NOTAS DE AULA PARA MATEMÁTICA DISCRETA II

ANDREAS B.M. BRUNNER
UFBA

Salvador-Bahia
Abril de 2018

Sumário

Comentário inicial

Estas notas de aula para *Matemática Discreta II* devem ajudar aos estudantes a entender conceitos básicos em teoria dos números e teoria das ordens. A minha ideia de elaborar notas de aula para as disciplinas de Matemática Discreta I e II, já existe bastante tempo. As notas de aula para *Matemática Discreta I* foram finalizadas em julho de 2013. A segunda parte vem em seguida, e se baseia parcialmente na primeira parte, embora um estudante não familiar com a primeira parte deve poder acompanhar sem maiores problemas estas notas. Alguns assuntos como a aritmética de Peano, os vários princípios de indução são repetidos nesta segunda parte, e assim, esta segunda parte é de fato independente da primeira parte, ou seja, das notas para Matemática Discreta I.

Todos os assuntos nestas notas de aula são abordados nos livros citados na bibliografoia. Os livros, [8] e [15], abordam muitos assuntos acerca da matemática discreta, inclusive assuntos que não fazem parte dos cursos oferecidos da UFBA, Matemática Discreta I e II.

Em seguida, explicamos numa primeira parte, conceitos básicos da teoria dos números, como divisibilidade, divisão com resto, numeração, o algoritmo de Euclides, o maior divisor em comum como o mínimo múltiplo em comum de dois números inteiros, equações Diofantinas e o teorema chinês dos restos. Numa segunda parte, introduzimos noções básicas da teoria das ordens. Introduzimos o conceito de ordem parcial com exemplos, esclarecemos ordens no produto, como a ordem por coordenadas e a ordem lexicográfica. Exibimos exemplos e desenhamos ordens em diagramas de Hasse. Definimos conceitos importantes como *infimo* e *supremo* e passo a passo, vamos chegando a definição do conceito de reticulado - importante para estudante da ciência da computação, engenharia da computação, como também da matemática. Exibimos exemplos e demonstramos alguns dos principais resultados acerca da teoria dos reticulados. Finalmente, podemos definir *álgebra de Boole* através de uma ordem parcial, qual é um reticulado distributivo, limitado e complementado. Damos exemplos de álgebras de Boole e demonstramos um teorema do ponto fixo de Tarski para reticulados completos. Tal teorema é de importância para a teoria da computação. Num apendix, explicamos rapidamente como a criptografia **RSA** funciona, e porque ela funciona.

Observemos que as noções abordadas nestas notas se direcionam a estudantes a partir do segundo semestre, cursando algum curso na área das ciências exatas, principalmente aos estudantes das áreas da ciência da computação, sistemas de informação, engenharia da computação, mas acreditamos que também estudantes de matemática - licenciatura e bacharelado - podem tirar bastante aproveito destas notas. Claramente, estas notas devem servir também a estudantes interessados e curiosos em matemática de qualquer outra área. As notas são escritas numa maneira elementar tal que uma pessoa com segundo grau completo deve ser capaz de entender os conceitos. Às vezes, citamos resultados das Notas de Aula para Matemática Discreta I, quais em geral são bastante básicos e conhecidos.

Finalmente, peço desculpas pelos erros, sejam da língua portuguêsa como também de outra natureza.

Salvador, em abril de 2018.

Capítulo 1

Axiomática de Peano, indução e os números inteiros

Neste capítulo, explicamos como podemos justificar matematicamente os números naturais, introduzindo-os pela axiomática de Peano, às vezes conhecido sob o nome de axiomática de Dedekind-Peano. Além disso, falamos da indução matemática e da introdução dos números inteiros. Seguimos [14]. A parte da axiomática de Peano é idêntica a parte sobre os naturais no capítulo 3, em *Notas de aula para matemática discreta I*, cf. [5]. Optamos por repetir esta axiomática, para relembrar ao estudante dos naturais, como também a dar condições de acompanhamento ao estudantes quais não frequentavam a disciplina Matemática Discreta I. Além disso, explicamos rapidamente o conceito de indução em naturais. Finalmente, introduzimos usando uma certa relação de equivalência em pares de naturais, os números inteiros reunido no conjunto $\mathbb{Z}$.

O leitor interessado pode acompanhar vários assuntos desta seção em [4, 8, 11, 14, 15].

1.1 A axiomática de Peano

Começamos com uma citação do matemático Leopold Kronecker:

"Deus criou os números naturais. O resto é obra dos homens."

Os números naturais foram usados durante muito tempo como digamos *dado por deus* ou seja, sem nenhum fundamento matemático. No século 19, Giuseppe Peano (1858-1932) introduziu uma axiomática para fundamentar os naturais matematicamente. Peano era um lógico matemático e distinguiu entre aritmética e lógica - abodagens e ideias novas na época. Na mesma época (por volta de 1879), Gottlob Frege (1848-1925) começou a escrever e terminar o seu *Begriffsschrift*, onde a lógica matemática foi tratada de maneira simbolizada com regras lógicas e com notação bidimensional. Aparentemente, Peano não conhecia o trabalho de Frege, e trabalhou acerca da lógica matemática através de ideias de Boole e Schröder. Entre os axiomas de Peano, foram inicialmente também citados os quatro axiomas acerca da igualdade, ou seja, a igualdade é uma relação reflexiva, simétrica, transitiva e permite substituição em funções por objetos iguais, cf. [5]. Porém, a igualdade pertence a lógica, i.e., a igualdade é um símbolo lógico, e os quatro axiomas são subentendidos na lógica. Logo, não é preciso enunciá-los cada vez falando de uma teoria matemática. Assim, podemos resumir os axiomas de Peano em três axiomas.

Os conceitos básicos[1] são *número natural* e assim o conjunto dos números naturais $\mathbb{N}$, *número zero*, abreviado por 0 e a função *sucessor*, abreviado por $S : \mathbb{N} \to \mathbb{N}$.

[1] O leitor interessado no método axiomático usado em matemática pode consultar [3] ou [5], *Notas de aula para matemática discreta I* capítulo 1, seção 1.1

Observação 1.1.1. *(**A axiomática de Peano**) Existem um conjunto $\mathbb{N}$ dos números naturais, uma constante $0 \in \mathbb{N}$ e uma função $S : \mathbb{N} \to \mathbb{N}$, satisfazendo*

(i) $0 \notin im(S)$, i.e., não existe $n \in \mathbb{N}$ tal que $0 = S(n)$.

(ii) S é uma função injetiva.

(iii) O princípio da Indução Completa:

Se $A \subseteq \mathbb{N}$ é tal que (a) $0 \in A$ e (b) sempre quando $n \in A$, então $S(n) \in A$, então $A = \mathbb{N}$.

Observação 1.1.2. *A axiomática de Peano descreve a estrutura dos naturais. O primeiro axioma garante o elemento 0 é o como dizemos* primeiro elemento em $\mathbb{N}$. *Já os primeiro e segundo axiomas, não permitem uma certa ordem digamos* circular *dos naturais, como também a existência de um natural maior. O último axioma dá conta do fato de que um natural ou é 0 ou é um sucessor de um outro natural. Este axioma é importante, pois não permite a existência de números naturais entre n e $S(n)$.*
*Intuitivamente, podemos pensar que a função S é simplesmente a adição "*mais um*".*

Notação 1.1.3. *Denotamos $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$.*

Proposição 1.1.4. *Com as notações de cima, $im(S) = \mathbb{N}^*$.*

Demonstração: Fazemos a prova por indução sobre $n \in \mathbb{N}$. Primeiramente, observe que se conseguirmos mostrar que $im(S) \cup \{0\} = \mathbb{N}$, então temos a afirmação da proposição. Tomemos agora $A := im(S) \cup \{0\}$ e usamos o axioma (iii) de 1.1.1 para mostrar que $A = \mathbb{N}$.
Num início da indução observe que $0 \in A$, pois $0 \in \{0\}$ e assim vale ítem (a) de axioma (iii) de 1.1.1.
No passo da indução, supomos como *hipótese da indução*, $n \in A$. Queremos mostrar que $S(n) \in A$. Observe que de $n \in A$, temos que $n \in \mathbb{N}$ e consequentemente, $S(n) \in im(S)$. Logo $S(n) \in A$. Pelo princípio da indução completa, $A = \mathbb{N}$, terminando a demonstração. ∎

Antes de demonstrar algumas propriedades acerca dos números naturais, enunciamos algumas definições.

Definição 1.1.5. *Seja $n \in \mathbb{N}$ um natural. Dizemos que $S(n)$ é o* **sucessor** *de n. Neste caso também dizemos que n é o* **antecessor** *de $S(n)$.*

Para poder trabalhar adequadamente com os naturais, é preciso saber da adição e da multiplicação dos naturais. Temos a seguinte

Definição 1.1.6. *(Soma de naturais) Seja m um natural. Definimos por recursão*

$$\begin{cases} m + 0 := m \\ m + S(n) := S(m + n) \end{cases} \tag{1.1}$$

É preciso verificar que esta definição de fato define a adição para quaisquer dois números naturais m e n. Podemos demonstrar isso por indução na próxima proposição, mas observemos que isso também segue do *Teorema da recursão* enunciado em [5].

Proposição 1.1.7. *Sejam $m, n \in \mathbb{N}$. Então, a soma $m + n$ é definida pela definição 1.1.6.*

Demonstração: Seja $m \in \mathbb{N}$ um natural fixo. Tomemos o conjunto $A := \{n \in \mathbb{N} | \quad m + n$ é definida $\}$. Observe que $A \subseteq \mathbb{N}$. Vamos usar o axioma da indução de 1.1.1. Inicialmente, observe que $0 \in A$, pois $m+0 = m$ por 1.1, e assim é definido $m+0$. No passo da indução temos por hipótese da indução que $m+n$ é definida. Vejamos que $m + S(n)$ é definida. Pela definição 1.1.6, observe que $m + S(n) = S(m + n)$, e como $m + n$ é definida, temos que $S(n + m)$ é definida, e portanto $n + S(m)$ é definida. Assim, mostramos que $A = \mathbb{N}$. ∎

Proposição 1.1.8. *(Associatividade) Sejam $m, n, p \in \mathbb{N}$. Então, $(m + n) + p = m + (n + p)$.*

Demonstração: Exibimos mais uma vez uma prova por indução. Sejam os naturais m e n fixos, e mostramos por indução em p que $(m+n)+p = m+(n+p)$ para todo $p \in \mathbb{N}$. Tomemos assim $A := \{p \in \mathbb{N} | \quad (m+n)+p = m+(n+p)\}$.
Início da indução: $0 \in A$, pois $(m+n)+0 = m+n$ por definição 1.1.6. Por outro lado, temos que $m+(n+0) = m+n$, também por 1.1.6.
Passo da indução: Temos por hipótese da indução que $n \in A$, ou seja, $(m+n)+p = m+(n+p)$. Vamos mostrar que $S(p) \in A$. Para isso, observe que usando 1.1, a hipótese de indução e novamente 1.1:
$(m+n)+S(p) = S((m+n)+p) = S(m+(n+p)) = m+S((n+p)) = m+(n+S(p))$, ou seja, $S(p) \in A$.
Pelo axioma (iii) de 1.1.1, temos que $A = \mathbb{N}$, ou seja, vale a afirmação da proposição. ∎

Proposição 1.1.9. *(Elemento neutro) Seja $m \in \mathbb{N}$. Então,*

$$m + 0 = m = 0 + m \tag{1.2}$$

Demonstração: Observe que por 1.1, temos que $m+0 = m$. Falta mostrar que $0+m = m$, para todo $m \in \mathbb{N}$. Para isso, tomamos $A := \{m \in \mathbb{N} | \quad 0+m = m\}$. Observe que por 1.1, $0+0 = 0$ e portanto $0 \in A$. Para o passo de indução, temos usando 1.1 e a hipótese da indução o seguinte:
$0+S(m) = S(0+m) = S(m)$, e assim, $S(m) \in A$. Logo, vale 1.2. ∎

Observação 1.1.10. *O elemento 0 é único elemento em $\mathbb{N}$ satisfazendo 1.2.*

Demonstração: Sejam 0 e $0'$ dois elementos de $\mathbb{N}$, satisfazendo 1.2. Vamos mostrar que $0 = 0'$. Observe que para qualquer $m \in \mathbb{N}$ temos que $m + 0' = m = 0' + m$. Em particular, usando isso e 1.2 para $m = 0$, temos que $0' = 0 + 0' = 0$. ∎

Definição 1.1.11. *Definimos $1 := S(0)$.*

As provas dos próximos dois resultados deixamos como exercícios. Uma simples indução junto com os resultados obtidos anteriormente resolvem isto.

