < 0$ aplicamos o primeiro caso para x e $|y|$. neste caso, existem únicos $q', r \in \mathbb{Z}$ tais que

$$x = q'|y| + r \qquad \text{com } 0 \leq r < |y|.$$

Portanto, $x = q'(-y) + r = (-q)y + r$ ou seja, pondo $q = -q'$, temos

$$x = qy + r \qquad \text{com } 0 \leq r < |y|.$$

□

Um teorema particularmente interessante no estudo da estrutura dos números inteiros é o *Lema de Bézout}, escrito em pelo matemático francês Étienne Bézout, nascido em 1730 e morto em 1783. O Lema de Bézout foi inicialmente enunciado para o máximo divisor comum de polinômios com coeficientes racionais, e o resultado similar para números inteiros passou a ser chamado de Teorema de Bézout . Veremos que ao estudar a estrutura dos inteiros sob o ponto de vista de teoria de grupos, utilizaremos o teorema de Bézout para descrever todos os subgrupos de* $\mathbb{Z}$*. a demonstração do Teorema de Bézout, enunciado a seguir, consiste em mostrar que o máximo divisor comum de dois inteiros,*x, y *é o menor dos inteiros positivos(não nulo!) que pode ser escrito como soma de múltiplos de* x *e de* y

Teorema 2.29 (Bézout)**.** *Dados números inteiros x, y não ambos nulos, seja $d =$ $\mathbf{MDC}(x, y)$. Existem inteiros n, m tais que*

$$d = nx + my$$

Demonstração. *Sejam x, y, d como na hipótese do teorema. Considere o conjunto $\mathbb{A} = \{ax + by; a, b \in \mathbb{Z}\}$ e seja $\mathbb{B} = \mathbb{A} \bigcap \mathbb{N}^*$. Uma vez que x e y não são simultaneamente nulos, o conjunto $\mathbb{B}$ é diferente do vazio e limitado inferiormente pelo zero. De acordo com o princípio do menor inteiro, existe $\delta \in \mathbb{B}$ tal que $\delta \leq h \quad \forall h \in \mathbb{B}$. Além disto, existem $n, m \in \mathbb{Z}$ tais que $\delta = nx + my$.*

Uma vez que $d|x$ e $d|y$ tem-se que $d|\delta$. Logo, como $\delta > 0$, tem-se $d \leq \delta$. Para mostrar que $\delta \leq d$ e que portanto $d = \delta$, mostraremos que δ é divisor comum de x e y. De fato. Dados $a, b \in \mathbb{Z}$ existem únicos valores $q, r \in \mathbb{Z}$ tais que

$$ax + by = q\delta + r \qquad com\ 0 \leq r < \delta.$$

Substituindo o valor de δ na equação acima temos:

$$\begin{aligned} ax + by &= q(nx + my) + r \\ (a - qn)x + (b - qm)y &= r \end{aligned}$$

Portanto, $r \in \mathbb{A}$, e $0 \leq r < \delta$. Como δ é o menor inteiro em $\mathbb{B}$, r não pode ser maior que zero e obrigatoriamente deve-se ter $r = 0$. Concluimos que δ divide $ax + by$ quaisquer que sejam $a, b \in \mathbb{Z}$. Isto é, δ divide todo valor em $\mathbb{A}$ e em particular divide x e y.

Desta forma, temos $\delta \leq d$ e $d \leq \delta$. Isto é, $d = \delta$. Portanto existem $n, m \in \mathbb{Z}$ tais que

$$d = nx + my.$$

□

Teorema 2.30 (Propriedade fundamental do MDC)**.** *Sejam $x, y, d \in Z$. Se x e y não são simultaneamente nulos e $d \in Z_+$ é um divisor comum de x e y. Então são equivalentes:*

(i) $d = \mathbf{MDC}(x, y)$.

(ii) Dado $z \in \mathbb{Z}$. Se $z|x$ e $z|y$ então $z|d$.

Demonstração. *Suponha* $d = \mathbf{MDC}(x, y)$. *Pelo teorema de Bézout, existem $n, m \in \mathbb{Z}$ tais que $d = nx + my$. Logo se $z \in \mathbb{Z}$, é tal que $z|x$ e $z|y$, então z divide d.*

Reciprocamente, Suponha que um valor positivo d seja divisor comum de x e y e satisfaça o ítem "ii ´ ´. Em particular, o $\mathbf{MDC}(x, y)$ *deve dividir d e portanto* $\mathbf{MDC}(x, y) \leq d$. *Por outro lado como d é divisor comum de x e y ele deve ser menor ou igual a* $\mathbf{MDC}(x, y)$. *Ou seja* $d = \mathbf{MDC}(x, y)$. □

2.4.3 Exercícios

1. *Analise cada uma das afirmações abaixo. Demonstre as verdadeiras e dê contra exemplo para as falsas.*

   (a) *Dados inteiros não ambos nulos,* x, y. *Se* $d = \mathbf{MDC}(x, y)$, $x = ad$ e $y = bd$, *então* $\mathbf{MDC}(a, b, =)1$.

   (b) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x|yz$ *então* $x|y$ *ou* $x|z$.

   (c) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x|yz$ *e* $\mathbf{MDC}(x, y) = 1$ *então* $x|z$.

   (d) *Se* $\wp \in \mathbb{Z}$ *é primo e* $\wp|xy$ *então* $\wp|x$ *ou* $\wp|y$.

   (e) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x|z$ *e* $y|z$ *então* $xy|z$.

   (f) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x|z, y|z$ *e* $\mathbf{MDC}(x, y) = 1$ *então* $xy|z$.

   (g) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x > 0$ *e* $\mathbf{MDC}(y, z) = d$ *então* $\mathbf{MDC}(xy, xz) = xd$.

   (h) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x|(y + z)$ *e* $\mathbf{MDC}(y, z) = 1$ *então* $\mathbf{MDC}(x, y) = \mathbf{MDC}(x, z) = 1$.

   (i) *Dado* $x \in \mathbb{Z}$. *Se* $2 \nmid x$ *então* $4|(x^2 - 1)$.

   (j) $\mathbf{MDC}(x, x + 1) = 1 \quad \forall x \in \mathbb{Z}$.

   (k) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $x|(y + z)$ *então* $x|z$ *e* $x|y$.

   (l) *Sejam* $x, y, z \in \mathbb{Z}$. *Se* $\mathbf{MDC}(x, z) = \mathbf{MDC}(y, z) = 1$ *então* $\mathbf{MDC}(xy, z) = 1$.

2. *Dado* $n \in \mathbb{Z}$, *quais os valores possíveis para:*

   (a) $\mathbf{MDC}(n, n + 2)$

   (b) $\mathbf{MDC}(n, n + 6)$

3. *Mostre que qualquer que seja* $n \in \mathbb{Z}$, $\mathbf{MDC}(n + 1, n^2 - n + 1)$ *é* 1 *ou* 3
   Dica: *Peça ajuda a Euclides.*

4. *Defina MDC para uma lista finita de números inteiros* $x_1, \ldots, x_n$.

5. *Sejam* $x_1, \ldots, x_n$ n *números inteiros não todos nulos e* $d = \mathrm{MDC}(x_1, \ldots, x_n)$. *Mostre que existem* n *inteiros,* $a_1, \ldots, a_n$ *tais que*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$$

2.4.4 Representação Numérica

Nesta seção discutiremos a representação numérica dos números naturais. A forma de representação dos números naturais influenciou diretamente na popularização e domínio da aritmética. Povos cujos sistemas de representação eram simples e funcionais têm, quase sempre, sua aritmética disseminada mais facilmente, tanto as operações básicas quanto os resultados e processos mais sofisticados. Compare, por exemplo, a contribuição dos gregos, babilônios, indús e árabes com a contribuição dos romanos e egípcios para a Aritmética.

Um sistema de representação numérica consiste basicamente da adoção de um número finito de símbolos para representar uma certa quantidade finita, e de um modus operandus , isto é de um regra para leitura dos valores descritos. Pesquise sobre os sistemas antigos de representação numérica dos povos citados no parágrafo anterior.

2.4.5 Representação $\mathfrak{p}$-ádica

Teorema 2.31. *Fixado um natural $\mathfrak{p} \geq 2$, todo número natural x, não nulo, pode representado de forma única por*

$$x = a_s\mathfrak{p}^s + \cdots + a_1\mathfrak{p} + a_0 \qquad com\ 0 \leq a_\imath \leq \mathfrak{p} - 1 \quad e\ a_s \neq 0.$$

Demonstração. *Dado $x \in \mathbb{N}^*$, existem $q_1, a_0 \in \mathbb{Z}$ tais que $x = q_1\mathfrak{p} + a_0$ com $0 \leq a_0 \leq \mathfrak{p} - 1$. Uma vez que $x, \mathfrak{p}, a_0$ são positivos, devemos obrigatoriamente ter $0 \leq q_1$. Caso $q_1 \leq \mathfrak{p}$ tomamos $a_1 = q_1$ e x terá a forma procurada– Observe que o quociente na divisão Euclideana, só é zero se o dividendo for menor que o divisor. Se $q_1 \geq \mathfrak{p}$, existem $q_2, a_1 \in \mathbb{N}$ tais que $q_1 = q_2\mathfrak{p} + a_1$ com $0 \leq a_1 \leq \mathfrak{p} - 1$. Desta forma, tem-se:*

$$x = q_2\mathfrak{p}^2 + a_1\mathfrak{p} + a_0 \quad com\ 0 \leq q_2 < q_1 \quad 0 \leq a_\imath \leq \mathfrak{p} - 1.$$

Segue que após um número finito de repetição do raciocínio acima, digamos s-vezes, obtém-se para x a forma desejada.

Resta mostrar que tal expressão é unicamente determinada para cada inteiro positivo x.