Proposição 1.1.12. *Para qualquer $n \in \mathbb{N}$, temos que $S(n) = 1 + n$.* ∎

Proposição 1.1.13. *(Comutatividade) Para quaisquer $n, m \in \mathbb{N}$, temos que $n + m = m + n$.* ∎

Falta definir a multiplicação de dois naturais. Para isso, precisamos a adição a as suas propriedades introduzidas anteriormente. Temos por recursão a seguinte

Definição 1.1.14. *(Produto de naturais) Seja m um natural. Definimos por recursão*

$$\begin{cases} m \cdot 0 := 0 \\ m \cdot S(n) := (m \cdot n) + m \end{cases} \tag{1.3}$$

Como acima é preciso demonstrar a seguinte

Proposição 1.1.15. *Sejam $m, n \in \mathbb{N}$. Então, o produto $m \cdot n$ é definida pela definição 1.1.14.* ∎

Observação 1.1.16. *Na lista de exercícios temos algumas propriedades para o produto de números naturais, entre outros a lei do cancelamento da adição:*

$$\forall n, m, k \in \mathbb{N}, \qquad n + k = m + k \quad \Rightarrow \quad n = m.$$ ∎

Finalizando a seção sobre os naturais, introduzimos ainda a relação de *menor ou igual* entre números naturais, como segue.

Definição 1.1.17. *Sejam $n, m \in \mathbb{N}$ naturais. Dizemos que n é* **menor ou igual** *a m, $n \leq m$ sse existe $k \in \mathbb{N}$ tal que $n + k = m$.*

Notação 1.1.18. *Denotamos $n < m$ para $n \leq m$ e $n \neq m$, para números naturais n e m.*

As demonstrações dos ítens da próxima observação é feito nos exercícios.

Observação 1.1.19. *A relação introduzido em 1.1.17 satisfaz*
(a) $\forall n \in \mathbb{N}, \quad n \leq n$. (reflexividade)
(b) $\forall n, m \in \mathbb{N}, \quad$ se $n \leq m$ & $m \leq n$, então $n = m$. (anti-simetria)
(c) $\forall n, m, p \in \mathbb{N}, \quad$ se $n \leq m$ & $m \leq p$, então $n \leq p$. (transitividade)
(d) $\forall n, m \in \mathbb{N}, \quad n \leq m$ ou $m \leq n$. (conexão) ∎

1.2 Dois princípios de indução

O princípio da indução matemática nos números naturais, qual aparece na axiomática de Peano, cf. 1.1.1 (iii), é de uma importância, pois este princípio permite demonstrar propriedades acerca de todos os números naturais. Além da forma da indução introduzido na seção 1.1, temos mais dois princípios equivalentes para indução nos naturais. Vamos exibi-los sem demonstração.

Observação 1.2.1. *(Princípio da indução 1^a forma) Seja φ uma propriedade para naturais tal que*
(i) 0 tem a propriedade φ, i.e., $\varphi(0)$, e
(ii) Se $\varphi(k)$ for verdadeira então $\varphi(k+1)$ é verdadeira.
Então, $\varphi(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

Observação 1.2.2. *(Princípio da indução 2^a forma) Seja φ uma propriedade para naturais tal que*
(i) 0 tem a propriedade φ, i.e., $\varphi(0)$, e
(ii) Se $\varphi(r)$ for verdadeira para qualquer $0 \leq r \leq k$, $k > 0$ então $\varphi(k+1)$ é verdadeira.
Então, $\varphi(n)$ é verdadeira, para qualquer $n \in \mathbb{N}$.

Proposição 1.2.3. *São equivalentes*

(a) O princípio da indução completa, cf. 1.1.1,
(b) O princípio da indução 1^a forma, cf. 1.2.1, e
(c) O princípio da indução 2^a forma, cf. 1.2.2

Demonstração: A demonstração dessa proposição pode ser consultada em *Notas de aula para matemática discreta I*, cf. [5], no capítulo 3, seção 3.2. O leitor interessado deve tirar as eventuais dúvidas. ∎

Temos os seguintes dois exemplos para ilustrar provas por indução, usando os princípios novos introduzidos acima.

Exemplo 1.2.4. *(a) Vamos mostrar que $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. $\forall n \in \mathbb{N} \quad (*)$*
Usamos a indução (1^a forma), cf. 1.2.1 e começamos pelo
Início da indução, $n = 0$: Observe que para o lado esquerdo, $\sum_{k=0}^{0} = 0$. Para o lado direito, calculamos $\frac{0(0+1)}{2} = 0$. Assim coincidem os dois lados e provamos a afirmação $(*)$ para $n = 0$.
Passo da indução: Vale $(*)$ para n, observe que isto é a hipótese da indução. Vejamos que $(*)$ vale também para $(n+1)$. Para isso, calculamos usando a definição da soma e a hipótese da indução:

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2+3n+2}{2}.$$

Por outro lado, temos que $\frac{(n+1)(n+2)}{2} = \frac{n^2+3n+2}{2}$, mostrando $(*)$ para $n+1$. Pelo princípio da indução temos que $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. $\forall n \in \mathbb{N}$. ∎

(b) Definimos a série de **Fibonacci** *no seguinte modo por recursão:*

$$\begin{cases} a_0 := 1, \quad a_1 := 1 \\ a_{n+2} := a_n + a_{n+1}, \quad \forall n \geq 0 \end{cases} \tag{1.4}$$

Vamos mostrar que $\quad a_n < (\frac{7}{4})^n, \quad \forall n \geq 1 \quad (**)$
Elaboramos a prova por indução (2^a forma), cf. 1.2.2. O início da indução para $n = 1$ é trivial.
Vejamos agora o passo da indução e para isso, seja $n > 1$. Vamos mostrar que $a_{n+1} < (\frac{7}{4})^{n+1}$. Temos as seguintes hipóteses da indução: $a_k < (\frac{7}{4})^k$, para $n > 1$ e $2 \leq k \leq n$.
Pela definição dos números de Fibonacci, 1.4, temos que $a_{n+1} = a_{n-1} + a_n$. Então, observe que pela definição e pelas hipóteses da indução temos que

$$a_{n+1} = a_{n-1} + a_n < (\tfrac{7}{4})^{n-1} + (\tfrac{7}{4})^n = (\tfrac{7}{4})^{n-1}(1 + \tfrac{7}{4}) < (\tfrac{7}{4})^{n-1} \cdot (\tfrac{7}{4})^2 = (\tfrac{7}{4})^{n+1},$$

o que era para mostrar. ∎

1.3 Os números inteiros

Sabemos então como podemos justificar matematicamente os números naturais através da axiomática de Peano. Vimos que todas as propriedades dos naturais são demonstráveis a partir da axiomática. A seguinte construção da introdução dos números inteiros é *standard*, e importante para estudantes de matemática. Damos aqui as idéias básicas para esta construção. Para os estudantes de áreas como ciência da computação ou engenharia da computação a aplicação da relação de equivalência é um bom momento repetir as sabedorias acerca da relação de equivalência.

Em seguida, introduzimos os números inteiros através dos naturais. Para isso, consideremos primeiramente o produto Cartesiano

$$\mathbb{N} \times \mathbb{N} := \{\langle n; m\rangle | \quad n, m \in \mathbb{N}\}.$$

Definição 1.3.1. *No conjunto $\mathbb{N} \times \mathbb{N}$ introduzimos a seguinte relação:*

$$\forall n, m, k, l \in \mathbb{N}, \qquad \langle n; m\rangle \sim \langle k; l\rangle \quad sse \quad n + l = m + k.$$

Observe que por exemplo, $\langle 4; 6\rangle \sim \langle 7; 9\rangle$.

Agora vamos relembrar do conceito da relação de equivalência introduzida em [5], no capítulo 4, seção 4.2. Uma relação de equivalência r no conunto a é simplesmente uma relação reflexiva, simétrica e transitiva. O leitor é convidado em consultar a seção 4.2. Temos agora a seguinte

Observação 1.3.2. *Com as notações.*
(a) A relação $\sim$ introduzida acima é de fato uma relação de equivalência em $\mathbb{N} \times \mathbb{N}$.
(b) Podemos formar o conjunto quociente, $\big((\mathbb{N} \times \mathbb{N})/\sim\big) := \{\overline{\langle n; m\rangle} | \quad n, m \in \mathbb{N}\}$, onde a classe $\overline{\langle n; m\rangle}$ é dada pelo conjunto $\overline{\langle n; m\rangle} := \{\langle k; l\rangle \in \mathbb{N} \times \mathbb{N} | \quad \langle n; m\rangle \sim \langle k; l\rangle\}$.

Demonstração: É preciso verificar as três condições para relação de equivalência. Vejamos somente que $\sim$ é reflexiva em $\mathbb{N} \times \mathbb{N}$, ficando o resto da demonstração como exercício.
Seja $\langle n; m\rangle \in \mathbb{N} \times \mathbb{N}$. Vamos mostrar que $\langle n; m\rangle \sim \langle n; m\rangle$ - o que é a condição da reflexividade. Mas, observe que por 1.1.13, sabemos que $n + m = m + n$, o que significa pela definição 1.3.1 que $\langle n; m\rangle \sim \langle n; m\rangle$. Assim, $\sim$ é reflexiva.
Falta demonstrar que $\sim$ é simétrica e transitiva, no ítem (b) não há nada a demonstrar. ∎

Podemos definir agora matematicamente o conjunto dos inteiros.

Definição 1.3.3. *Com as notações.*
(i) Dizemos que $\mathbb{Z} := \big((\mathbb{N}\times\mathbb{N})/\sim\big)$ *é o* **conjunto dos inteiros**.
(ii) Introduzimos para $\alpha := \overline{\langle n;m\rangle}$ *e* $\beta := \overline{\langle k;l\rangle}$ *dois inteiros a soma* $+_{\mathbb{Z}}$ *por*

$$\alpha +_{\mathbb{Z}} \beta := \overline{\langle n+k, m+l\rangle}.$$

Observação 1.3.4. *(a) Observe que a soma* $+_{\mathbb{Z}}$ *nos inteiros é definida da soma* $+$ *entre os naturais. Em seguida, não diferenciamos entre* $+_{\mathbb{Z}}$ *e* $+$ *am naturais, usamos a notação* $+$ *em ambos os casos.*
(b) Observe que a definição 1.3.3 é uma definição entre dois conjuntos. Assim é preciso ter certeza que esta definição é uma **boa definição***, ou seja,* **independente dos seus representantes**.

Demonstração: Vamos demonstrar o ítem (b). Esta demonstração é importante, pois sempre definindo funções ou relações em classes de equivalências é preciso ter certeza que temos uma boa definição. Procedemos de seguinte maneira:
Sejam $\overline{\langle n;m\rangle} = \overline{\langle n';m'\rangle}$ e $\overline{\langle k;l\rangle} = \overline{\langle k';l'\rangle}$. $(*)$
Para tivermos uma boa definição da soma é preciso agora que acontece

$$\overline{\langle n;m\rangle} + \overline{\langle k;l\rangle} = \overline{\langle n';m'\rangle} = \overline{\langle k';l'\rangle}, \text{ ou seja}$$
$$\overline{\langle n+k, m+l\rangle} = \overline{\langle n'+k', m'+l'\rangle}.$$

Mas isto é equivalente - usando a definição de $\sim$ dada em 1.3.1 com

$$(n+k)+(m'+l') = (m+l)+(n'+k').$$

Observe que temos pela hipótese $(*)$, que $n+m' = m+n'$ e $k+l' = l+k'$. Usando isso e propriedades demonstradas (associatividade e comutatividade) acerca dos números naturais em seção 1.1, obtemos que $(n+k)+(m'+l') = (n+m')+(k+l') = (m+n')+(l+k') = (m+l)+(n'+k')$, o que era para demonstrar. Assim, não importa qual representante escolhemos para somar dois números inteiros, a soma é **unicamente** determinada pela definição introduzida em 1.3.3. ∎

Sabendo que a nossa definição da soma entre dois inteiros é boa podemos demonstrar algumas propriedades bem conhecidos acerca dos números inteiros.