De fato. Se $x = a_s\mathfrak{p}^s + \cdots + a_1\mathfrak{p} + a_0 \qquad com\ 0 \leq a_\imath \leq \mathfrak{p} - 1 \quad \forall \imath \in \{0, \ldots, s\}$ e $a_s \neq 0$, então

$$\mathfrak{p}^s \leq x < \mathfrak{p}^{s+1}$$

pois, sendo $a_s \geq 1$ e $0 \leq a_\imath \leq \mathfrak{p} - 1 \quad \forall \imath \in \{0, \ldots, s\}$, tem-se:

$$\mathfrak{p}^s \leq a_s\mathfrak{p}^s \leq a_s\mathfrak{p}^s + \cdots + a_1\mathfrak{p} + a_0 \leq (\mathfrak{p}-1)\mathfrak{p}^s + (\mathfrak{p}-1)\mathfrak{p}^{s-1} + \cdots + (\mathfrak{p}-1)\mathfrak{p} + (\mathfrak{p}-1) = \mathfrak{p}^{s+1} - 1 < \mathfrak{p}^{s+1}.$$

Desta forma, se tivermos outra representação ,digamos

$$x = b_t\mathfrak{p}^t + \cdots + b_1\mathfrak{p} + b_0 \qquad com\ 0 \leq b_\imath \leq \mathfrak{p} - 1 \quad \forall \imath \in \{0, \ldots, t\}\ e\ a_t \neq 0,$$

devemos obrigatoriamente ter $s = t$ *pois caso contrário ter-se-ia* $\mathfrak{p}^s \leq x < \mathfrak{p}^{s+1} \leq \mathfrak{p}^t \leq x < \mathfrak{p}^{t+1}$ *ou* $\mathfrak{p}^t \leq x < \mathfrak{p}^{t+1} \leq \mathfrak{p}^s \leq x < \mathfrak{p}^{s+1}$, *conforme fosse* $s < t$ *ou* $t < s$. *Além disto, como* a_0 *eb*$_0$ *são os restos da divisão de* x *por* $\mathfrak{p}$, *temos* $a_0 = b_0$. *Ou seja,*

$$\begin{aligned} (a_s - b_s)\mathfrak{p}^s + \cdots + (a_1 - b_1)\mathfrak{p} &= 0 \qquad \textit{dividindo por } \mathfrak{p} \\ (a_s - b_s)\mathfrak{p}^{s-1} + \cdots (a_2 - b_2)\mathfrak{p} + (a_1 - b_1) &= 0 \end{aligned}$$

Desta forma, a_1 *e* b_1 *são os restos da divisão de* $x - a_0$ *por* $\mathfrak{p}$. *Repetindo o processo, concluimos que* $a_\imath = b_\imath \quad \forall \imath$. □

A expressão $a_s\mathfrak{p}^s + \cdots + a_1\mathfrak{p} + a_0$ *é dito ser a representação* $\mathfrak{p}$*-ádica de* x. *As expressões :*

$$(a_s, a_{s-1}, \ldots, a_0)_\mathfrak{p} \qquad a_s a_{s-1} \cdots a_{0_\mathfrak{p}} \qquad a_s a_{s-1} \cdots a_0$$

são chamadas de representação de x *na base* $\mathfrak{p}$. *Observe que a terceira forma de representação, usando números decimais, só é adequada quando fixado um valor* $\mathfrak{p} \leq 10$.

Exemplo 2.32. Sistema Decimal: *Quando consideramos o caso em que* $\mathfrak{p} = 10$ *obtemos que todo número natural pode ser representado usando-se 10 símbolos, algarismos,* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. *Desta forma a representação* 54923 *significa* $5 \times 10^4 + 4 \times 10^3 + 9 \times 10^2 + 2 \times 10 + 3$.

Exemplo 2.33. Sistema binário: *Quando consideramos o caso em que* $\mathfrak{p} = 2$ *obtemos que todo número natural pode ser representado por uma seqüência de* 1 *e zeros. Por exemplo o número decimal* $167 = 1 \times 10^2 + 6 \times 10 + 7$ *pode ser escrito como*

$$1 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

ou simplesmente

$$10100111_2 \qquad ou \quad 10100111$$

Exemplo 2.34. Sistema Hexadecimal: *Para o caso em que* $\mathfrak{p} = 16$ *obtemos uma representação numérica muito utilizado em computação. Considere que os símbolos* $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$ *representam os valores decimais de* 0 *a* 15. *Desta forma a representação o número decimal* 54923 *é representado por* $D68B$. *Para este sistema , em particular pode utilizar ainda a letra H, no final da representação, para diferenciar entre um número decimal um número hexadecimal. Por exemplo, para diferenciar o número decimal 12 de* $12H := 12_{16}$ *(18 na base 10).*

2.4.6 Exercícios

1. *Escreva o número decimal 4634575 na base* $\mathfrak{p}$ *para cada valor* $\mathfrak{p} \in \{2, 3, 5, 6, 8, 11, 16, 20, 60, 100\}$.
2. *Converta para o sistema decimal a representação de cada valor abaixo:*
   (a) 10101011_2
   (b) 354_5
   (c) $2FEDB5_{16}$
   (d) $29 \times 30^3 + 5 \times 30^2 + 17$
3. *Estude o diagrama utilizado para a multiplicação e soma de números na base decimal e descreva uma forma similar para soma e multiplicação em base* $2, 5, 11 e 16$.
4. *Desenvolva uma regra para mudança de bases, sem a necessidade de conversão para o sistema decimal.*

2.4.7 Algoritmo de Euclides para cálculo do MDC

Nesta subsecção estudaremos o algoritmo de Euclides para o cômputo do MDC de dois inteiros não nulos. A fundamentação teórica para a validade do algoritmo reside no seguinte teorema:

Teorema 2.35. *Sejam* x, y, q, r *inteiros tais que* $x = qy + r$. *Se* x *e* y *não são simultaneamente nulos então* $\mathbf{MDC}(x, y) = \mathbf{MDC}(y, r)$.

Demonstração. *Sejam* x, y, q, r *como no enunciado do teorema,* $d = \mathbf{MDC}(x, y)$ *e* $u = \mathbf{MDC}(y, r)$. *Como* u *divide simultaneamente* y *e* r *então* u *divide simultaneamente* x *e* y, *logo* $u \leq d$. *por outro lado, como* d *divide simultaneamente* x *e* y *então* d *divide simultaneamente* y *e* r, *logo* $d \leq u$. *Portanto,uma vez que* u, d *são números positivos,* $u = d$. □

Corolário 2.36. *Sejam* $x, y, r \in \mathbb{Z}$, *com* $y \neq 0$. *Se* r *é o resto da divisão euclidiana de* x *por* y, *então* $\mathbf{MDC}(x, y) = \mathbf{MDC}(y, r)$.

Demonstração. *De acordo com o algoritmo de divisão euclidiana, tem-se* $x = qy+r$. *Logo, em acordo com o teorema 2.35, tem-se* $\mathbf{MDC}(x, y) = \mathbf{MDC}(y, r)$. □

Teorema 2.37 (Método das divisões sucessivas)**.** *Sejam* x, y *inteiros não nulos, com* $y \neq 0$. *Defina* $a_0 = x$ *e* $a_1 = y$. *Para* $\imath > 1$ *defina* $a_\imath$ *como sendo o resto da divisão euclidiana de* $a_{\imath-2}$ *por* $a_{\imath-1}$. *Se* a_n *é o último resto não nulo então* $\mathbf{MDC}(x, y) = a_n$.

Demonstração. *Uma vez que* $\mathbf{MDC}(x,y) = \mathbf{MDC}(|y|,|r|)$, *podemos sem perda de generalidade assumir que* $x, y > 0$. *Em acordo com o teorema 2.28 e com a finitude do conjunto* $\{a \in \mathbb{Z}; 0 \leq a < y\}$ *existe* $n \in \mathbb{N}$ *tal que:*

$$\begin{aligned}
a_0 &= q_1 a_1 + a_2 \qquad 0 \leq a_2 < a_1 \\
a_1 &= q_2 a_2 + a_3 \qquad 0 \leq a_3 < a_2 \\
\vdots &= \vdots \qquad \vdots \\
a_{n-2} &= q_{n-1} a_{n-1} + a_n \qquad 0 \leq a_n < \cdots < a_3 < a_2 \\
a_{n-1} &= q_n a_n + 0 \qquad \textit{em que } 0 < a_n
\end{aligned}$$

Neste caso, em acordo com o teorema 2.35, tem-se

$$\mathbf{MDC}(x,y) = \mathbf{MDC}(a_0,a_1) = \mathbf{MDC}(a_1,a_2) = \cdots = \mathbf{MDC}(a_{n-1},a_n) = \mathbf{MDC}(a_n,0) = a_n.$$

□

O método descrito acima é comumente ensinado na $5^{\underline{a}}$ *série por meio da construção de uma tabela composta de 3 linhas e tantas colunas quantas forem necessárias e preenchida como a seguir:*

- *Na primeira linha registra-se, a partir da segunda coluna, os quocientes obtidos pela divisão euclidiana de* $a_{\imath-2}$ *por* $a_{\imath-1}$*;*
- *Na segunda linha registra-se, a partir da primeira coluna, os valores de* $a_\imath$;
- *Na terceira linha registra-se, a partir da primeira coluna e começando com* $\imath = 2$, *os restos divisão euclidiana de* $a_{\imath-2}$ *por* $a_{\imath-1}$*;*

Contando-se da esquerda para a direita, o MDC ó último valor não nulo obtido na terceira linha.

2.4.8 Exercícios

1. *Use o método das divisões sucessivas para determinar* $\mathbf{MDC}(x,y)$ *para cada caso abaixo:*
   (a) $x = 252$ *e* $y = 1325$;
   (b) $x = 221$ *e* $y = 195$;
   (c) $x = -221$ *e* $y = -195$;
   (d) $x = -7293$ *e* $y = 3640$;
   (e) $x = 76084$ *e* $y = -63020$;

2. *Escreva o número 100 como soma de múltiplos de 7 e 9.*

3. *Mostre que se* $\mathbf{MDC}(x, y) = 1$ *então todo número inteiro pode ser escrito como soma de múltiplos de* x *e* y*.*

4. *O que pode ser dito sobre a recíproca da afirmação feita no item acima ser verdadeira ou falsa? Prove tua afirmação!*

2.4.9 Teorema Fundamental da Aritmética

O teorema 2.26 nos mostra que um número inteiro, diferente de $-1, 0$ *e* 1*, ou é primo ou um produto finito de números primos. Nesta seção mostraremos que tal expressão é única a menos de ordem entre os fatores do produto. este resultado é conhecido como "***Teorema Fundamental da Aritmética***". Para a demonstração definiremos para cada* $x \in \mathbb{Z} - \{-1, 0, 1\}$ *o valor* $\ell(x) = \min\{n \in \mathbb{N}; x$*pode ser escrito como produto de n prin*
e procederemos por indução sobre este número. O argumento para utilização da hipótese de indução é o **Lema de Gauss** *enunciado e provado a seguir.*

Lema 2.38 (Lema de Gauss)**.** *Sejam* x, y, z *inteiros não nulos. Se* $\mathbf{MDC}(x, y) = 1$ *e* $x|yz$ *então* $x|z$*.*

Demonstração. *Sejam* x, y, z *como no enunciado. Como* $\mathbf{MDC}(x, y) = 1$*, existem inteiros* u, v *tais que* $ux + yv = 1$*. Multiplicando a última igualdade por* z *obtemos* $uxz + vyz = z$*. Por hipótese,* $x|yz$*, logo existe* $q \in \mathbb{Z}$ *tal que* $yz = qx$*. Portanto,*

$$x(uz + vq) = z.$$

Isto é, x *divide* z*.* □

Corolário 2.39. *Sejam* p, a, b *números inteiros e* p *primo. Se* $p|ab$ *então* $p|a$ *ou* $p|b$*.*

Demonstração. *Sejam* $a, b, p \in \mathbb{Z}$*. Suponha que* p *é primo,* $p|ab$ *e* $p \nmid a$*. Queremos mostrar que* $p|b$*. De fato, se* $p \nmid a$ *então* $\mathbf{MDC}(p, a) = 1$*. De acordo com o teorema de Bézout temos que existem inteiros* n, m *tais que:*

$$an + pm = 1.$$

Multiplicando por b *temos que* $abn + pbm = b$*. Como* $p|ab$ *e* $p|pmb$ *podemos concluir que* $p|b$*.*

□

Teorema 2.40 (Teorema Fundamental da Aritmética)**.** *Todo número inteiro* $x \notin \{-1, 0, 1\}$ *é primo ou pode ser expresso como um produto finito de números primos. Além disto, a expressão de* x *como produto de números primos é única a menos de troca de sinal e de permutação entre os fatores do produto.*

Demonstração.
A primeira parte do **Teorema Fundamental da Aritmética** *decorre do teorema 2.26. Resta-nos, portanto, demonstrar a unicidade da fatoração a menos de permutação entre os fatores. Para isto procederemos por indução sobre o natural* $\ell(x)$ *definido a seguir.*

Para cada $x \in \mathbb{Z}-\{-1,0,1\}$ *seja* $\ell(x) := \min\{n \in \mathbb{N}; x = p_1 \cdots p_n \text{ com } p_1, p_2, \ldots, p_n \text{ primos}\}$. *Em decorrência do teorema 2.26, temos que* $\ell(x) \geq 1 \quad \forall x \in \mathbb{Z} - \{-1,0,1\}$.

Dado $x \in \mathbb{Z}-\{-1,0,1\}$, *se* $\ell(x) = 1$ *então* x *é número primo. Suponha que existam* r *primos* $q_1, q_2, \ldots, q_r$ *tais que* $x = q_1 \cdots q_r$ *e que* $r \geq 2$. *Como* x *é primo, deve existir um* $\jmath \in \{1,2,\ldots,r\}$ *tal que* $x|q_\jmath$. *Re-enumerando, se necessário for, podemos supor que* $x|q_1$. *Neste caso,* $q_1 = ux$ *para algum* $u \in \mathbb{Z}$ *e conseqüentemente temos* $x = (ux)q_2 \cdots q_r$ *ou equivalentemente,* $x(1 - uq_2 \cdots q_r) = 0$. *Uma vez, que* $x \neq 0$ *devemos, obrigatoriamente, ter* $1 - uq_2 \cdots q_r = 0$, *ou seja* $(uq_2), q_2, \ldots, q_r$ *são inversíveis em* Z *e isto contradiz a definição de número primo. Portanto* r *não pode ser maior ou igual a 2 e a outra expressão possível para* x *é* $x = q_1$. *Concluimos que tese do teorema é verdadeira sempre que* $\ell(x) = 1$.

Dado um natural $r \geq 1$. *Suponha que a tese seja verdadeira para todo* $y \in \mathbb{Z} - \{-1,0,1\}$ *tal que* $\ell(y) \leq r$. *Seja* $x \in \mathbb{Z} - \{-1,0,1\}$ *tal que* $\ell(x) = r+1$. *Neste caso, existem primos* $p-1, \ldots, p_{r+1}$ *tais que* $x = p_1 \cdots p_{r+1}$. *Se* $q_1 \cdots q_t$ *é outra expressão de* x *como produto de números primos. Isto é, se*

$$p_1 \cdots p_{r+1} = q_1 \cdots q_t,$$

então $t \geq r+1$, *e como* p_1 *é primo temos que* p_1 *deve dividir algum dos fatores em* $q_1 \cdots q_t$. *Após uma permutação, se necessário, podemos supor que* $p_1|q_1$, *e uma vez que* q_1 *também é primo temos que* $q_1 = up_1$ *com* $u = 1$ *ou* $u = -1$. *Sendo assim,*

$$\begin{aligned} p_1 \cdots p_{r+1} &= (up_1)q_2 \cdots q_t \qquad \therefore \\ p_1(p_2 \cdots p_{r+1} - (uq_2)q_3 \cdots q_t) &= 0 \qquad \therefore \\ p_2 \cdots p_{r+1} &= (uq_2)q_3 \cdots q_t \end{aligned}$$

Definindo $y = p_2 \cdots p_{r+1}$ *temos* $\ell(y) \leq r$. *Segue por hipótese de indução que* $t - 1 = (r+1) - 1$, *isto é* $t = r+1$ *pois na útima igualdade encontramos duas fatorações de* y *como produto de números primos. Além disto, ainda da hipótese de indução obtemos que após uma reindexação, se necessário for, podemos escrever para* $\jmath \in 2, 3, \ldots, r+1$, $p_\imath = q_\jmath$ *ou* $p_\jmath = -q_\jmath$. *Conseqüentemente, em acordo com o princípio de indução, a tese é válida para todo inteiro* $x \notin \{-1,0,1\}$.

□

Corolário 2.41. *Todo inteiro positivo* $x > 1$ *ou é uma potência de um primo positivo ou pode ser escrito como um produto finito de potências primos positivos distintos*

dois-a-dois. Esta representação é única a menos de permutação e de fatores com expoente nulo.

Demonstração. *De acordo com o Teorema Fundamental da Aritmética, podemos escrever qualquer inteiro positivo $x > 1$ na forma $x = p_1 \cdots p_n$ para algum natural n e números primos $p_1, \ldots, p_n$. Uma vez que $x = |x| = |p_1| \cdot |p_2| \cdots |p_n|$, podemos assumir que $p_1, \ldots, p_n$ são positivos. Finalmente, basta usar a associatividade do produto para agrupar os fatores primos que se repetem.*

□.

Dados $x, y \in \mathbb{Z}$, inteiros positivos, considere o conjunto $\{\wp \in \mathbb{N}, \wp | x \text{ ou } \wp | y\}$, isto é, o conjunto dos primos positivos que dividem x ou dividem y. Em acordo com Teorema Fundamental da Aritmética este conjunto é finito, de forma que podemos representá-lo como $\{p_1, \ldots, p_r\}$ e podemos escrever

$$x = p_1^{\alpha_1} \cdots p_r^{\alpha_r} y = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

com $\alpha_\imath \geq 0$, $\beta_\imath \geq 0 \forall \imath \in \{1, \ldots, r\}$, e convencionando-se escrever $p_\jmath^0 := 1$.

Corolário 2.42 (Cálculo do MDC)**.** *Dados inteiros positivos x e y. Se $x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ e $y = p_1^{\beta_1} \cdots p_r^{\beta_r}$ com $p_1, \ldots, p_r$ primos distintos dois-a-dois, então*

$$\mathbf{MDC}(x, y) = p_1^{a_1} \cdots p_r^{a_r} \quad \text{em que } a_\imath = \min\{\alpha_\imath, \beta_\imath\} \quad \forall \imath \in \{1, \ldots, r\}.$$

Teorema 2.43. *Sejam $x, y, z \in \mathbb{Z}$ tais que $\mathbf{MDC}(x, y) = 1$. Se $x|z$ e $y|z$ então $xy|z$.*

Demonstração. *Se $\mathbf{MDC}(x, y) = 1$ então existem $u, v \in \mathbb{Z}$ tais que*

$$ux + by = 1.$$

Portanto, podemos escrever,

$$uxz + byz = z.$$

Por outro lado, como $x|z$ e $y|z$ temos $xy|yz$ e $xy|xz$. Logo, $xy|z$. □

Definição 2.44. *Dados $x, y \in \mathbb{Z}$ dizemos que $\mathfrak{m} \in \mathbb{N}$ é um mínimo múltiplo comum de x e y se satisfaz:*

i) $x|\mathfrak{m}$ e $y|\mathfrak{m}$

ii) Para todo $u \in \mathbb{Z}$. Se $x|u$ e $y|u$ então $\mathfrak{m}|u$.