Proposição 1.3.5. *Sejam* $\alpha,\beta,\gamma \in \mathbb{Z}$ *inteiros. Então,*

(i) $\alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma$, *(associativivdade da adição).*
(ii) $\alpha+\mathfrak{o} = \mathfrak{o}+\alpha = \alpha$, *para algum* $\mathfrak{o}\in\mathbb{Z}$, *(elemento neutro da adição).*
(iii) $\alpha+\alpha' = \mathfrak{o} = \alpha'+\alpha$, *para um único* $\alpha'\in\mathbb{Z}$, *(elemento oposto da adição).*
(iv) $\alpha+\beta = \beta+\alpha$, *(comutatividade da adição).*

Demonstração: A demonstração desta proposição é uma (simples) aplicação da definição 1.3.3 e das propriedades demonstradas sobre os naturais em seção 1.1. Observe que o elemento neutro $\mathfrak{o}$ é dado pela classe $\overline{\langle 0;0\rangle}$, enquanto o elemento oposto de $\alpha := \langle n;m\rangle$ é dado por $\alpha' := \langle m;n\rangle$. Denotamos o elemento oposto de α com $-\alpha$.
Vejamos a demonstração de (iv). Sejam $\alpha := \overline{\langle n;m\rangle}$ e $\beta := \overline{\langle k;l\rangle}$. Assim, temos que $\alpha+\beta = \overline{\langle n+k;m+l\rangle} = \overline{\langle k+n;l+m\rangle} = \beta+\alpha$, onde a penúltima igualdade é consequência de 1.1.13. Os outros detalhes desta demonstração são feitos em exercícios. ∎

Para poder trabalhar bem com os números inteiros introduzimos agora a multiplicação.

Definição 1.3.6. *Sejam* $\alpha := \overline{\langle n;m\rangle}$ *e* $\beta := \overline{\langle k;l\rangle}$ *dois inteiros. Definimos o* **produto de** α **e** β *como sendo o seguinte elemento em* $\mathbb{Z}$, $\quad \alpha\cdot_{\mathbb{Z}}\beta = \overline{\langle nk+ml; nl+mk\rangle}$.

Temos a observação análoga de 1.3.4.

Observação 1.3.7. *(a) Observe que o produto* $\cdot_{\mathbb{Z}}$ *nos inteiros é definida do produto* $\cdot$ *entre os naturais. Em seguida, não diferenciamos entre* $\cdot_{\mathbb{Z}}$ *e* $\cdot$ *em naturais, usamos a notação* $\cdot$ *em ambos os casos.*

(b) Observe que a definição 1.3.6 é uma definição entre dois conjuntos. Assim é preciso ter certeza que esta definição é uma **boa definição***, ou seja,* **independente dos seus representantes***.*

Demonstração: Mostre que de fato a definição do produto é uma boa definição. Adapte as idéias da demonstração de 1.3.4. ∎

Temos as seguintes propriedades acerca do produto entre dois inteiros.

Proposição 1.3.8. *Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$ inteiros. Então,*

(i) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$, *(associativivdade da multiplicação).*
(ii) $\alpha \cdot \mathtt{1} = \mathtt{1} \cdot \alpha = \alpha$, *para algum* $\mathtt{1} \in \mathbb{Z}$, *(elemento neutro da multiplicação).*
(iii) $\alpha \cdot \beta = \beta \cdot \alpha$, *(comutatividade da multiplicação).*
(iv) $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$, *(distributividade entre multiplicação e adição).*
(v) Se $\alpha \neq \mathtt{0}$, $\alpha \cdot \gamma = \alpha \cdot \beta \quad \Rightarrow \quad \gamma = \beta$, *(cancelamento da multiplicação).*

Demonstração: As demonstrações ficam com exercícios e são simples aplicações das definições e das propriedades sobre os números naturais. Observe que $\mathtt{1} := \overline{\langle 1; 0 \rangle}$. ∎

Introduzimos agora a ordem $\leq$ em $\mathbb{Z}$.

Definição 1.3.9. *Sejam $\alpha := \overline{\langle n; m \rangle}$ e $\beta := \overline{\langle k; l \rangle}$ dois inteiros.*
(a) Dizemos que α é **menos ou igual a** *β, $\alpha \leq \beta$, sse $n + l \leq_{\mathbb{N}} m + k$, ond $\leq_{\mathbb{N}}$ é a relação de ordem nos naturais definida em 1.1.17. Definimos normalmente $\alpha < \beta$ sse $\alpha \leq \beta$ e $\alpha \neq \beta$.*
(b) Dizemos que α é **negativo** *sse $\alpha < \mathtt{0}$.*
Analogamente, definimos $\alpha \geq \beta$ e α é positivo. (Elabore as definições em exercício).

Observação 1.3.10. *Com as notações.*
(i) A definição 1.3.9 é de fato uma boa definição*.*
(ii) O inteiro $\alpha := \overline{\langle n; m \rangle}$ é negativo sse $n < m$.
(iii) Em seguida, identificamos as classes $\mathtt{0} = \overline{\langle 0, 0 \rangle}$ simplesmente com 0, $\mathtt{1} = \overline{\langle 1; 0 \rangle}$ com 1 e $\overline{\langle 0; 1 \rangle}$ com -1.

Demonstração: Exercício. ∎

A seguinte proposição reune boa parte das propriedades dos números inteiros. Em vez das letras gregas voltamos a usar letras de latim. O leitor deve estar alerto que na hora da demonstração dos resultados é transferir as classes e trabalhar com as definições feitas acima e com as propriedades nos naturais.

Proposição 1.3.11. *Sejam a, b, c inteiros. Então,*

(i) $(a + b) + c = a + (b + c)$, *(associativivdade da adição).*
(ii) $a + 0 = a = 0 + a$, *(0 é elemento neutro da adição).*
(iii) $a + (-a) = 0 = (-a) + a$, *($-a$ é elemento oposto de a da adição).*
(iv) $a + b = b + a$, *(comutatividade da adição).*
(v) $(ab)c = a(bc)$, *(associatividade da multiplicação).*
(vi) $a1 = a = 1a$, *(1 é elemento neutro da multiplicação).*
(vii) $ab = ba$, *(comutatividade da multiplicação).*
(viii) $a(b + c) = ac + bc$, *(distributividade entre multiplicação e adição).*
(ix)[2] $0 \neq 1$.
(x) Se $a \neq 0$, *então,* $ab = ac \quad \Rightarrow \quad b = c$, *(cancelamento da multiplicação),*
(xi) $a \leq a$, *(reflexividade de $\leq$).*
(xii) $a \leq b$ *e* $b \leq a \quad \Rightarrow \quad a = b$, *(anti-simetria de $\leq$).*
(xiii) $a \leq b$ *e* $b \leq c \quad \Rightarrow \quad a \leq c$, *(transitividade de $\leq$).*

[2]Este axioma exclui anéis degenerados com um só elemento.

(xiv) $a \leq b$ *ou* $b \leq a$, *(linearidade de* $\leq$*).*
(xv) $a \leq b \quad \Rightarrow \quad a + c \leq b + c$, *(monotonicidade de* $\leq$ *em respeito da adição).*
Se $0 \leq c$ *e* $a \leq b \quad \Rightarrow \quad ac \leq bc$, *(monotonicidade de* $\leq$ *em respeito da multiplicação).*
(xvi) **O princípio da boa ordem***:*
Seja A *um conjunto não vazio de inteiros não negativos. Então* A *contém um primeiro (i.e., menor) elemento, ou seja, existe* $a \in A$ *tal que* $\forall x \in A, a \leq x$.

Demonstração: Exercício. ∎

Observação 1.3.12. *(a) Poderíamos ter introduzidos os números inteiros postulando axiomas. Alguns livros abordam esta tática. Principalmente, em falta de tempo (às vezes acontece nas aulas de Matemática Discreta II), se introduz os inteiros de maneira axiomática. A lista de axiomas é dada na proposição 1.3.11. A introdução dos inteiros a partir dos naturais deve ser interessante para estudantes de matemática. Para os estudantes , digamos* não da matemática *a introdução dos inteiros via axiomas de 1.3.11 é suficiente. Optamos mesmo assim em exibir a introdução matematicamente fundada, pela simples razão que o estudante pode aprender a trabalhar axiomaticamente, treinar o conceito da relação de equivalência e de ter uma talvez nova visão acerca da matemática que tenta justificar o máximo possível.*
Resumindo, é possível justificar os números inteiros - em quais vamos trabalhar em seguida - totalmente dos números naturais - quais dependem da axiomática de Peano. Uma outra abordagem é introduzir, como dito acima, os inteiros com os axiomas de 1.3.11.
(b) O estudante deveria saber as principais regras*, trabalhando nos inteiros. Um dos pontos importantes é que nos inteiros* **não** *temos divisão.*
(c) Uma estrutura algébrica[3] $(G; +, 0)$ *satisfazendo os axiomas (i) - (iii) de 1.3.11 é dito um* **grupo**.
(d) Uma estrutura algébrica $(A; +, \cdot, 0, 1)$ *satisfazendo os axiomas (i) - (ix) da proposição 1.3.11, é dito* **anel comutativo com unidade**.
(e) O princípio da boa ordem é um outro equivalente aos princípios de indução introduzido em seção 1.2. Em [5], as equivalências são demonstradas detalhadamente. O leitor interessado deve consulta-los. ∎

A partir da última proposição 1.3.11, podemos demonstrar mais propriedades importantes acerca dos inteiros.

Proposição 1.3.13. *Sejam* $a, b, c \in \mathbb{Z}$ *inteiros. Então,*

(i) Se $a + b = a + c$ *então,* $a = c$ *(cancelamento da adição).*
(ii) $a0 = 0$.

Demonstração: Vejamos o ítem (a). Sejam $a, b, c \in \mathbb{Z}$ inteiros tais que $a + b = a + c$. Aí, observe que $(-a) + (a + b) = (-a) + (a + c)$. Aplicando a associatividade, e o fato de que $-a$ é oposto de a, cf. 1.3.11, obtemos que $b = c$.
Para o ítem (b), observe que para $a \in \mathbb{Z}$, temos usando distributividade, elemento neutro de 1.3.11 que $a0 + a0 = a(0 + 0) = a0 = a0 + 0$. Logo, usando (a), obtemos que $a0 = 0$. ∎

Proposição 1.3.14. *(***Regra dos sinais***) Sejam* $a, b \in \mathbb{Z}$ *inteiros. Então,*

(i) $-(-a) = a$, *(ii)* $(-a)b = -(ab) = a(-b)$, *(iii)* $(-a)(-b) = ab$.

Demonstração: Usamos novamente a proposição 1.3.11. Observe que $a + (-a) = 0$, e assim a é o oposto de $(-a)$. Por outro lado, o oposto de $(-a)$ é formalmente $-(-a)$. Como o oposto é único, e $(-a)$ tem os

[3]Uma estrutura algébrica em matemática consiste de um conjunto não vazio de suporte, digamos A, e de operações f_i, $i \in I$, de aridade n_i. Denotamos uma estrutura por $(A; (f_i)_{i \in I})$. Por exemplo, $(\mathbb{Z}; +, \cdot, 0, 1)$ é neste contexto uma estrutura algébrica, onde temos um conjunto de suporte $\mathbb{Z}$, duas operações binárias $+$ e $\cdot$, e duas operações 0-árias que são as constantes 0 e 1. Também em caso de grupo, temos $G \neq \emptyset$, $+$ uma operação binária e 0 uma constante, é considerada uma estrutura algébrica. Veja também 4.3.1 na seção 4.3

opostos a e $-(-a)$, é preciso ter $a = -(-a)$, mostrando o ítem (i).
Observe que $ab + (-a)b = (a + (-a))b = 0b = b0 = 0$, usando 1.3.11 e 1.3.13. Assim, obtemos que o oposto de ab é $(-a)b$, e pela unicidade do elemento oposto, $-(ab) = (-a)b$. Analogamente, demonstramos $-(ab) = a(-b)$ (exercício !), mostrando o ítem (ii).
Para o ítem (iii), observe que $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, usando duas vezes (ii) e a última igualdade segue de (i). ∎

Em seguida, temos mais uma proprosição importante.

Proposição 1.3.15. *Seja $a \in \mathbb{Z}$ um inteiro. Então,*
(i) $a \leq 0 \quad \Rightarrow \quad 0 \leq (-a)$.
(ii) $0 \leq a \quad \Rightarrow \quad (-a) \leq 0$.
(iii) $0 \leq a^2$.
(iv) $0 < 1$.

Demonstração: Observe que de $a \leq 0$ temos de 1.3.11 que $(-a) + a \leq (-a)$. Novamente por 1.3.11, temos que $0 \leq (-a)$, sendo demonstrado (i). O ítem (ii) se mostra analogamente (exercício). O ítem (iii), faremos em dois casos.
Caso 1: $0 \leq a$. Então, por 1.3.11, $0 \cdot a \leq a^2$, ou seja, por 1.3.13, $0 \leq a^2$.
Caso 2: $a \leq 0$. Então, por (i), $0 \leq (-a)$, e usando 1.3.11, $0(-a) \leq (-a)(-a)$. Por 1.3.13 e 1.3.14, temos que $0 \leq a^2$.
Assim, está demonstrada (iii). Para verificar (iv) observe que como $1^2 = 1$, temos que $0 \leq 1$. Como $0 \neq 1$, temos que $0 < 1$. ∎

As próximas duas proposições são consequências do princípio da boa ordem.

Proposição 1.3.16. *Seja $a \in \mathbb{Z}$ um inteiro tal que $0 \leq a \leq 1$. Então, $a = 0$ ou $a = 1$.*

Demonstração: Exibimos uma demonstração *por absurdo*, cf. capítulo 1, seção 1.4 em [5]. Suponha que existe $a \in \mathbb{Z}$ tal que $0 \leq a \leq 1$ e $a \neq 0$ e $a \neq 1$. Assim é claro que o conjunto $A := \{t \in \mathbb{Z} | \quad 0 < t < 1\}$ não é vazio. Logo, estamos em condições de aplicar o princípio da boa ordem, cf. 1.3.11, (xvi), e achar um menor elemento $m \in A$. Observe que $m \in A$ significa $m \in \mathbb{Z}$, $0 < m$ e $m < 1$. Portanto, usando 1.3.11, (xv), obtemos que $m^2 < m1 = m < 1$. Sabendo que $0 < m^2$, pela proposição anterior, temos que $m^2 \in A$. Temos resumindo que $m^2 \in \mathbb{Z}$, $0 < m^2 < 1$ e $m^2 < m$, contradizendo ao fato que m era menor elemento em A. Portanto a nossa suposição inicial de $A \neq \emptyset$ era falsa, e temos que $A = \emptyset$, mostrando a proposição. ∎

Proposição 1.3.17. *(Propriedade Arquimediana) Sejam a e b dois inteiros positivos. Então, existe um inteiro $k > 0$ tal que $b < na$.*

Demonstração: Mais uma vez vamos aplicar o princípio da boa ordem, 1.3.11, (xvi). Sejam a, b inteiros tais que $a, b > 0$. Vamos supor (por absurdo) que

$$\forall n > 0, \quad na \leq b, \text{ ou seja, } 0 \leq b - na. \qquad (*)$$

Consideremos então o conjunto $A := \{b - na | \quad n > 0\}$. Observe que A é conjunto de inteiros não negativos e obviamente não vazio. Pelo princípio da boa ordem, existe menor elemento $m \in A$. Assim, existe $n > 0$ tal que $m = b - na$.
Observe que $m' = b - (n + 1)a = (b - na) - a = m - a$. Como $a > 0$, temos que $m - a < m$ e por $(*)$ temos que $(m - a) = b - (n + 1)a \in A$. Mas, isto é um absurdo à minimalidade de m. Logo, a suposição $(*)$ é falsa, e vale a proposição. ∎

Capítulo 2

Introdução à teoria dos números

Neste capítulo introduzimos conceitos importantes e básicos acerca da teoria dos números. Os assuntos são abordados talvez de maneiras diferentes nos livros [1], [10], [11], [13] e [14]. Muitas vezes seguimos [14], neste capítulo.

2.1 Divisibilidade e divisão com resto

Vamos relembrar novamente que **não** temos *frações* do tipo $\frac{a}{b}$. Isto simplesmente, pois sabemos que números do tipo $\frac{a}{b} \notin \mathbb{Z}$. Mesmo assim queremos e podemos falar de uma divisibilidade, e esta divisibilidade vamos expressar via multiplicação.

Definição 2.1.1. *Sejam $a, b \in \mathbb{Z}$ dois inteiros. Dizemos que a* **divide** *b, $a|b$, sse existe $k \in \mathbb{Z}$ tal que $b = ka$. Neste caso, também podemos dizer que b é* **múltiplo** *de a.*

Observação 2.1.2. *(i) Observe que $1|0$, pois $0 = 0 \cdot 1$. Também $4|(-16)$, pois $-16 = (-4) \cdot 4$.*
(ii) Sejam a e b dois inteiros e $a \neq 0$ tais que $a|b$, então existe um **único** *$k \in \mathbb{Z}$ tal que $b = ka$.*
(iii) Temos a seguinte equivalência: $0|a$ *sse* $a = 0$.

Demonstração: Vamos demonstrar (ii). Sejam $a, b \in \mathbb{Z}$ tais que $a \neq 0$ e $a|b$. Para mostrar a unicidade do inteiro k tal que $b = ka$, vamos supor que temos $k' \in \mathbb{Z}$ tal que $b = k'a$. Vejamos que $k = k'$. Mas isto é simples, observe que das hipóteses, $ka = k'a$. Como pela hipótese $a \neq 0$, podemos cancelar, 1.3.11 (xv), e obtemos que $k = k'$, mostrando a unicidade da constante k.
Para o ítem (iii), observe pela definição da dividisibilidade que $0|a$ sse existe $k \in \mathbb{Z}$ tal que $a = k0 = 0$. ∎

Em seguida, sempre vamos excluir o caso de dividir por 0, ou seja, escrevendo $a|b$, já estamos *entendendo* que $a \neq 0$.

Relembramos que o valor absoluto de um inteiro $a \in \mathbb{Z}$ pode ser definido como sendo

$$|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{caso contrário} \end{cases}$$

Observação 2.1.3. *Sejam a e b inteiros tais que $a|b$ e $b \neq 0$. Então $|a| \leq |b|$.*

Demonstração: Como $a|b$, sabemos que existe único $k \in \mathbb{Z}$ tal que $b = ka$. Logo, temos que $|b| = |ka| = |k||a|$. Usando agora a hipótese que $b \neq 0$, temos que $|k| \geq 1$. Assim, temos por 1.3.11, (xv), que $|a| \leq |k||a| = |b|$. ∎

Temos o seguinte Lema, qual segue da última observação.

Lema 2.1.4. *(a)* 1 *tem somente os divisores* 1 *e* -1.
(b) Sejam a, b *inteiros tais que* $a|b$ *e* $b|a$*, então* $|a| = |b|$.

Demonstração: Seja b um divisor de 1, então temos por 2.1.3 que $|b| \leq 1$. Usando 1.3.16 e o fato de que $b \neq 0$, temos que $|b| = 1$, mostrando (a).
Para verificar (b), sejam a e b inteiros tais que $a|b$ e $b|a$. Assim, existem $k, k' \in \mathbb{Z}$ tais que $b = ka$ e $a = k'b$. Substituindo, obtemos que $b = ka = k(k'b) = (kk')b$. Como $b \neq 0$, podemos cancelar b, cf 1.3.11, e assim $1 = kk'$. Portanto, $k|1$ e pelo ítem (a), $|k| = 1$. Analogamente, $|k'| = 1$, e logo, $|a| = |b|$. ∎

Proposição 2.1.5. *Sejam* a, b, c *e* d *números inteiros. Então*

(a) $a|a$ *(reflexividade da divisão),*
(b) $a|b$ *e* $b|c \quad \Rightarrow \quad a|c$ *(transitividade da divisão),*
(c) $a|b$ *e* $c|d \quad \Rightarrow \quad (ac)|(bd)$,
(d) $a|b$ *e* $a|c \quad \Rightarrow \quad a|(mb + nc), \quad \forall m, n \in \mathbb{Z}$*. Em particular,* $a|b$ *e* $a|c \quad \Rightarrow \quad a|(b + c)$.

Demonstração: A demonstração é obtida através de aplicações da definição. Vejamos somente o ítem (c). Sejam a, b, c e d inteiros tais que $a|b$ e $c|d$. Então, temos (pela definição 2.1.1) que existem $k, k' \in \mathbb{Z}$ tais que $b = ka$ e $d = k'c$. Usando isso obtemos que $bd = (ka)(k'c)$. Usando as propriedades dos números inteiros conforme 1.3.11, (v), (vii) temos que $bd = (ka)(k'c) = k(ak')c = k(k'a)c = (kk')(ac)$. Como os inteiros são fechados pela operação da adição e multiplicação sabemos que $kk' \in \mathbb{Z}$, e pela definição 2.1.1, temos que $(ac)|(bd)$, o que era para demonstrar. Os itens restantes são demonstrados de maneira analoga e ficam como exercício para o estudante. ∎

Observação 2.1.6. *(a) Observe que a divisibilidade* $|$ *é uma relação nos números inteiros, ou seja, temos que* $| \subseteq \mathbb{Z} \times \mathbb{Z}$*, conforme a definição de [5].*
(b) Já mostramos na proposição anterior que a estrutura $(\mathbb{Z}, |)$ *é uma pré-ordem, i.e., satisfaz os axiomas (xi) e (xiii) de 1.3.11.* ∎

Agora, sabemos como se comporta a divisibilidade nos inteiros. Podemos perguntar o que acontece se tivermos dois inteiros a e b para quais nem $a|b$, nem $b|a$. O que podemos fazer neste caso? No segundo grau, aprendemos a divisão com resto. Temos por exemplo que $15 \not| 4$ e $4 \not| 15$. Mas podemos dividir 15 por 4 e obtemos que 15 é igual a 3 vezes 4 com resto 3, ou seja, $15 = 3 \cdot 4 + 3$. Também, temos que $4 = 0 \cdot 15 + 4$. Assim, perguntamos se sempre é possível dividir um número inteiro por outro com resto positivo menor possível?[1] Observe que assim também os números negativos são inclusos.

Vejamos em seguida que isto de fato é sempre possível, ou seja, para números inteiros $a, b \in \mathbb{Z}$, $b \neq 0$, temos que

$$a = q \cdot b + r, \text{ onde } r \text{ é tal que } 0 \leq r < |b|. \qquad (*)$$

Em seguida, vamos mostrar $(*)$ qual é um dos teoremas fundamentais nesta introdução à teoria dos números. Podemos reduzir o caso geral para o caso dos números não negativos, e usamos na demonstração o princípio da boa ordem, cf. 1.3.11, (xvi).

Lema 2.1.7. *Sejam* $a \geq 0$ *e* $b > 0$ *inteiros. Então, existem* $q, r \in \mathbb{Z}$ *tais que*
$$a = qb + r, \text{ onde } 0 \leq r < b.$$

Demonstração: Vamos aplicar o princípio da boa ordem para verificar a existência dos números q e r. Sejam então $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Tome agora $S := \{a - bt| \quad t \in \mathbb{Z} \ \& \ 0 \leq a - bt\}$. Observe que $S \neq \emptyset$, pois para $t = 0$, temos que $a = a - b0 \geq 0$ e assim $a \in S$. Podemos então aplicar o princípio da boa ordem, 1.3.11 (xvi), e portanto existe $r \in S$ menor elemento, i.e., $\forall s \in S$, $r \leq s$. Como $r \in S$, existe

[1] *menor possível* neste caso significa que é menor positivo menor do que o divisor positivo.