Observação 2.45. *Para o natural definido acima, emprega-se a notação $\mathbf{MMC}(x, y)$. Observe que que não podemos dizer que o $\mathbf{MMC}(x, y)$ é o menor dos números inteiros não negativos que são simultaneamente múltiplos de x e de y. De fato, como zero é múltiplo de todo e qualquer valor inteiro, o menor dos números inteiros não*

negativos que são simultaneamente múltiplos de x e de y é sempre zero. Entretanto o $\mathbf{MMC}(x, y)$ *só é zero se, e somente se,* $x = 0$ *ou* $y = 0$. *Por esta razão alguns autores reservam a palavra múltiplo apenas para comparação entre números não nulos e evitar a sutileza expressa nesta observação. Se no entanto,* x *e* y *são ambos não nulos o* $\mathbf{MMC}(x, y)$ *é o menor dos inteiros positivos que são simultaneamente múltiplos de* x *e de* y.

Proposição 2.46. *O MMC de dois números inteiros é único.*

Demonstração. *De fato, dados* $x, y \in Z$ *suponha que* $\mathfrak{m}_1$ *e* $\mathfrak{m}_2$ *satisfaçam as condições da definição de MMC para* x *e* y. *Neste caso, temos que* $x|\mathfrak{m}_2$ *e* $y|\mathfrak{m}_2$ *e portanto* $\mathfrak{m}_1|\mathfrak{m}_2$. *Por outro lado,* $x|\mathfrak{m}_1$ *e* $y|\mathfrak{m}_1$ *portanto* $\mathfrak{m}_2|\mathfrak{m}_1$. *Como ambos,* $\mathfrak{m}_1$ *e* $\mathfrak{m}_2$ *são não negativos, temos obrigatoriamente* $\mathfrak{m}_1 = \mathfrak{m}_2$.

□

Teorema 2.47. *Quaisquer que sejam os inteiros ,*x *e* y *não simultaneamente nulos, tem-se*

$$\mathbf{MMC}(x, y) \cdot \mathbf{MDC}(x, y) = |xy|$$

Demonstração. *A tese do teorema é evidentemente verdadeira se* $x = 0$ *ou* $y = 0$. *Pois neste caso,* $\mathbf{MMC}(x, y) = 0$. *Além disto, como* $\mathbf{MMC}(x, y) = \mathbf{MMC}(|x|, |y|)$ *e* $\mathbf{MDC}(x, y) = \mathbf{MDC}(|x|, |y|)$, *basta mostrar a igualdade para o caso em que* $x > 0$ *e* $y > 0$.

Sejam pois x, y *inteiros positivos,* $d = \mathbf{MDC}(x, y)$ *e* $\mathfrak{m} = \mathbf{MMC}(x, y)$. *Como* $d|xy$, *podemos escrever* $xy = dz$ *para algum* $z \in \mathbb{N}$. *Vamos mostrar que* $\mathbf{MMC}(x, y) = z$.

De fato, uma vez que $d = \mathbf{MDC}(x, y)$, *podemos escrever* $x = ad$ *e* $y = bd$ *com* $\mathbf{MDC}(a, b) = 1$. *Desta forma,*

$$xy = abd^2 = dz \tag{2.5}$$

ou seja,

$$z = abd. \tag{2.6}$$

Consequentemente $z = (ad)b = xb$, *e* $z = a(db) = ay$. *Sendo assim,* $x|z$ *e* $y|z$ *e portanto* $\mathfrak{m}|z$ *(em particular* $0 < \mathfrak{m} \leq z$*).*

Por outro lado, como $d|x$ *e* $x|\mathfrak{m}$ *podemos escrever*

$$\mathfrak{m} = dc. \tag{2.7}$$

Além disto, como $x = ad$ *e* $y = bd$ *temos que* $ad|dc$ *e* $bd|dc$. *Portanto,* $a|c$ *e* $b|c$. *Em acordo com o teorema 2.43, uma vez que* $\mathbf{MDC}(a, b) = 1$, *temos que* $ab|c$ *e consequentemente* $abd|dc$ *isto é,* $z|\mathfrak{m}$.

Segue que $z \leq \mathfrak{m}$ *e* $\mathfrak{m} \leq z$. *Isto é,* $\mathfrak{m} = z$. □

2.4.10 Outra caracterização de números primos

A recíproca do Corolário 2.39 é verdadeira, considerando a hipótese $p \notin \{-1, 0, 1\}$. Isto é: Se um número inteiro $p \notin \{-1, 0, 1\}$ é tal que $p|x$ ou $p|y$ sempre que $p|xy$ então este número p é primo.

Podemos então dizer que o seguinte teorema é uma caracterização de números primos.

Teorema 2.48. *Dado um número inteiro $p \notin \{-1, 0, 1\}$ as seguintes afirmações são equivalentes:*

1. *p é primo.*

2. *$p|x$ ou $p|y$ sempre que $p|xy$.*

Demonstração. *Que a afirmação (1) implica na afirmação (2) foi provado no corolário 2.39.*

Para mostrarmos arecíproca, suponha que $p \notin \{-1, 0, 1\}$ satisfaça a propriedade em (2) e seja $d \in \mathbb{Z}$ um divisor de p. Neste caso podemos escrever $p = db$, para $b \in \mathbb{Z}$, e aplicando a propriedade (2) devemos ter $p|d$ ou $p|b$, isto é $d = up$ ou $b = up$ para algum inteiro u. No primeiro caso temos $p = (up)b$, ou seja $p(1 - ub) = 0$ o que só é possível com $1 - ub = 0$. Isto é, $u, b \in \{-1, 1\}$ e $d \in \{p, -p\}$. O segundo caso nos fornece, de forma similar, $d \in \{-1, 1\}$ e $b \in \{p, -p\}$.

Do raciocínio acima podemos concluir que os únicos divisores de p são $\{-1, 1, -p, p\}$ e portanto que p é um número primo. □

Outra caracterização de primos é dado pelo teorema a seguir:

Teorema 2.49. *Seja $\mathfrak{b}$ um inteiro positivo maior que 1. Seja $\mathfrak{q}$ o maior inteiro cujo quadrado é menor ou igual a $\mathfrak{b}$. Se $\mathfrak{b}$ não possui divisores positivos menores ou iguais a $\mathfrak{q}$, e maiores que 1, então $\mathfrak{b}$ é primo.*

Demonstração. *Dado $\mathfrak{b} \in \mathbb{N} - \{0, 1\}$. Seja $\wp$ o menor primo positivo que divide que divide $\mathfrak{b}$. Temos,*

$$\mathfrak{b} = \wp \cdot \omega$$

para algum $\omega \in \mathbb{N}$. Suponha que $\omega > 1$. Neste caso, como $\wp$ é o menor dos divisores positivos maiores que 1, devemos obrigatoriamente ter $1 < \wp \leq \omega$. Sendo assim, $\wp^2 \leq \mathfrak{b}$. Portanto se $\mathfrak{b} > 1$, não possui divisores cujos quadrados são menores ou iguais a $\mathfrak{b}$, então $\omega = 1$ e $\mathfrak{b}$ é primo. □.

Corolário 2.50. *Seja $\mathfrak{b}$ um inteiro positivo maior que 1. Seja $\mathfrak{q}$ o maior inteiro cujo quadrado é menor ou igual a $\mathfrak{b}$. Se nenhum primo positivo menor ou igual a $\mathfrak{q}$,divide $\mathfrak{b}$, então $\mathfrak{b}$ é primo.*

Exemplo 2.51. *Vamos utilizar o resultado do corolário 2.50 para mostrar que 101 é primo.*

De fato, temos que o maior inteiro cujo quadrado é menor ou igual a 101 é 10. Os primos positivos menores que 10 são $\{2, 3, 5, 7\}$. *Como nenhum deles divide 101, podemos concluir que 101 é primo.*

2.4.11 Exercícios

1. *sejam* x, y *inteiros ímpares. Mostre que:*
   (a) $8|(x^2 - y^2)$
   (b) $8|(x^4 + y^4 - 2)$
2. *Mostre por indução sobre* n *que para todo* $n \in \mathbb{N}$ *tem-se que* $9|(10^n + 3 \cdot 4^{n+2} + 5)$.
3. *Sejam* $x \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Mostre que:*
   (a) $(x - 1)|(x^n - 1)$
   (b) $x^{2n+1}+1 = (x+1)(x^{2n}-x^{2n-1}+x^{2n-2}-x^{2n-3}+\cdots-x+1)$ **dica:** *Observe a alternância de sinais*
   (c) *Se* n *é ímpar então* $(x + 1)|(x^n + 1)$
   (d) *Se* n *é par então* $(x + 1)|(x^n - 1)$
4. *Liste ordenadamente numa tabela* 10×20, *todos os números positivos de 1 a 200. Use Teorema 2.49 para eliminar os números que não são primos (Crivo de Eratóstenes.)*
5. **(Primos de Mersenne)** *Os números primos da forma* $2^x - 1$ *são chamados de primos de Mersenne, em homenagem a Marin Mersenne(1588-1648). Dados* $x, n \in \mathbb{N}$, *mostre que se* $x^n - 1$ *é primo então* $x = 2$ *e* n *é primo.*
6. **(Números de Fermat)** *Os números da forma* $2^{2^m} + 1$, *com* m *natural, são chamados de números de Fermat em homenagem a Pierre Fermat (1601-1655). Fermat conjecturou que todos estes números eram primos. Leonhard Euler (1707-1783) mostrou que 641 divide* $2^{2^5} + 1$.
   (a) *Use um programa de computação algébrica(Maple,Scilab,Mathcad,Mathematica,...), ou uma calculadora programável, e o Teorema 2.49 para mostrar que para* $0 \leq m \leq 4$ *todo número de Fermat é primo.*
   (b) *Sejam* x, n *inteiros maiores que 1. Mostre que se* $x^n + 1$ *é primo então* x *é par e* n *é potência de 2.* **dica:** *Use os exercícios 3b e 3c .*
7. *Sejam* x, y *números naturais. Mostre que se* $\alpha = \min\{x, y\}$ *e* $\beta = \max\{x, y\}$ *então* $\alpha + \beta = x + y$.