$q \in \mathbb{Z}$ tal que $r = a - bq$, ou seja, $a = bq + r$. Como $r \geq 0$, falta agora verificar que $r < b$.
Elaboramos uma demonstração por absurdo, cf. [5], 1.4.2, e suponhamos que não é verdade que $r < b$, ou seja, $b \leq r$. Aí, temos que $0 \leq r - b$, e pela definição de r, temos que $0 \leq (a - bq) - b = a - (b+1)q$, mas assim $s := a - (b+1)q \in S$. Isto é um absurdo, pois do fato que $b > 0$, temos que $s < r$, contradizendo ao fato que r era menor elemento de S. Concluimos então que $r < b$, e acabamos de mostrar a afirmação do Lema. ∎

Observação 2.1.8. *Observe que a nossa demonstração feita acima, não dá muita idéia como obter os inteiros q e r. É possível exibir uma demonstração, qual chamamos de construtiva, e qual constrói de fato os inteiros q e r. Num curso de programação o estudante deve implementar um algoritmo para o computador calcular os números q e r. Este algoritmo se baséia na demonstração construtiva do último lema e usa basicamente subtração e a ordem $\leq$.*

O teorema principal vem agora, e após municiosa apuração da demonstração vejamos que o caso geral é deduzido do caso especial tratado em 2.1.7.

Teorema 2.1.9. *(Divisão com resto) Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que $a = qb + r$, onde $0 \leq r < |b|$.*

Demonstração: A demonstração deste teorema é dividida em duas partes. Como é preciso demonstrar que *existem* e são *únicos* os inteiros q e r, temos uma parte qual trata da existência e a segunda tratando da unicidade. Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$

I. Existência:
Vamos dividir a demonstração da existência em vários casos.
Caso 1: Seja $b > 0$.

Caso 1.1: Seja $a \geq 0$. Assim basta aplicar 2.1.7 e obtemos o desejado.

Caso 1.2: Seja $a < 0$. Assim $|a| > 0$ e pelo lema 2.1.7, existem $q', r' \in \mathbb{Z}$ tais que $|a| = q'b + r'$, onde $0 \leq r' < |b| = b$.
Em caso de $r' = 0$, temos que $-|a| = a = (-q')b$ e portanto $q := q'$ e $r = 0$ resolvem o teorema.
Em caso de $r' \neq 0$, temos que $-|a| = a = (-q')b - r' = (-q')b - b + b - r' = (-q' - 1)b + (b - r')$. Agora observe que como $0 < r' < b$, temos que $0 < b - r' < b$. Tomando $q := (-q' - 1)$ e $r := b - r'$, também resolvemos o teorema neste caso.

Caso 2: Seja $b < 0$. Assim observe que $|b| > 0$.
Usando o primeiro caso, podemos determinar inteiros q', r' tais que $a = |b|q' + r'$, onde $0 \leq r' < |b|$. Como $b < 0$, temos que $|b| = -b$ e assim, $\quad a = (-b)q' + r' = b(-q') + r'$, onde $0 \leq r' < |b|$. Logo $q := (-q')$ e $r := r'$, satisfazem o teorema.

II. Unicidade:
Supomos agora que os inteiros q, q', r, r' satisfazem o teorema, ou seja, $a = bq + r = bq' + r'$, onde $0 \leq r, r' < |b|$. Logo, tem,os que $b(q - q') = r' - r$, $(*)$. Sem perda da generalidade (s.p.d.g.), podemos supor $r' \geq r$ (Por quê?). Assim, temos que $0 \leq r' - r$. Como $r' < |b|$ temos agora que $0 \leq r' - r \leq r' < |b|$. Portanto, usando $(*)$, $0 \leq |b(q - q')| = |b||q - q'| < |b|$. Aplicando a lei do cancelamento para adição, observando que $b \neq 0$, temos que $0 \leq |q - q'| < 1$. Como q, q' são inteiros, temos usando 1.3.16, $|q - q'| = 0$, o que implica que $q = q'$. Daí, temos que $r = r'$, mostrando a unicidade dos inteiros q e r.

Com as partes I. e II., demonstramos o teorema. ∎

Definição 2.1.10. *Os números inteiros q e r obtidos no teorema 2.1.9 chamamos de* **quociente** *e* **resto** *da divisão de a por b, respectivamente.*

Observação 2.1.11. *(a) O último teorema é de uma importância grande para certos argumentos em teoria dos números, como veremos em seguida.*

(b) Vejamos que qualquer inteiro ímpar, i.e., da forma $2k+1$, para algum $k \in \mathbb{Z}$, sempre tem a forma $4k+1$ ou $4k+3$, para algum $k \in \mathbb{Z}$. Seja $m \in \mathbb{Z}$ um inteiro, então pelo teorema 2.1.9, m pode ter as formas, $4k$, $4k+1$, $4k+2$ ou $4k+3$ (pense e justifique isso para você!). Como m é ímpar, as possibilidades $4k$ e $4k+2$ não podem ocorrer, pois estes números são pares. Assim, somente restam as formas $4k+1$ ou $4k+3$. ∎

2.2 Numeração

Os números que usamos geralmente em matemática são escritos em base decimal. O computador em geral usa a base 2, e perguntamos nos se é possível escrever um número qualquer numa base arbitrária maior ou igual a 2 sempre? Se for possível queremos saber como converter os números de uma base para outra. Vejamos que existe um algoritmo simples para fazer isso. Na demonstração usamos o teorema da divisão com resto, 2.1.9.

Seja $a \in \mathbb{N}$ um número natural. Assim, sabemos que em base decimal, $a = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_1 10 + a_0$, onde $a_n \neq 0$, e $a_i \in \{0, 1, 2, \ldots, 9\}$ para todo $0 \leq i \leq n$. Escrevemos em geral, a como $a_n a_{n-1} \ldots a_1 a_0$.

Proposição 2.2.1. *Sejam $a > 0$ e $b \geq 2$ inteiros. Então a pode ser escrito de maneira única da forma $a = r_n b^n + r_{n-1}b^{n-1} + \ldots + r_1 b + r_0$, onde $n \geq 0$, $r_n \neq 0$ e $0 \leq r_i < b$, para $i \in \{0, 1, \ldots, n\}$.*

Demonstração: Também esta demonstração dividimos em duas partes. Sejam a e b interios como no enunciado.

I. Existência: Para mostrar a existência vamos aplicar o teorema 2.1.9. Dividimos a por b e obtemos únicos q_0 e r_0, tais que $a = q_0 b + r_0$, onde $0 \leq r_0 < b$. Caso, $q_0 = 0$, estamos prontos. Caso contrário, dividimos agora q_0 por b e novamente pelo teorema da divisão com resto, obtemos únicos q_1 e r_1 tais que $q_0 = q_1 b + r_1$, onde $0 \leq r_1 < b$. Novamente, se $q_1 \neq 0$ dividimos q_1 por b. Este processo da divisão continuamos até um $q_n = 0$. Observe (!) que como estamos dividindo a por $b \geq 2$, e depois cada quociente q_i está sendo dividido por b, em um número finito de passos $q_n = 0$.
Em particular, obtemos que

$a = q_0 b + r_0$, onde $0 \leq r_0 < b$,
$q_0 = q_1 b + r_1$, onde $0 \leq r_1 < b$,
$q_1 = q_2 b + r_2$, onde $0 \leq r_2 < b$,
$\vdots$
$q_{n-2} = q_{n-1} b + r_{n-1}$, onde $0 \leq r_{n-1} < b$,
$q_{n-1} = q_n b + r_n$, onde $0 \leq r_n < b$ e $q_n = 0$,

Agora substituindo as linhas sucessivamente, obtemos que
$a = q_0 b + r_0 = (q_1 b + r_1)b + r_0 = ((q_2 b + r_2)b + r_1)b + r_0 = q_2 b^2 + r_2 b^2 + r_1 b + r_0 = \ldots =$
$= r_n b^n + r_{n-1} b^{n-1} + \ldots + r_1 b + r_0$, o que era para demonstrar.

II. Unicidade: Para mostrar a unicidade, suponha que temos duas expressões satisfazendo o teorema, $a = r_n b^n + r_{n-1}b^{n-1} + \ldots + r_1 b + r_0$ e $a = r'_m b^m + r'_{m-1}b^{m-1} + \ldots + r'_1 b + r'_0$. Igualando as duas equações, obtemos o seguinte: $r_n b^n + r_{n-1}b^{n-1} + \ldots + r_1 b + r_0 = r'_m b^m + r'_{m-1}b^{m-1} + \ldots + r'_1 b + r'_0$, ou seja, $b(r_n b^{n-1} + r_{n-1}b^{n-2} + \ldots + r_1) + r_0 = b(r'_m b^{m-1} + r'_{m-1}b^{m-2} + \ldots + r'_1) + r'_0$. Pela unicidade do quociente e resto conforme 2.1.9, é preciso termos que $(r_n b^{n-1} + r_{n-1}b^{n-2} + \ldots + r_1) = (r'_m b^{m-1} + r'_{m-1}b^{m-2} + \ldots + r'_1)$ e $r_0 = r'_0$. O mesmo argumento usando a unicidade do teorema da divisão com resto, obtemos sucessivamente que $n = m$ e $r_i = r'_i$, para todos $i \in \{0, 1, \ldots n\}$, mostrando a unicidade da representação de um número numa base $b \geq 2$. ∎

Temos a seguinte

Notação 2.2.2. *Usamos $(r_n r_{n-1} \ldots r_1 r_0)_b$ para denotar um número na base b, se $b \neq 0$.*

Exemplo 2.2.3. *Vamos escrever* 855 *na base* 12*. Como somente temos dez dígitos na base usual decimal, é preciso introduzir dois novos dígitos, para* 10 *e* 11*. Tomemos* $\alpha := 10$ *e* $\beta := 11$*. Vamos executar as divisões adequadas e dadas pela demonstração da proposição 2.2.1 e obtemos que:*

$855 = 71 \cdot 12 + 3$,

$71 = 5 \cdot 12 + 11$,

$5 = 0 \cdot 12 + 5$.

Pela proposição última, obtemos que $855 = (5\beta 3)_{12}$.
Escreva 855 *em base* 2*. Na lista de exercícios temos mais exemplos para conversão de números.*

2.3 Ideais, mdc, mmc e o algoritmo de Euclides

Para poder justificar matematicamente de maneira correta o mdc como também o mmc vamos introduzir primeiramente o conceito de ideal no anel comutativo $\mathbb{Z}$, e demonstrar uma propriedade importante dos números inteiros, cf. 2.3.3.

Definição 2.3.1. *Seja* $I \subseteq \mathbb{Z}$*. Dizemos que* I *é* **ideal** *em* $\mathbb{Z}$ *sse* $I \neq \emptyset$ *e*
(i) $\forall a, b \in I, \quad (a+b) \in I$ *e* *(ii)* $\forall a \in I, \forall k \in \mathbb{Z}, \quad (ka) \in I$.

Exemplo 2.3.2. *(i) É fácil para demonstrar que* $\{0\}$ *e* $\mathbb{Z}$ *são ideais em* $\mathbb{Z}$*. Dizemos que estes dois ideais são os ideais triviais de* $\mathbb{Z}$*.*
(ii) Seja $P := \{m \in \mathbb{Z} | \quad m$ *é número par em* $\mathbb{Z}\}$*. Vejamos que* P *é ideal em* $\mathbb{Z}$*. Primeiramente, observe que* $P = \{m \in \mathbb{Z} | \quad \exists k \in \mathbb{Z},\ m = 2k\}$ *é não vazio, pois* $0 \in I$*. Resta verificar os ítens (i) e (ii) de 2.3.1. Para isso, sejam* $a, b \in I$*, i.e.,* $\exists k, m \in \mathbb{Z}$ *tais que* $a = 2k$ *e* $b = 2m$*. Assim,* $a + b = 2k + 2m = 2(k + m)$*, mostrando que* $(a + b) \in P$*. Se agora* $t \in \mathbb{Z}$*, então temos que* $ta = t(2k) = 2(ta)$*, o que é um número par, mostrando que* $(ta) \in P$*. Logo* P *é um ideal em* $\mathbb{Z}$*.*
(iii) Seja $I := \{m \in \mathbb{Z} | \quad m$ *é número ímpar em* $\mathbb{Z}\}$*. Sabemos que todo número ímpar tem a forma* $2k + 1$ *para algum* $k \in \mathbb{Z}$*. Perguntamos se* I *também é ideal em* $\mathbb{Z}$*? Se for ideal,* I *tem que satisfazer as condições da definição 2.3.1. Obviamente* $I \neq \emptyset$*. Assim, conseguindo refutar alguma condição de 2.3.1,* I *não é ideal. Sabemos que em geral não todo múltiplo de um número ímpar é novamente ímpar, por exemplo,* 3 *é ímpar e* $2 \cdot 3 = 6$ *porém é par. Consequentemente, a condição (ii) da definição 2.3.1 não vale, e assim* I *não pode ser ideal em* $\mathbb{Z}$*.*
(iv) Seja $m \in \mathbb{Z}$*. Verifique que* $(m) := \{km | \quad k \in \mathbb{Z}\}$ *é ideal em* $\mathbb{Z}$*.*

O próximo teorema é importante para os resultados a serem demonstrados em seguida, e caracteriza o anel $\mathbb{Z}$.