8. *Use o Teorema 2.40 e o exercício 7 Para obter uma nova prova do Teorema 2.47.*

9. *Determinar os números, de dois algarismos, que são iguais ao quádruplo da soma de seus algarismos.*

10. *No último recenseamento, um recenseador visitou a casa de um matemático que possuia três filhas. O matemático informou que o produto das idades das filhas era 72 e que a soma das idades era o número da sua casa, e este número estava visível. O recenseador informou que assim era impossível determinar as idades. Prontamente o matemático disse: tudo bem, darei mais uma informação e com ela o senhor saberá quais as idades. A mais velha das minhas filhas gosta de milk shake de chocolate. Qual a idade de cada uma das filhas?*

11. *Numa escola militar, ao longo de um corredor, estão enfileirados mil armários, enumerados de 1 a 1000, com as portas fechadas. Mil alunos, também enumerados, resolveram fazer a seguinte brincadeira:*

    - *O primeiro aluno passa e abre toda as portas.*
    - *O aluno 2 passa e fecha todas as portas de número par.*
    - *Cada aluno, passando ordenadamente, inverte a posição de todas as portas cujos números sejam divíveis por seu número.*

    Após a passagem dos mil alunos, determine:

    (a) Quantas portas ficaram abertas?

    (b) Qual o número do último armário que ficou aberto?

2.5 Aritmética Modular

A noção de congruência foi introduzida por Johann Carl Friedrich Gauss(1777-1855) em seu trabalho Disquisitiones Arithmeticae publicado em 1801. Veja [5] para mais informações.

Nesta seção estudaremos algumas propriedades básicas da noção de congruência de números inteiros. Usaremos esta noção para construir critérios de divisibilidade para números inteiros, o teorema de Wilson, o pequeno teorema de Fermat e a função de Euler.

Definição 2.52. *Seja $\mathfrak{m}$ um número natural maior que 1. Dados $x, y \in \mathbb{Z}$, diz-se que x é congruente a y módulo $\mathfrak{m}$ se $\mathfrak{m}|(x-y)$.*

Notação: *Escrevemos $x \equiv_{\mathfrak{m}} y$ ou $x = y \text{Mod } \mathfrak{m}$ para expressar que x é congruente a y módulo $\mathfrak{m}$.*

Proposição 2.53. *Seja $n \in \mathbb{N}$ tal que $n > 1$. Sejam x, y, z, w números inteiros.*

1. *Se $x \equiv_n y$ e $z \equiv_n w$ então $(x + z) \equiv_n (y + w)$.*
2. *Se $x \equiv_n y$ e $z \equiv_n w$ então $(xz) \equiv_n (yw)$.*
3. *Se $x \equiv_n y$ então $ux \equiv_n uy \qquad \forall u \in \mathbb{Z}$*

Demonstração. *De fato, se $x \equiv_n y$ e $z \equiv_n w$ então existem $\alpha, \beta \in \mathbb{Z}$ tais que $x = y + \alpha n$ e $z = w + \beta n$.*

Logo, $x + z = y + w + (\alpha + \beta)n$, isto é, $(x + z) \equiv_n (y + w)$.

Para o produto, temos $xz = yw + y\beta n + w\alpha n + \alpha\beta n^2 = yw + (y\beta + w\alpha + \alpha\beta n)n$. Portanto, $xz \equiv_n yw$.

Além disto, para todo $u \in \mathbb{Z}$ temos $ux = uy + u\alpha n$. Ou seja, $ux \equiv_n uy$.

Proposição 2.54. *A relação de congruência é uma relação de equivalência. isto é, a relação $\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}; x \equiv_n y\}$ é uma relação de equivalência.*

Demonstração. *A demonstração é deixada como exercício para o leitor.* □

Proposição 2.55. *Se $ax \equiv_n ay$ e $\mathbf{MDC}(a, n) = 1$ então $x \equiv_n y$.*

Demonstração. *A demonstração é deixada como exercício para o leitor.* □

2.5.1 Exercícios

1. *Seja $n \in \mathbb{N}$ tal que $n > 1$. Dado, $k \in \mathbb{Z}$ e $a \in \mathbb{Z}$ tal que $\mathbf{MDC}(a, n) = 1$, mostre que os conjuntos, dados abaixo, são sistemas completos de resíduos:*

   (a) $\{0, 1, 2, \ldots, n - 1\}$

   (b) $\{0, a, 2a, \ldots, (n - 1)a\}$

   (c) $\{k, a + k, 2a + k, \ldots, (n - 1)a + k\}$

2. *Sejam p um número primo positivo e $x \in \mathbb{Z}$. Mostre que se $x^2 \equiv_p 1$ então $x \equiv_p 1$ ou $x \equiv_p (p - 1)$.*

3. *Mostre por indução em r que se $x_\imath \equiv_{\mathfrak{m}} y_\imath \quad \imath \in \{1, 2, \ldots, r\}$ então*

   (a) $(\sum_{\imath=1}^{r} x_\imath \equiv_{\mathfrak{m}} (\sum_{\imath=1}^{r} y_\imath)$

   (b) $(\prod_{\imath=1}^{r} x_\imath) \equiv_{\mathfrak{m}} (\prod_{\imath=1}^{r} y_\imath)$

Teorema 2.56 (Teorema de Wilson)**.** *Seja $p \in \mathbb{N}$ Então:*

1. *Se p é primo então $(p-1)! \equiv_p -1$.*
2. *Se $p > 1$ e $(p-1)! \equiv_p -1$ então p é primo.*

Demonstração. $(i\ )$ *Se $p = 2$ então $(p-1)! = 1! = 1$. Se $p = 3$ então $p - 1 = 2$ e portanto $2! = 2 \equiv_3 -1$.*

Suponha que $p > 3$. Neste caso, cada elemento do conjunto $\{2, 3, \ldots, p-2\}$ tem um inverso módulo p, neste mesmo conjunto. Além disto, o inverso de cada $x \in \{2, 3, \ldots, p-2\}$ é diferente de x.

Uma vez que p é ímpar, podemos no produto $2 \cdot 3 \cdots (p-2)$ associar cada fator com seu inverso módulo p, e neste caso, cada novo fator do produto será côngruo a 1 módulo p. sendo assim teremos:

$$\begin{aligned} 2 \cdot 3 \cdots (p-2) &\equiv_p 1 \qquad \therefore \\ 2 \cdot 3 \cdots (p-2)(p-1) &\equiv_p -1 \qquad \therefore \\ 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) &\equiv_p -1 \qquad \therefore \\ (p-1)! &\equiv_p -1 \end{aligned}$$

Para demonstrar o item $(ii\ )$ basta observar que se $\mathfrak{m} \in \mathbb{N} - \{0, 1\}$ não é primo então podemos escrever $\mathfrak{m} = xy$ com $1 < x, y < \mathfrak{m}$. Portanto estes valores, x e y aparecem como fatores de $(\mathfrak{m}-1)!$ e conseqüentemente $(\mathfrak{m}-1)! \equiv_{\mathfrak{m}} 0$. □

Teorema 2.57 (Pequeno Teorema de Fermat)**.** *Sejam $p \in \mathbb{N}$ um número primo e $x \in Z$. Se $p \nmid x$ então $x^{p-1} \equiv_p 1$.*

Demonstração. *Seja p primo positivo e $x \in \mathbb{Z}$ tal que $p \nmid x$. Neste caso, o conjunto $\{0, x, 2x, 3x, \ldots, (p-1)x\}$ é um sistema completo de resíduos módulo p. Sendo assim, a função*

$$\sigma : \{0, x, 2x, 3x, \ldots, (p-1)x\} \to \{0, 1, 2, \ldots, p-1\}$$

que a cada elemento associa o seu resto na divisão euclidiana por p, é uma bijeção e isto implica que cada elemento do conjunto $\{x, 2x, 3x, \ldots, (p-1)x\}$ é côngruo módulo p a um elemento do conjunto $\{1, 2, \ldots, p-1\}$. Consequentemente,

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) &\equiv_p x \cdot 2x \cdot 3x \cdots (p-2)x \cdot (p-1)x \qquad \therefore \\ (p-1)! &\equiv_p x \cdot 2x \cdot 3x \cdots (p-2)x \cdot (p-1)x \qquad \therefore \\ -1 &\equiv_p x \cdot 2x \cdot 3x \cdots (p-2)x \cdot (p-1)x \qquad \therefore \\ -1 &\equiv_p x^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1)) \qquad \therefore \\ -1 &\equiv_p x^{p-1}(p-1)! \qquad \therefore \\ -1 &\equiv_p x^{p-1}(-1) \qquad \therefore \\ 1 &\equiv_p x^{p-1} \end{aligned}$$

□

Corolário 2.58. *Seja $p \in \mathbb{N}$ um número primo. Então $x^p \equiv_p x \qquad \forall x \in \mathbb{Z}$.*

Demonstração. *Seja p primo positivo e $x \in \mathbb{Z}$. Se $p|x$ então $p|x^p$. Neste caso, $x^p \equiv_p 0$ e $0 \equiv_p x$. Logo, $x^p \equiv_p x$.*

Se $p \nmid x$ então pelo Pequeno Teorema de Fermat temos $x^{p-1} \equiv_p 1$ e $x \equiv_p x$. Neste caso, em acordo com a proposição 2.53, temos $x^p \equiv_p x$.

Portanto,

$$x^p \equiv_p x \qquad \forall x \in \mathbb{Z}.$$

Definição 2.59 (Função de Euler Φ)**.** *A função $\Phi : \mathbb{N} \to \mathbb{N}$ que a cada natural x associa a quantidade de naturais menores que x e relativamente primos com x, é chamada de função de Euler.*

$$\Phi(x) = \#\{y \in \mathbb{N}; 0 \leq y \leq x \ e \ \mathbf{MDC}(x, y) = 1\}$$

Proposição 2.60. *Seja Φ a função de Euler. Então.*

1. *Se p é primo positivo então $\Phi(p^r) = (p-1)p^{r-1} \qquad \forall r > 0$.*
2. *Se $x, y \in \mathbb{N} - \{0\}$ são relativamente primos então $\Phi(xy) = \Phi(x) \cdot \Phi(y)$.*
3. *Se $x = p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}$ é a fatoração de x em potências de números primos dois-a-dois relativamente primos, então*

$$\Phi(x) = (p_1 - 1)(p_2 - 1) \cdots (p_s - 1)p_1^{r_1 - 1} \cdot p_2^{r_2 - 1} \cdots p_s^{r_s - 1}$$

Demonstração. *Uma vez que p seja primo, um número é relativamente primo com p^r se e somente se não é múltiplo de p. Desta forma basta contar quantos múltiplos positivos de p temos entre os p^r números*

$$\{1, 2, \ldots, p, p+1, \ldots, 2p, 2p+1, \ldots, 3p, \ldots, (p-1)p^{r-1}, (p-1)p^{r-1}+1, \ldots, p^r\}$$

Dentre estes números, os múltiplos de p são:

$$\{p, 2p, 3p, \ldots, (p-1)p, p^2, p^2+p, \ldots, 2p^2, \ldots, (p-1)p^2, \ldots, p^{r-1}, \ldots, 2p^{r-1}, \ldots, (p-1)p^{r-1}, p^r\}$$

Portanto, a quantidade de elementos positivos divisíveis por p é p^{r-1}, pois

$$\{1, 2, \ldots, p, p+1, \ldots, p^{r-1}\}$$

são todos os naturais cujos produtos por p são menores ou iguais a p^r. Desta forma, a quantidade de naturais positivos e relativamente primos com p^r é $p^r - p^{r-1} = p^{r-1}(p-1)$. Isto é,

$$\Phi(p^r) = (p-1)p^{r-1} \qquad \forall r > 0.$$

Isto demonstra o item (1).

Para demonstrar o item (2), sejam $x, y \in \mathbb{N} - \{0\}$ *tais que* $\mathbf{MDC}(x, y) = 1$. *Considere a tabela abaixo formada pelos números de 1 a* xy*:*

$$\begin{array}{ccccccc} 1 & 2 & \cdots & k & \cdots & x \\ x+1 & x+2 & \cdots & x+k & \cdots & 2x \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (y-1)x+1 & (y-1)x+2 & \cdots & (y-1)x+k & \cdots & xy \end{array}$$

Observemos que $\mathbf{MDC}(z, xy) = 1$ *se, e somente se,* $\mathbf{MDC}(z, x) = 1$ *e* $\mathbf{MDC}(z, y) = 1$. *Por um lado, os naturais em uma mesma coluna da tabela acima são todos relativamente primos com* x *ou não são todos relativamente primos com* x. *Portanto, existem* $\Phi(x)$ *colunas com todos os elementos relativamente primos com* x. *Por outro lado, cada coluna é um sistema completo de resíduos módulo* y *e consequentemente em cada coluna temos* $\Phi(y)$ *naturais relativamente primos com* y. *Sendo assim, temos* $\Phi(x) \cdots \Phi(y)$ *naturais simultaneamente relativamente primos com* x *e* y. *Isto é,*

$$\Phi(xy) = \Phi(x) \cdot \Phi(y).$$

O item (3) é conseqüência imediata dos itens (1) e (2).

□

2.5.2 Exercícios

1. *Considere* $p = 11$ *e refaça cada etapa da demonstração da primeira parte do Teorema de Wilson.*

2. *Mostre que se um número natural é soma de dois quadrados perfeitos então* $x \equiv_4 0$, *ou* $x \equiv_4 1$ *ou* $x \equiv_4 2$.

3. *Mostre que se um primo* $x > 2$ *é soma de dois quadrados perfeitos então* $x \equiv_4 1$.

4. *Quantos números inteiros* x *tais que* $79479^2 \leq x \leq 79480^2$ *não são quadrados perfeitos?*

5. *Determine os números que divididos por 17 têm resto igual ao quadrado do quociente correspondente.*

6. *Seja* n *um natural tal que* $n > 1$. *Seja* M *um matriz de ordem* 2 *com entradas inteiras.*

   (a) *Mostre que o determinante de* M *é um número inteiro.*

   (b) *Mostre que* M *admite uma inversa, módulo* n, *se, e somente se, o determinante de* M *é inversível módulo* n.

   (c) *Mostre que as afirmações nos exercícios 2.15 e 6b valem para qualquer matriz de ordem* $r \geq 2$, *com entradas inteiras.*

7. *Determine as soluções inteiras, módulo* n, *para cada equação e cada* n *correspondente.*

   (a) $x^2 + 1 \equiv_5 0$

   (b) $x^3 - 2x^2 - 3x \equiv_{12} 0$

(c) $3x \equiv_{23} 2$

(d) $x^2 + 2x + 2 \equiv_6 0$

(e) $x^2 + 2x + 4 \equiv_6 0$

8. *Dado um primo* p*, mostre que* $(x+y)^p \equiv_p (x^p + y^p) \quad \forall x, y \in \mathbb{Z}$.

9. *O que podemos afirmar sobre a validade da recíproca do afirmação feita no item acima.*

10. *Mostre que se* $3 \nmid x$ *então* $x^2 \equiv_3 1$.

11. *Mostre que* 15 *divide* $x^{33} - x \quad \forall x \in \mathbb{Z}$ *(***Dica:** *peça ajuda a Gauss, Fermat e Euclides.)*

12. *Encontre o resto da divisão euclidiana de* x *por* y *para cada caso abaixo:*

(a) $x = 3^{47} \qquad y = 23.$

(b) $x = 37^{49} \qquad y = 7.$

(c) $x = 2^{2^{17}} + 1 \qquad y = 19.$ **Dica:** *Calcule* $2^{17}\text{Mod } 18.$

(d) $x = 34! \qquad y = 37.$ **Dica:** *Peça ajuda a Wilson.*

(e) $x = 49! \qquad y = 53.$

(f) $x = 24! \qquad y = 29.$

13. *Use o Pequeno Teorema de Fermat para mostrar que* 383838 *divide* $x^{37} - x \quad \forall x \in \mathbb{Z}$. **Dica:** *Fatore* 383838.

14. *Calcule o valor de* Φ *em cada um dos números*

(a) 125

(b) 16200

(c) 2097

(d) 36

(e) 120

15. *Determine o valor de* $x \in \mathbb{N}$ *em cada caso*

(a) $\Phi(x) = 2^2$

(b) $\Phi(x) = 2^3$

(c) $\Phi(x) = 2^4$

(d) $\Phi(x) = 2^5$

(e) $\Phi(x) = 18$

(f) $\Phi(x) = 10$

16. *mostre que se* $\Phi(x) = 2^r$ *então* x *é um produto finito de uma potência de 2 e de primos positivos da forma* $2^{2^u} + 1$*, distintos dois-a-dois.*

2.5.3 Critérios de Divisibilidade

nesta seção desenvolveremos, como aplicação da noção de congruência, os critérios de divisibilidade por números entre 2 e 13, considereando a representação decimal dos números inteiros. Por motivo de simplicidade, trabalharemos apenas com números naturais.

Considere a representação decimal $a_n 10^n + \cdots + a_1 10 + a_0$ *de um número natural* x*.*

Divisibilidade por 2, 5 e 10

Considere a representação decimal $a_n 10^n + \cdots + a_1 10 + a_0$ *de um número natural* x*.*

Para todo $r > 0$ *temos que*

$$10^r a_r \equiv_2 0 \quad e \quad 10^r a_r \equiv_5 0.$$

Logo,

$$x \equiv_2 a_0 \quad e \quad x \equiv_5 a_0.$$

Portanto,

- **Um número natural é divisível por 2 se, e somente se, seu último dígito é 0,2,4,6 ou 8.**
- **Um número natural é divisível por 5 se, e somente se, seu último dígito é 0 ou 5.**

Como $\mathbf{MDC}(2, 5) = 1$ *temos que* x *é divisível simultaneamente por 2 e 5 se, e somente se, é divisível por 10. Logo,*

- **Um número natural é divisível por 10 se, e somente se, seu último dígito é 0.**

Divisibilidade por 3 e por 9

Considere a representação decimal $a_n10^n + \cdots + a_110 + a_0$ *de um número natural* x.

Uma vez que $10 \equiv_3 1$ *e* $10 \equiv_9 1$ *temos que* $10^r \equiv_3 1$ *e* $10^r \equiv_9 1 \quad \forall r > 0$. *Sendo assim,*

$$x \equiv_3 (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

e

$$x \equiv_9 (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

Portanto,

- **Um número natural é divisível por 3 se, e somente se, a soma dos seus algarismos é divisível por 3.**
- **Um número natural é divisível por 9 se, e somente se, a soma dos seus algarismos é divisível por 9.**

Divisibilidade por 4 e 8

Considere a representação decimal $a_n10^n + \cdots + a_110 + a_0$ *de um número natural* x.

Podemos escrever,

$$x = a_n10^n + \cdots + a_110 + a_0 = 100(a_n10^{n-2} + \cdots + a_2) + a_110 + a_0 = 1000(a_n10^{n-3} + \cdots + a_3) + 10^2a_2 + 10a_1 + a_0$$

Logo,

$$x \equiv_4 (10a_1 + a_0) \quad e \quad x \equiv_8 (10^2a_2 + 10a_1 + a_0)$$

Portanto,

- **Um número natural é divisível por 4 se, e somente se, sua dezena é divisível por 4.**
- **Um número natural é divisível por 8 se, e somente se, sua centena é divisível por 8.**

Divisibilidade por 6

Considere a representação decimal $a_n10^n + \cdots + a_110 + a_0$ *de um número natural* x.