Teorema 2.3.3. *(*$\mathbb{Z}$ *é domínio de ideal principal) Seja* $I \subseteq \mathbb{Z}$ *um ideal. Então existe* $m \in \mathbb{Z}$ *tal que* $I = (m)$*, onde* $(m) := \{km | \quad k \in \mathbb{Z}\}$.

Demonstração: Seja $I \subseteq \mathbb{Z}$ ideal. Então, $I \neq \emptyset$. Em caso de $I = \{0\}$ é claro que $I = (0)$. Assim, podemos supor que $I \neq \{0\}$. Logo, existe $a \in \mathbb{Z}$ tal que $a \neq 0$ e $a \in I$. Como I é ideal, sabemos que $-a = (-1)a \in I$. Portanto, é claro que o conjunto $I^+ := \{b \in I | \quad b > 0\}$ é conjunto não vazio com elementos positivos. Podemos então aplicar o princípio da boa ordem, 1.3.11 (xvi), e existe portanto $m \in I^+$ o menor elemento. Vamos mostrar o seguinte

Fato: $I = (m)$.
Prova do fato: É preciso verificar as duas inclusões $\subseteq$ e $\supseteq$. Observe que como $m \in I$, temos pela definição 2.3.1 que $km \in I$, para qualquer $k \in \mathbb{Z}$, mostrando assim facilmente que $(m) \subseteq I$. Resta mostrar a outra inclusão. Para isso, seja $t \in I$. Como t é inteiro e m não é 0, podemos aplicar a divisão com resto, cf. 2.1.9, e obtemos únicos $q, r \in \mathbb{Z}$ tais que $t = qm + r$, onde $0 \leq r < m$. Supondo $r \neq 0$, obtemos que $r = t - qm$ e $t - qm < m$. Mas pelas condições de I ser ideal, temos que $r \in I$, sendo $t \in I$ e $qm \in I$ e assim,

$(t - qm) \in I$. Mas, isso é absurdo, pois $m \in I$ era menor elemento positivo em I^+. Logo, a suposição que $r \neq 0$ era falsa, e assim $r = 0$. Portanto, $t = qm$, e assim, $t \in (m)$.
Concluimos que $I = (m)$. ∎

Em seguida, introduzimos a definição do maior ou máximo divisor em comum (mdc) de dois inteiros, e demonstramos algumas propriedades do mdc de dois inteiros. Somente depois vejamos que sempre existe o mdc e como podemos calcular o mdc usando o algoritmo de Euclides, além da relação entre minimo múltiplo em comum e maior divisor em comum.

Definição 2.3.4. *Sejam $a, b \in \mathbb{Z}$ doi inteiros não nulos e seja c outro inteiro.*
(a) Dizemos que c é **divisor em comum** *de a e b, sse $c|a$ e $c|b$. Denotamos por $D(a;b) := \{t \in \mathbb{Z} | \quad t|a \ \& \ t|b\}$ o conjunto de todos os divisores em comum de a e b.*
(b) Dizemos que c é **máximo divisor em comum** *de a e b, $mdc(a;b)$, sse c é o maior de seus divisores em comum, ou seja, $c = maxD(a;b)$. Denotamo-lo por $mdc(a;b)$.*

O próximo teorema é importante.

Teorema 2.3.5. *(Bézout) Sejam $a, b \in \mathbb{Z}$ inteiros não nulos e $d := mdc(a;b)$. Então, existem inteiros $r, s \in \mathbb{Z}$ tais que $d = ar + bs$. Dizemos que as constantes r e s são as constantes de Bézout.*

Demonstração: O último teorema 2.3.3 está sendo usado para a demonstração qual corre basicamente em duas partes. Seja $I := \{ax + by| \quad x, y \in \mathbb{Z}\}$ para a e b não nulos inteiros.

Fato 1: I é ideal em $\mathbb{Z}$.
A prova deste fato está sendo deixado como exercício. Observe que é preciso verificar as propriedades da definição 2.3.1.

Pelo Fato 1 e pelo teorema 2.3.3, existe $m \in \mathbb{Z}^+$ tal que $I = (m)$.

Fato 2: $m = d$.
Prova: Vejamos que m é o mdc de a e b. Inicialmente, observe que como $a = 1 \cdot a + 0 \cdot b$, temos que $a \in I = (m)$. Assim, existe $k \in \mathbb{Z}$ tal que $a = km$, ou seja, $m|a$. Analogamente podemos demonstrar que $m|b$, ou seja, m é divisor em comum de a e b. Falta demonstrar que m é máximo divisor em comum de a e b. Observe que de $(m) = I$, existem constantes digamos r e s tais que $m = ar + bs$. Seja agora $m' \in D(a;b)$, então, $m'|a$ e $m'|b$. Pela proposição 2.1.5 (d), $m'|(ar + bs)$, ou seja, $m'|m$. Pela observação 2.1.3, temos que $|m'| \leq |m| = m$. Logo, m é maior elemento de $D(a;b)$, ou seja, $m = mdc(a;b)$.

Pelos Fatos 1 e 2, temos que existem $r, s \in \mathbb{Z}$ tais que $d = ar + bs$, e o teorema de Bézout está demonstrado. ∎

Até agora, sabemos somente uma propriedade interessante do máximo divisor em comum, mas nada sobre a sua existência ou seu cálculo. Vejamos antes destas questões ainda mais algumas propriedades do mdc de dois inteiros.

Proposição 2.3.6. *Sejam a e b dois inteiros não nulos e $d > 0$ outro inteiro. São equivalentes:*
(a) $d = mdc(a;b)$, e
(b) d satisfaz
(i) $d|a$ e $d|b$, e
(ii) para qualquer $d' \in \mathbb{Z}$, $d'|a$ e $d'|b \quad \Rightarrow \quad d'|d$.

Demonstração: Observe que é preciso demonstrar $\Rightarrow$ e $\Leftarrow$. Vejamos $\Rightarrow$. Para isso, seja $d = mdc(a;b)$. Assim é claro pela definição 2.3.4 que vale o ítem (i). Seja a gora $d' \in \mathbb{Z}$ tal que $d'|a$ e $d'|b$. Sabendo que d é mdc de a e b, existem pelo teorema de Bézout as constantes $r, s \in \mathbb{Z}$ tais que $d = ar + bs$ e por 2.1.5, $d'|d$, terminando a prova do ítem (b).
Vejamos então $\Leftarrow$. Seja $d > 0$ satisfazendo o ítem (b). Mostramos que d é o máximo divisor em comum de

a e b. É claro que $d \in D(a;b)$. Falta então ver que d é elemento maior de $D(a;b)$. Mas seja $d' \in D(a;b)$, então por (ii), temos que $d'|d$. Usando a observação 2.1.3, temos que $d' \leq |d| = d$, justificando que $d = maxD(a;b)$. ∎

Observe que em alguns livros as condições (i) e (ii) da última proposição estão sendo usadas para *definir* o mdc de dois inteiros. Pensando um pouco acerca da proposição 2.3.6, vejamos que de fato é possível definir o mdc de duas maneiras, ou via (a) ou via (b) de 2.3.6.

Proposição 2.3.7. *Sejam a, b e c inteiros não nulos e $d = mdc(a;b)$. Então, $mdc(ac;bc) = |c|mdc(a;b)$.*

Demonstração: Sejam $a, b, c \in \mathbb{Z}$ inteiros não nulos e seja $d := mdc(a;b)$. Vamos mostrar que $d|c|$ satisfaz as propriedades de 2.3.6, (b). Observe que é imediato que $(d|c|)|ac$ e $(d|c|)|bc$. Pelo Teorema de Bézout, existem $r, s \in \mathbb{Z}$ tais que $d = ar + bs$. Assim, $d|c| = ar|c| + bs|c|$. Seja d' inteiro tal que $d'|(ac)$ e $d'|(bc)$, temos que d' também divide qualquer combinação linear de ac e bc, por 2.1.5, (d), ou seja, $d'|(d|c|)$, acabando a prova da proposição. ∎

A seguinte propriedade da divisibilidade pode ser usado em muitas ocasiões.

Teorema 2.3.8. *(Euclides) Sejam a, b e c inteiros não nulos satisfazendo $a|(bc)$. Se $mdc(a;b) = 1$, então, $a|c$.*

Demonstração: Sejam $a, b, c \in \mathbb{Z} \setminus \{0\}$ tais que $a|(bc)$. Como $mdc(a;b) = 1$, temos por último teorema 2.3.7 que $mdc(ac;bc) = |c|$. Mas, como obviamente, $a|(ac)$ e por hipótese, $a|(bc)$, temos que $a|(mdc(ac;bc))$, ou seja, $a|(|c|)$. Logo, $a|c$. ∎

Observação 2.3.9. *(a) Em exercícios da lista, vamos mostrar que $6|(n(n+1)(2n+1))$. Para mostrar isso, podemos fazer uso do teorema de Euclides 2.3.8, e assim basta mostrarmos que $2|(n(n+1)(2n+1))$ e $3|(n(n+1)(2n+1))$. (Por quê?).*
(b) Às vezes, dizemos em caso de $mdc(a;b) = 1$ para inteiros, que a e b são **relativamente primos**. ∎

Em seguida, queremos calcular efetivamente o máximo divisor em comum de dois inteiros não nulos. Vejamos que existe de fato um *algoritmo* para o cálculo do mdc. Começamos com o seguinte

Lema 2.3.10. *Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$ e $q, r \in \mathbb{Z}$ satisfazendo $a = bq + r$, onde $0 \leq r < |b|$.*
Então, $D(a;b) = D(b;r)$ e assim $mdc(a;b) = mdc(b;r)$.

Demonstração: Sejam os números inteiros dados conforme a hipótese, i.e., $a = bq + r$, onde $0 \leq r < |b|$. Vejamos as duas inclusões. Para isso, seja $t \in D(a;b)$. Então, $t|a$ e $t|b$. Por 2.1.5, (d), $t|(a - bq)$, ou seja, $t|r$. Logo, $t \in D(b;r)$. Por outro lado, sendo $t \in D(b;r)$, temos que $t|b$ e $t|r$. Assim, $t|(bq + r)$ (cf. 2.1.5, (d)). Logo, $t \in D(a;b)$. ∎

O último lema, dá a base do algoritmo de Euclides para o cálculo do mdc de dois números inteiros. Temos a

Observação 2.3.11. *(Algoritmo de Euclides) Queremos calcular eficientemente o $mdc(a;b)$, para a e b inteiros não nulos. Dividimos a por b e obtemos $a = bq_1 + r_1$, com $0 \leq r_1 < |b|$.*
Caso $r_1 = 0$, temos que $a = bq_1$, ou seja, $b|a$. Logo, $mdc(a;b) = |b|$.
Em caso de $r_1 \neq 0$ temos pelo último lema, 2.3.10, $mdc(a;b) = mdc(b;r_1)$. Assim, é preciso calcular $mdc(b;r_1)$. Novamente dividimos, mas agora b por r_1, e obtemos pela divisão com resto que $b = r_1q_2 + r_2$, onde $0 \leq r_2 < r_1$.
Caso $r_2 = 0$, temos que $b = r_1q_2$, ou seja, $r_1|b$. Logo, $mdc(b;r_1) = r_1$. E assim, $mdc(a;b) = r_1$.
Em caso de $r_1 \neq 0$ temos pelo último lema, 2.3.10, $mdc(b;r_1) = mdc(r_1;r_2)$. Assim, é preciso calcular $mdc(r_1;r_2)$. Entramos assim novamente em nosso algoritmo. Observe que os restos r_i estão diminuindo mesmo, i.e., $|b| > r_1 > r_2 > r_3 > \ldots$. $(*)$.

Obtemos então a sguinte cadeia:

(i) $a = bq_1 + r_1$, *com* $0 \leq r_1 < |b|$.

(ii) $b = r_1q_2 + r_2$, *com* $0 \leq r_2 < r_1$.