Uma vez que $\mathbf{MDC}(2, 3) = 1$, *um número natural é divisível por 6 se, e somente se, é divisível por 2 e por 3. Logo,*

- **Um número natural é divisível por 6 se, e somente se,é par e a soma dos seus algarismos é divisível por 3 .**

Divisibilidade por 12

Considere a representação decimal $a_n10^n + \cdots + a_110 + a_0$ *de um número natural* x.

Uma vez que $\mathbf{MDC}(3,4) = 1$, *um número natural é divisível por 12 se, e somente se, é divisível por 3 e por 4. Logo,*

- **Um número natural é divisível por 12 se, e somente se, a soma dos seus algarismos é divisível por 3 e sua dezena é divisível por 4 .**

Divisibilidade por 7, 11 e 13

Inicialmente observemos que $10^3 = 1001-1$ *e que por outro lado,* $1001 = 7\cdot 11\cdot 13$. *Desta forma,*

$$10^{3r} \equiv_7 (-1)^r \qquad 10^{3r} \equiv_{11} (-1)^r \qquad e \qquad 10^{3r} \equiv_{13} (-1)^r.$$

Por outro lado,Considerando a representação decimal $a_n10^n + \cdots + a_110 + a_0$ *de um número natural* $x > 1000$. *Podemos escrever,*

$x = u_t10^{3t}+u_{t-1}10^{3(t-1)}+\cdots+u_110^3+u_0$ *em que cada* u_i *é uma centena exceto, possivelmente,* u_t.

Isto é,

$$\begin{aligned} u_0 &= 10^2a_2 + 10a_1 + a_0 \\ u_1 &= 10^2a_5 + 10a_4 + a_3 \\ \vdots &= \vdots \\ u_t &= \begin{cases} a_n & se \quad n+1 \equiv_3 1 \\ 10a_n + a_{n-1} & se \quad n+1 \equiv_3 2 \\ 10^2a_n + 10a_{n-1} + a_{n-2} & se \quad (n+1) \equiv_3 0 \end{cases} \end{aligned}$$

Desta forma, podemos escrever

$$x = u_t(1001-1)^t + u_{t-1}(1001-1)^{(t-1)} + \cdots + u_1(1001-1)^+u_0$$

Portanto,

$$\begin{aligned} x &\equiv_7 (-1)^tu_t + (-1)^{t-1}u_{t-1} + \cdots + (-1)^2u_2 + (-1)u_1 + u_0 \\ x &\equiv_{11} (-1)^tu_t + (-1)^{t-1}u_{t-1} + \cdots + (-1)^2u_2 + (-1)u_1 + u_0 \\ x &\equiv_{13} (-1)^tu_t + (-1)^{t-1}u_{t-1} + \cdots + (-1)^2u_2 + (-1)u_1 + u_0 \end{aligned}$$

Ou seja,

- **Um número natural é divisível por 7 se, e somente se, agrupando seus algarismos em grupos de três algarismos consecutivos, a partir da direita, a soma com sinais alternados é divisível por 7.**
- **Um número natural é divisível por 11 se, e somente se, agrupando seus algarismos em grupos de três algarismos consecutivos, a partir da direita, a soma com sinais alternados é divisível por 11.**
- **Um número natural é divisível por 13 se, e somente se, agrupando seus algarismos em grupos de três algarismos consecutivos, a partir da direita, a soma com sinais alternados é divisível por 13.**

Exemplo 2.61. *O número* 3288285 *é divisível por 7, 11 e por 13. De fato,* $003 - 288 + 285 = 0$.

Outro critério de divisibilidade por 11

Considere a representação decimal $a_n 10^n + \cdots + a_1 10 + a_0$ *de um número natural* x. *Como* $10 = 11 - 1$ *temos que* $10^r \equiv_{11} (-1)^r$. *Logo,* $10^r \equiv_{11} 1$ r *é par ou* $10^r \equiv_{11} -1$ r *é ímpar. Portanto,*

$$a_n 10^n + \cdots + a_1 10 + a_0 \equiv_{11} (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$$

Ou seja,

- **Um número natural é divisível por 11 se, e somente se, a diferença entre a soma dos seus algarismos de posição par e a soma dos seus algarismos de posição ímpar, é divisível por 11.**

2.5.4 Equações Diophantinas e o Teorema chinês dos restos

Nesta seção estudaremos um pouco sobre equações diophantinas. Assim chamadas em homenagem a Diophantus, matemático grego que viveu no século III A.C.

Chamamos de equação diophantina a toda e qualquer equação polinomial, em uma ou mais variáveis, com coeficientes inteiros(não todos nulos). Diophantus tratou destas equações em seu livro aritmetike (Foi na margem de um exemplar deste livro que Fermat escreveu o último teorema de Fermat.)

Estaremos tratando , especificamente das equações diophantinas de grau um a duas variáveis. Isto é, equações da forma:

$$ax + by = c \qquad \text{com } a, b \in \mathbb{Z}. \tag{2.8}$$

A resolução de tais equações é equivalente a resolução de equações de congruência em uma variável. Ou seja, a resolução da equação

$$ax \equiv_b c$$

equivale a resolução da equação 2.8

Existência de Solução

Dado uma equação diophantina

$$ax + by = c \qquad com\ a, b \in \mathbb{Z}. \tag{2.9}$$

Dizemos que um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *é solução desta equação se satisfaz*

$$ax_0 + by_0 = c \tag{2.10}$$

o conjunto de todas as soluções é dito ser o conjunto solução da equação diophantina.

Proposição 2.62. *A Equação diophantina*

$$ax + by = c \qquad com\ a, b \in \mathbb{Z}, \tag{2.11}$$

tem conjunto solução não vazio se, e somente se, $\mathbf{MDC}(a, b)$ *divide c.*

Demonstração.

dada uma equação diophantina

$$ax + by = c \qquad com\ a, b \in \mathbb{Z}. \tag{2.12}$$

Sejam $d = \mathbf{MDC}(a, b)$.

Se existe uma solução $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *, isto é, se* $ax_0 + by_0 = c$ *então d divide c. Reciprocamente, se d divide c então podemos escrever:*

$$a = \alpha d \qquad b = \beta d\ rm\ e \qquad c = \kappa d\ em\ que\ mdc\alpha\beta = 1$$

Desta forma existem $u, v \in \mathbb{Z}$ *tais que*

$$u\alpha + v\beta = 1$$

multiplicando por $c = \kappa d$*, temos:*

$$\begin{aligned} u\kappa d\alpha + v\kappa d\beta &= \kappa d \quad \therefore \\ (u\kappa)(d\alpha) + (v\kappa)(d\beta) &= c \quad \therefore \\ (u\kappa)a + (v\kappa)b &= c \end{aligned}$$

Portanto, o par $(u\kappa, v\kappa) \in \mathbb{Z} \times \mathbb{Z}$ *é uma solução, e o conjunto solução é não vazio.*

□

Proposição 2.63. *Se a equação diophantina*

$$ax + by = c \qquad com\ a, b \in \mathbb{Z}, \tag{2.13}$$

tem uma solução $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *então a conjunto solução é dado por*

$$S = \{(x_0 + t\beta, y_0 - t\alpha); t \in \mathbb{Z}\}$$

em que $d = \mathbf{MDC}(a, b)$, $a = d\alpha$ *e* $b = d\beta$.

Demonstração. *Seja* $d = \mathbf{MDC}(a, b)$. *Se a equação diophantina*

$$ax + by = c \qquad com\ a, b \in \mathbb{Z}, \tag{2.14}$$

tem uma solução $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *então* d *divide* c. *Desta forma, existem* $\alpha, \beta, \kappa \in \mathbb{Z}$ *tais que* $a = d\alpha \quad b = d\beta, \quad c = d\kappa$ *e a equação* $ax + by = c$ *tem o mesmo conjunto solução que a equação:*

$$\alpha x + \beta y = \kappa \qquad com\ \ \mathbf{MDC}(\alpha, \beta) = 1.$$

Portanto se (x_0, y_0) *é uma solução da equação 2.14 então*

$$\alpha x_0 + \beta y_0 = \kappa \tag{2.15}$$

Suponha que (x_1, y_1) *é outra solução. Neste caso,*

$$\begin{aligned}
\alpha x_0 + \beta y_0 &= \kappa = \quad \alpha x_1 + \beta y_1 \quad \therefore && (2.16)\\
0 &= \quad \alpha(x_1 - x_0) + \beta(y_1 - y_0) \quad \therefore && (2.17)\\
\alpha(x_1 - x_0) &= \quad \beta(y_0 - y_1) \quad com\ \ \mathbf{MDC}(\alpha, \beta) = 1 && (2.18)
\end{aligned}$$

Logo, $\alpha|(y_0 - y_1)$ *e* $\beta|(x_1 - x_0)$. *Como* a, b *não são ambos nulos, digamos* $b \neq 0$ **(** $a \neq 0$ **leva ao mesmo resultado)** *e neste caso, existe* $t \in \mathbb{Z}$ *tal que* $x_1 = x_0 + t\beta$. *Substituindo na equação 2.18 e eliminando* β, *temos*

$$\begin{aligned}
\alpha \cdot t \cdot \beta &= \beta(y_0 - y_1) \quad \therefore\\
\alpha \cdot t &= y_0 - y_1 \qquad \therefore\\
y_1 &= y_0 - t\alpha
\end{aligned}$$

Reciprocamente, se (x_0, y_0) *é uma solução da equação 2.14, e portanto da equação 2.15, então*

$$\alpha(x_0 + t\beta) + \beta(y_0 - t\alpha) = (\alpha x_0 + \beta y_0) - t\beta\alpha + \alpha t\beta = \alpha x_0 + \beta y_0 = \kappa$$

Isto é, $(x_0 + t\beta, y_0 - t\alpha)$ *também é solução qualquer que seja o valor* $t \in \mathbb{Z}$.