(iii) $r_1 = r_2q_3 + r_3$, *com* $0 \leq r_3 < r_2$.

$\vdots$

$r_{n-1} = r_nq_{n+1} + r_{n+1}$, *com* $r_{n+1} = 0$.

Observe que a cadeia $(*)$, *de fato chega a um resto* $r_{n+1} = 0$. *Usando sucessivmente o lema 2.3.10, obtemos que* $mdc(a; b) = mdc(b; r_1) = \ldots = mdc(r_{n-1}; r_n) = r_n$.

O método explicado acima é de fato um algoritmo e pode ser implementado usando uma linguagem computacional num programa de computação. Além disso, este método fornece - fazendo substituções seguidas - também uma possibilidade de obter as constantes de Bézout para os inteiros a *e* b. *Vejamos isto agora:*

Da equação (i), obtemos que $r_1 = a - bq_1$, *e substituindo isto na equação (ii) temos que* $b = (a - bq_1)q_2 + r_2$, *ou seja,* $r_2 = (-q_2)a + (1 + q_1q_2)b$. *Continuando estas substituições, podemos escrever* $r_n = ar + bs$, *com* r *e* s *adequadas. Faça os detalhes como exercício.* ∎

Vejamos agora um exemplo de cálculo de mdc.

Exemplo 2.3.12. *Queremos calcular, via algoritmo de Euclides, o mdc dos números* 1.128 *e* 336 *e determinar as constantes de Bézout. Elaboramos o algoritmo e obtemos a seguinte tabela:*

	3	2	1	4
1.128	336	120	96	24
120	96	24	0	

Ou seja, temos as seguintes equações:

(i) $1.128 = 3 \cdot 336 + 120$ *(ii)* $336 = 2 \cdot 120 + 96$ *(iii)* $120 = 1 \cdot 96 + 24$ *e* *(iv)* $96 = 4 \cdot 24$.

Logo, $mdc(1.128; 336) = 24$. *Para calcular as constantes de Bézout, substituimos as equações sucessivamente e obtemos que*

$24 = 120 - 96 = (1.128 - 3 \cdot 336) - 96 = (1.128 - 3 \cdot 336) - (336 - 2 \cdot 120) = (1.128 - 3 \cdot 336) - (336 - 2 \cdot (1.128 - 3 \cdot 336)) = 3 \cdot 1.128 + (-10) \cdot 336$. ∎

Falta agora só a introdução do mínimo múltiplo em comum (mmc) de dois inteiros não nulos. Vejamos que a teoria sobre o mdc basta para podermos calcular o mmc de dois inteiros.

Definição 2.3.13. *Sejam* a *e* b *inteiros não nulos e* $m > 0$ *outro inteiro. Dizemos que* m *é* **mínimo múltiplo em comum** *de* a *e* b, $mmc(a; b)$ *sse*

(i) $a|m$ *e* $b|m$, *e*

(ii) para qualquer m' *tal que* $a|m'$ *e* $b|m'$, *temos que* $m|m'$.

Observação 2.3.14. *Compare a caracterização do mdc dado em 2.3.6 com a nossa definição. Mais tarde, no capítulo da teoria de ordem, cf. 3 fica claro que o mínimo múltiplo em comum é conceito* dual *do máximo divisor em comum.* ∎

Temos a seguinte proposição importante, qual garante que o mmc de dois números é obtido através do mdc. Relembrando que existe um algoritmo para o cálculo do mdc de dois inteiros, o mmc vem, digamos *de graça* junto com o mdc.

Proposição 2.3.15. *Sejam* $a, b \in \mathbb{Z} \setminus \{0\}$, $d := mdc(a; b)$ *e* $m := mmc(a; b)$. *Então,* $md = |ab|$.

Demonstração: Sem perda da generalidade, sejam a e b positivos. Tomemos $t \in \mathbb{Z}^+$ tal que $td = ab$. Observe que é preciso demonstrar que $t = mmc(a; b)$. Para isso, verifiquemos a definição 2.3.13.
Como $d = mdc(a; b)$, existem $a_1, b_1 \in \mathbb{Z}^+$ tais que $a = a_1 d$ e $b = b_1 d$. $(*)$.
Logo (verifique isso!), $mdc(a_1; b_1) = 1$. De $(*)$, obtemos que $t = a_1 b = ab_1$. Assim, $a|t$ e $b|t$, mostrando (i) de 2.3.13.
Seja agora $m' \in \mathbb{Z}$ tal que $a|m'$ e $b|m'$. Então, existe $q \in \mathbb{Z}$ tal que $m' = aq = a_1 dq$. Também, como $b|m'$, temos que $b|(a_1 dq)$, ou seja de $(*)$, $b_1 d|(a_1 dq)$. Pelo cancelamento, temos que $b_1|(a_1 q)$ e usando o teorema de Euclides 2.3.8, obtemos de $mdc(a_1; b_1) = 1$ que $b_1|q$. Portanto, existe $e \in \mathbb{Z}$ tal que $q = eb_1$. Substituindo isso em m', obtemos que $m' = a_1 deb_1$, o que mostra que $m' = a_1 be = te$, i.e., $t|m'$, o que era para mostrar no ítem (ii) de 2.3.13. ∎

2.4 Números primos e o teorema fundamental da aritmética

Nesta seção introduzimos os números primos e estabelecemos o teorema principal para primos, o teorema fundamental, cf. 2.4.4. Números primos são de importância para a ciência da computação. Até então, a criptografia **RSA**, veja o apendix e [13], funciona ainda com o uso de números primos, e é dada pelo produto de dois primos grandes. Na prática é difícil, também para um computador decidir se certo número é de fato primo e se não for primo descobrir a sua fatoração em produto de primos. Isso está sendo usado em **RSA**. Mas começamos com definição e proposições básicas. O leitor interresado em números primos pode consultar a página http://primes.utm.edu, onde problemas, pesquisas atuais e primos recordes são apresentados.

Definição 2.4.1. *Seja $p > 1$ um inteiro. Dizemos que p é* **número primo** *sse os únicos divisores positivos de p são 1 e p.*

Proposição 2.4.2. *Existe um número infinito de primos.*

Demonstração: A demonstração desta proposição está proposta em exercícios. A ideia (da prova por Euclides) é a seguinte : Vamos supor (por absurdo) que existe um número finito de primos, então sejam $p_1, \ldots, p_n$ estes primos. Consideremos agora o número $(p_1 \cdot \ldots \cdot p_n) + 1$, então é claro que nenhum p_i divide este número. Com isso é fácil derivar uma contradição à hipótese de existirem finitos primos. ∎

Proposição 2.4.3. *Seja $m > 1$ um inteiro. Então, m pode ser escrito como produto de números primos.*

Demonstração: Vamos elaborar uma prova por indução em m. Usamos a segunda forma de indução, cf. 1.2.2. O início da indução é imediato, pois aí, $m = 2$ é número primo, e assim é produto com um fator. Para o passo da indução seja a proposição válida para todo $2 \leq k \leq m$, e consideremos o número $m + 1$. Caso, $m + 1$ for primo, estamos prontos. Caso contrário, $m + 1 = ts$, onde $2 \leq t, s < m + 1$. Pela hipótese da indução t como também s são produtos de primos, e consequentemente, $m + 1$ como produto ts é produto de números primos.

Agora estamos em condições de formular e mostrar o

Teorema 2.4.4. *(Teorema Fundamental da Aritmética) Seja $m > 1$ um inteiro. Então, m pode ser escrito de maneira única como produto de números primos, i.e., existem únicos primos (não necessariamente distintos) $p_1 \leq p_2 \leq \ldots \leq p_k$ tais que $m = p_1 \cdot \ldots \cdot p_k$.*

Demonstração: Seja $m > 1$ um inteiro. A demonstração tem duas partes: existência e unicidade. Pela proposição anterior, a parte da existência está demonstrada. Falta verificar a unicidade dos primos no produto. Para isso, sejam $p_1 \leq p_2 \leq \ldots \leq p_k$ e $q_1 \leq q_2 \leq \ldots \leq q_l$ primos para duas fatorações de m, i.e., $m = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$. Vejamos que $k = l$ e para cada p_i existe j_i tal que $p_i = q_{j_i}$. Observe só

que como $p_1|m$, temos que $p_1|(q_1 \cdot \ldots \cdot q_l)$. Agora, relembrando que os p_i's como os q_j's são todos primos, temos que existe j tal que $p_1|q_j$, e sendo q_j primo, temos que $p_1 = q_j$. Continuando assim obtemos que $k = l$ e $p_i = q_{j_i}$ para todo i. Os detalhes são deixados como exercício. ∎

A próxima proposição justifica o *crivo de Eratóstenes*, qual dá um método de descobrir os números primos até um certo número dado.

Proposição 2.4.5. *Seja $m > 1$ um inteiro não primo. Então, existe um número primo p tal que $p|m$ e $p \leq +\sqrt{m}$.*

Demonstração: Seja $m > 1$ inteiro não primo, então existem inteiros a, b tais que $2 \leq a \leq b < m$ e $m = ab$. Portanto temos que $m = ab \geq a^2$, ou seja $a \leq +\sqrt{m}$. Pelo teorema fundamental da aritmética 2.4.4, existe número primo p tal que $p|a$. Assim, temos que $p|m$ e $p \leq +\sqrt{m}$. ∎

Exemplo 2.4.6. *(i) Queremos saber se 271 é primo ou não. Usando a proposição anterior, observe que se 271 fosse não primo, então, teríamos um divisor primo menor do que $\sqrt{271}$, ou seja, um divisor primo menor do que 16. Sabemos que os primos menores do que 16 são $2, 3, 5, 7, 11$ e 13. Agora, testamos todos estes primos e observemos que nenhum deles divide 271. Podemos concluir que 271 é número primo.*
(ii) O número 100 não é primo, pois temos um divisor 2 menor do que $\sqrt{100} = 10$.

Observação 2.4.7. *(O crivo de Eratóstenes) A última proposição justifica o* crivo de Eratóstenes *qual explicamos em seguida. Seja dado um número natural n, queremos saber quais são os primos menores ou igual a este número n. Fazemos o seguinte processo:*
(a) Vamos escrever todos os números entre 2 e n numa lista.
(b) Calculamos os primos p tais que $p \leq \sqrt{n}$.
(c) Deletamos na lista acima todos os múltiplos kp, para $k \geq 2$, destes primos calculados.
(d) Os números quais não foram deletas na lista são todos os primos menores ou igual a n.
Por quê? Pense acerca da última afirmação (d), e tente justificá-la.

Existem vários problemas (difíceis) envolvendo números primos. Vejamos alguns na seguinte

Observação 2.4.8. *(a) (A conjectura de Goldbach, 1742): Todo número par maior do que 2 pode ser escrito como soma de dois primos.*
Esta conjectura foi feita pelo matemático C.Goldbach em 1742 e comunicado para L.Euler na época.
Acontece que esta conjectura não foi demonstrado até hoje (maio de 2016) , mas existem indicações fortes que a conjectura é verdadeira e se o número par é grande que temos muitas *somas de dois primos para ele.*
(b) Números primos gemêos*: Dizemos que os números p e $p + 2$ são* números primos gemêos*, sse p e $p + 2$ são primos. Por exemplo, o par $(3; 5)$ é um par de números primos gemêos, também $(11; 13)$ ou $(1000000007; 1000000009)$. O maior par de gemêos descoberto até hoje (maio de 2016) é*

$$(242.206.083 \cdot 2^{38.880} - 1; 242.206.083 \cdot 2^{38.880} + 1).$$

A pergunta que se faz é quantos pares primos gemêos existem? Um número finito ou infinito?
(c) Seja p um primo. Sabe se que para o número $2^k - 1$ ser primo, é preciso que k é um número primo. Mas, o que não sabemos até hoje para quais primos p, $2^p - 1$ é número primo. Números primos da forma $2^p - 1$ chamam se números de Mersenne*.*
(d) Um problema conhecido da teoria dos números - embora não especificamente envolvendo números primos - e não solucionado até 1996, é o último teorema de Fermat*. Em 1996, o matemático A.Wiles[2] conseguiu demonstrar este teorema:*
Sejam x, y e z inteiros positivos. Então a equação $x^n + y^n = z^n$ não possui solução para todo $n \geq 3$.
Sabemos por exemplo, que $3^2 + 4^2 = 5^2$, e assim a equação acima tem solução para $n = 2$. ∎

[2]Um livro interessante sobre o trabalho de Wiles e o teorema de Fermat, escrito também para pessoas com pouco conhecimento de matemática é [17].