2.5.5 Congruências Lineares

A cada equação diophantina da forma

$$ax + by = c \qquad com\ a, b \in \mathbb{Z}, \tag{2.19}$$

corresponde uma equação de congruência do tipo

$$ax \equiv_b c \qquad com\ a, b \in \mathbb{Z}, \tag{2.20}$$

A equação 2.20, dita equação linear de congruência, tem solução se, e somente se, $\mathbf{MDC}(a, b)$ *divide c.*

Em decorrência da proposição 2.63, se x_0 *é uma solução da equação* $ax \equiv_b c$ *então o conjunto solução é dado por*

$$S = \{x_0 + t\beta; t \in \mathbb{Z}\} \qquad em\ que\ b = \beta \cdot\ \mathbf{MDC}(a, b).$$

Ou ainda, pondo $d =\ \mathbf{MDC}(a, b)$ *e usando a notação* $\beta = \frac{b}{d}$*, o conjunto solução é dado por:*

$$S = \{x_0 + t\frac{b}{d}; t \in \mathbb{Z}\}$$

e consequentemente existem exatamente d soluções incongruentes módulo b cujos representantes são

$$x_0, \quad x_0 + \frac{b}{d}, \quad x_0 + 2\frac{b}{d}, \quad \ldots, \quad x_0 + (d-1)\frac{b}{d}$$

Teorema 2.64 (Teorema chinês dos restos)**.** *Sejam* $a_1, a_2, b_1, b_2, m_1, m_2\mathbb{Z}$ *tais que* $m_1, m_2 > 1$,
$\mathbf{MDC}(m_1, m_2) = 1$ *e* $\mathbf{MDC}(a_1, m_1) =\ \mathbf{MDC}(a_2, m_2) = 1$*. Nestas condições o sistema de congruências lineares*

$$\begin{cases} a_1 x & \equiv_{m_1} & b_1 \\ a_2 x & \equiv_{m_2} & b_2 \end{cases}$$

tem uma única solução módulo $\mathbf{MMC}(m_1, m_2)$*.*

Demonstração. (Unicidade módulo $\mathbf{MMC}(m_1, m_2)$ **)**

Suponha que x_0, x_1 *sejam duas soluções do sistema. Então*

$$\begin{cases} a_1 x_0 & \equiv_{m_1} & b_1 \\ a_2 x_0 & \equiv_{m_2} & b_2 \end{cases} \qquad e \qquad \begin{cases} a_1 x_1 & \equiv_{m_1} & b_1 \\ a_2 x_1 & \equiv_{m_2} & b_2 \end{cases}$$

Ou seja, $a_1 x_0 \equiv_{m_1} a_1 x_1$ *e* $a_2 x_0 \equiv_{m_2} a_2 x_1$*. Portanto,* m_1 *divide* $a_1(x_0 - x_1)$ *e* m_2 *divide* $a_2(x_0 - x_1)$*. Como* $\mathbf{MDC}(a_1, m_1) =\ \mathbf{MDC}(a_2, m_2) = 1$*, podemos concluir*

que m_1 divide $(x_0 - x_1)$ e m_2 divide $x_0 - x_1$), e consequentemente, uma vez que $\mathbf{MDC}(m_1, m_2) = 1$, *temos que* $\mathbf{MMC}(m_1, m_2)$ *divide* $x_0 - x_1$.

(Existência de solução.)
Sejam $u, v, a_1', a_2' \in \mathbb{Z}$ *tais que*

$$\begin{cases} a_1 a_1' & \equiv_{m_1} & 1 \\ a_2 a_2' & \equiv_{m_2} & 1 \\ m_1 u & \equiv_{m_2} & 1 \\ m_2 v & \equiv_{m_1} & 1 \end{cases}$$

O inteiro

$$x_0 = a_1' v m_2 b_1 + a_2' u m_1 b_2$$

é uma solução particular para o sistema. De fato,

$$\begin{array}{lll} a_1 x_0 = a_1 a_1' v m_2 b_1 + a_1 a_2' u m_1 b_2 & \equiv_{m_1} & a_1 a_1' v m_2 b_1 \equiv_{m_1} b_1 \\ a_2 x_0 = a_2 a_1' v m_2 b_1 + a_2 a_2' u m_1 b_2 & \equiv_{m_1} & a_2 a_2' u m_1 b_2 \equiv_{m_1} b_2 \end{array}$$

□

Corolário 2.65. *Sejam* $a_1, \ldots, a_n, b_1, \ldots, b_n, m_1, \ldots, m_n \mathbb{Z}$ *tais que* $m_1, l \ldots, m_n > 1$, $\mathbf{MDC}(m_\imath, m_\jmath) = 1 \quad \forall \imath \neq \jmath$ *e* $\mathbf{MDC}(a_\imath, m_\jmath) = 1 \quad \forall \imath \neq \jmath$. *Nestas condições o sistema de congruências lineares*

$$\begin{cases} a_1 x & \equiv_{m_1} & b_1 \\ \vdots & \vdots & \vdots \\ a_n x & \equiv_{m_n} & b_n \end{cases}$$

tem uma única solução módulo $\mathfrak{m} = \mathbf{MMC}(m_1, m_2, \ldots, m_n)$. *Mais precisamente, o inteiro*

$$x_0 = a_1' u_1 \frac{\mathfrak{m}}{m_1} b_1 + \cdots + a_n' u_n \frac{\mathfrak{m}}{m_n} b_n$$

, em que $a_\imath'$ *é o inverso de* $a_\imath \bmod m_\imath$ *e* $u_\imath$ *é o inverso de* $\frac{\mathfrak{m}}{m_\imath} \bmod m_\imath$, *é uma solução particular do sistema.*

2.5.6 Exercícios

1. *Determine o conjunto solução das equações diophantinas abaixo:*

   (a) $4x + 7y = 3$

(b) $6x + 8y = 10$

(c) $5x - 9y = 2$

(d) $12x - 28y = 8$

(e) $9x + 12y = 25$

2. *Determine, para cada uma das equações de congruência* $ax \equiv_b c$ *abaixo, quantas soluções incongruentes módulo* b *existem.*

   (a) $4x \equiv_7 3$

   (b) $6x \equiv_8 10$

   (c) $5x \equiv_9 2$

   (d) $12x \equiv_{28} 8$

   (e) $9x \equiv_{12} 25$

3. *Determine a menor solução positiva para os sistema de congruências abaixo*

   (a)

$$\begin{cases} 2x & \equiv_7 & 6 \\ 5x & \equiv_4 & 2 \end{cases}$$

   (b)

$$\begin{cases} 8x & \equiv_{11} & 6 \\ 3x & \equiv_4 & 2 \\ 7x & \equiv_5 & 3 \end{cases}$$

4. *Dois satélites* S_1 *e* S_2 *em órbita sobre a Terra, passam periodicamente sobre Salvador. Sabendo-se que* S_1 *gasta 32 horas para completar sua órbita e que* S_2 *gasta 23 horas, e que hoje* S_1 *foi visto as 11 horas da manhã e* S_2 *foi visto as 10 horas da manhã, determine quando* S_1 *e* S_2 *serão vistos simultaneamente sobre Salvador.*

5. *Determine o resto da divisão de* $\overbrace{111\cdots111}^{2000 \text{ dígitos iguais a } 1}$ *por 7, 11 e 13.*

6. *Determine o resto da divisão de* 2^{100} *por 11.*

7. *Encontre o menor múltiplo positivo de 7 que deixa resto 1 quando dividido por 2,3,4,5 e 6*

8. *Dados $n, m \in \mathbb{N}$ com* $\mathbf{MDC}(n, m) = 1$. *Sejam S_n, S_m respectivamente, o conjunto dos restos possíveis na divisão euclidiana por n e por m. Mostre que a função $\omega : \mathbb{Z} \to S_n \times S_m$ dada por*

$$\omega(x) = (x \text{ Mod } n, x \text{ Mod } m)$$

é sobrejetora.

9. *Encontre o conjunto solução dos seguintes sistemas de congruências lineares*

(a)

$$\begin{cases} 2x & \equiv_4 & 6 \\ 5x & \equiv_3 & 2 \end{cases}$$

(b)

$$\begin{cases} 2x & \equiv_4 & 3 \\ 5x & \equiv_3 & 2 \end{cases}$$

(c)

$$\begin{cases} 2x & \equiv_4 & 6 \\ 6x & \equiv_9 & 12 \end{cases}$$

Referências Bibliográficas

[1] Coutinho, S. C., Números Inteiros e Criptografia RSA, Série de Computação e Matemática, IMPA - SBM, 1997

[2] Dean,R., Elementos de Álgebra Abstrata, Livros Técnicos e científicos editora S.A, 1974.

[3] Fraleigh,J. B., A first course in abstract algebra, sexta edição Addison Wesley longman,2000.

[4] Garcia, A. & Lequain,I., Introdução a Álgebra, Coleção Elementos de Matemática, IMPA-CNPQ, 2002.

[5] Hefez, Abramo.,Curso de Álgebra Coleção Matemática Universitária, vol I,IMPA,1997

[6] Hungerford, T. W., Abstract algebra. An introduction., segunda edição 1997.

[7] Monteiro,L.H. Jacy, Elementos de Álgebra , Coleção Elementos de Matemática, Ed. Ao Livro técnico S.A,1969

[8] Ribenboim, P.,Números primos: mistérios e recordes, Coleção Matemática Universitária, IMPA- CNPq, 2002

[9] Santos, J. Plínio de O., Introdução à Teoria dos Números, Coleção Matemática Universitária, IMPA- CNPq, 1998