2.5 Equações Diofantinas lineares

Começamos esta seção com o problema de solucionar uma equação Diofantina linear. Consideremos para $a, b, c \in \mathbb{Z}$:

$$ax + by = c. \qquad (*)$$

Perguntamos se esta equação é solucionável por valores *inteiros*. Observe que $(*)$ com certeza tem solução nos reais, $\mathbb{R}$, pois vejamos que $(*)$ trata de uma equação linear. A questão se existem soluções inteiras não é tal trivial. Temos o seguinte

Exemplo 2.5.1. *Numa loja, um certo líquido está sendo vendido em recipientes de* 7 *litros e* 15 *litros. Queremos comprar* 125 *litros deste líquido. Sabendo que o vendedor não pode abrir estes recipientes, queremos saber se é possível comprar* 125 *litros deste líquido. A solução está sendo dada por uma equação Diofantina:*

$$15x + 7y = 125.$$

Observação 2.5.2. *Às vezes é fácil saber se uma certa equação tem soluções inteiras. Consideremos a seguinte equação* $4x+6y = 13$*. Observe que o lado esquerdo da equação tem um valor par, pois* $4x+6y = 2(2x + 3y)$*. O lado direito porém tem o valor* 13*, ímpar. Obviamente esta equação não pode ter solução inteira, pois um número par não pode ser ímpar ao mesmo tempo.* ∎

Vejamos agora um critério simples de saber quando existe solução inteira. Em seguinda somente escrevemos que uma equação tem solução, em vez de *solução inteira*.

Lema 2.5.3. *(Existência de solução) Sejam* $a, b, c \in \mathbb{Z}$ *inteiros não nulos e* $d := mdc(a; b)$*. Então,*

A equação $(*)$ *tem solução (inteira)* sse $d|c$.

Demonstração: Sejam a, b, c inteiros e $d := mdc(a; b)$. Considere o ideal $I := \{ax + by| \quad x, y \in \mathbb{Z}\}$. Sabemos por 2.3.5 que I é de fato um ideal e $I = (d)$. Assim, temos que
$(x; y)$ é um par de solução para $(*)$ sse $ax + by = c$ sse $c \in I$ sse $d|c$. ∎

Com este lema 2.5.3, sabemos que o exemplo 2.5.1, tem solução, pois $mdc(15; 7) = 1$ e $1|125$. Falta saber como podemos calcular as soluções. Nas soluções reaparecem as constantes de Bézout. Temos o seguinte

Teorema 2.5.4. *(Solução de equação Diofantina) Sejam* a, b, c *inteiros e* $d := mdc(a; b)$ *tais que* $d|c$*, i.e.,* $c = kd$*. Escrevendo* d *da forma 2.3.5,* $d = ar + bs$ *para alguns* $r, s \in \mathbb{Z}$*, temos que*
(i) o par $(x_0; y_0)$*, onde* $x_0 := rk$ *e* $y_0 = sk$*, onde* $k = \frac{c}{d}$*, é um par de solução para* $(*)$*.*
(ii) o par $(x; y)$ *é uma solução para* $(*)$ sse $x = x_0 + \frac{b}{d}t$ *e* $y = y_0 - \frac{a}{d}t$*, para todo* $t \in \mathbb{Z}$*.*

Demonstração: Sejam a, b, c inteiros e $d := mdc(a; b)$ tais que $d|c$, i.e., $c = kd$, e $d = ar + bs$ para alguns $r, s \in \mathbb{Z}$. Assim, observe que multiplicando a última equação por k, obtemos que $c = kd = (ar + bs)k = a(rk) + b(sk)$, mostrando o ítem (i) do teorema.
Para justificar o ítem (ii), vejamos primeiramente que um par $(x; y)$ como dado acima, i.e., $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$, para qualquer $t \in \mathbb{Z}$, é de fato uma solução de $(*)$. Substituimos simplesmente os valores de x e y em $(*)$ e obtemos que
$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + a\frac{b}{d}t + by_0 - b\frac{a}{d}t = c + \frac{ab}{d}t - \frac{ab}{d}t = c.$
Por outro lado, é preciso demonstrar que qualquer solução de $(*)$ tem a forma dada pelo par $(x; y)$ acima. Seja então $(x'; y')$ um par de solução para $(*)$, i.e., $c = ax' + by'$. Sabendo por (i) que $(x_0; y_0)$ é solução particular, temos que $ax' + by' = c = ax_0 + by_0$. Assim, temos que $a(x' - x_0) = b(y_0 - y') \quad (**)$.
Como $d = mdc(a; b) \neq 0$, temos que $a = da_1$ e $b = db_1$, com $mdc(a_1; b_1) = 1$. Logo, podemos cancelar d

na equação $(**)$, e obtemos que $a_1(x' - x_0) = b_1(y_0 - y')$. $(***)$
Portanto, $b_1|(a_1(x' - x_0))$ e sabendo que $mdc(a_1; b_1) = 1$, é claro pelo teorema de Euclides 2.3.8 que $b_1|(x' - x_0)$, ou seja, existe $t \in \mathbb{Z}$ tal que $x' - x_0 = b_1 t$. Logo, $x' = x_0 + b_1 t = x_0 + \frac{b}{d}t$.
Substituindo $x' - x_0 = b_1 t$ em $(***)$, obtemos que $a_1 b_1 t = b_1(y_0 - y')$. Usando o fato de que $b_1 \neq 0$ podemos novamente cancelar b_1 e obtemos que $a_1 t = y_0 - y'$, ou seja, $y' = y_0 - a_1 t = y_0 - \frac{a}{d}t$, o que era para demonstrar, terminando a prova do ítem (ii). ∎

Exemplo 2.5.5. *Revejamos agora o exemplo 2.5.1. Já sabemos que o problema tem solução inteira. Agora queremos determinar todas as soluções, lembrando que neste caso somente interessam soluções positivas ! Como* $mdc(15; 7) = 1$*, é preciso determinar constantes de Bézout. Pela seção 2.3, sabemos que existe um algoritmo pra determinar as constantes. Em nosso caso porém, podemos achar um par de constantes de Bézout por tentativa. Observe que* $15 \cdot 1 + 7(-2) = 1$*, ou seja,* $r = 1$ *e* $s = -2$ *servem para as constantes de Bézout. Pelo último teorema 2.5.4,* $x_0 = 125$ *e* $y_0 = -250$ *são soluções particulares de* $15x + 7y = 125$*. As soluções gerais são dadas por* $x = 125 + 7t$ *e* $y = -250 - 15t$*. Agora porém, como se trata de saber se é possível a compra deste líquido, somente interessam as soluções não negativas. Assim, é preciso saber se existem soluções* $x \geq 0$ *e* $y \geq 0$*, ou seja,*
$125 + 7t \geq 0$ *e* $-250 - 15t \geq 0$*, i.e.,* $t \geq -17\frac{6}{7}$ *e* $t \leq -16\frac{10}{15}$.
Logo, é preciso que $t \in \mathbb{Z}$ *é tal que* $t = -17$*. Usando este valor para* t*, temos a única solução inteira não negativa dada por* $x = 125 + 7 \cdot (-17) = 6$ *e* $y = -250 - 15 \cdot (-17) = 5$.

2.6 Congruências

Vamos em seguida falar sobre um conceito importante na matemática e computação, a *congruência* entre números inteiros.

Definição 2.6.1. *Sejam* $m \geq 2$ *um inteiro e* $a, b \in \mathbb{Z}$*. Dizemos que* a *e* b *são* **congruentes módulo** m*,* $a \equiv_m b$*,* $a \equiv b$ *mod* m*, sse,* $m|(a - b)$.

Observação 2.6.2. *(i) Observe que* $3 \equiv 7$ *mod* 4*, pois* $4|(3 - 7)$*. Também* $-3 \equiv 5$ *mod* 4*, pois* $4|(-3 - 5)$*.*
(ii) A relação $\equiv_m$ *é de fato uma relação de equivalência em* $\mathbb{Z}$*.*
(iii) São equivalentes:
(a) $a \equiv_m b$ *e (b)* a *e* b *têm o mesmo resto após a divisão por* m*.*

Demonstração: O ítem (ii) não é difícil de mostrar. Observe que $a \equiv_m a$, pois para qualquer $m \geq 2$, $m|(a - a)$. Sejam agora $a, b \in \mathbb{Z}$ tais que $a \equiv_m b$, i.e., $m|(a - b)$. Assim, é imediato que $m|((-1)(a - b))$, ou seja $m|(b - a)$. Logo, $b \equiv_m a$. Portanto, mostramos que $\equiv_m$ é relação reflexiva e simétrica. O caso da transitividade deixamos como exercício.
Vejamos então (iii). Pelo teorema da divisão com resto, 2.1.9, sabemos que existem quocientes q_1, q_2 e restos r_1, r_2 únicos tais que
$a = q_1 m + r_1$, onde $0 \leq r_1 < m$, e $b = q_2 m + r_2$, onde $0 \leq r_2 < m$.
Assim, temos que $a - b = m(q_1 - q_2) + (r_1 - r_2)$, com $0 \leq r_1, r_2 < m$. Logo, sabemos que
$m|(a - b)$ sse $m|(r_1 - r_2)$ e como $0 \leq r_1, r_2 < m$, isto é equivalente a $r_1 = r_2$, ou seja,
$a \equiv_m b$ sse $r_1 = r_2$, o que era para mostrar. ∎

Sabemos que qualquer relação de equivalência dá origem a um conjunto quociente, como também a uma partição cf. [5], seção 4. Reunimos algumas propriedades na próxima

Observação 2.6.3. *Seja* $m \geq 2$*. Em observação, 2.6.2, demonstramos que* $\equiv_m$ *é uma relação de equivalência em* $\mathbb{Z}$*. Assim, temos o conjunto quociente* $\mathbb{Z}/\equiv_m := \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$*. Este conjunto quociente contém* m *elementos, a saber,* $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$*. Observe que cada classe de equivalência contém elementos quais têm o mesmo resto após a divisão por* m*. (Pense sobre isso, e observe que a observação,*

2.6.2, (iii) justifica esta afirmação). Assim, é claro que as classes de equivalência são 2 a 2 disjuntos. (Observe que o resto sempre é unicamente determinado!).
Além disso, sabemos de [5], seção 4, que $\mathbb{Z}_m$ forma uma partição para $\mathbb{Z}$, ou seja, $\bigcup \mathbb{Z}_m = \mathbb{Z}$[3] . ∎

A próxima proposição dá propriedades importantes ao conjunto $\mathbb{Z}_m$. Estas propriedades formam de $\mathbb{Z}_m$ um anel comutativo com unidade, também conhecido como *anel quociente*.

Proposição 2.6.4. *Seajm $m \geq 2$, $a, b, c, d \in \mathbb{Z}$. Então,*
(i) Se $a \equiv_m b$ e $c \equiv_m d$, então, $(a + b) \equiv_m (c + d)$ e $(ab) \equiv_m (cd)$.
(ii) Se $a \equiv_m b$, então, $(a + c) \equiv_m (b + c)$.
(iii) Se $a \equiv_m b$, então, para todo $n \in \mathbb{N}$, $a^n \equiv_m b^n$.

Demonstração: Sejam $m \geq 2$, $a, b, c, d \in \mathbb{Z}$. Vejamos o ítem (i). Para isso, sejam $a \equiv_m b$ e $c \equiv_m d$, i.e., $m|(a - b)$ e $m|(c - d)$. Pela proposição 2.1.5 (d), $m|((a - b) + (c - d))$. Logo, temos que $m|((a + c) - (b + d))$, ou seja, $(a + c) \equiv_m (b + d)$, mostrando a primeira parte de (i). Para ver o resto, observe que de $m|(a - b)$ e $m|(c - d)$, temos que $m|(c(a - b))$ e $m|(b(c - d))$. Também por 2.1.5 (d), obtemos que $m|((ac - bc) + (bc - bd))$, ou seja, $m|(ac - bd)$, o que implica que $ac \equiv_m bd$.
O ítem (ii) deixamos como exercício. O ítem (iii), segue de uma simples indução em n. O início da indução é imediato, pois $a^0 = b^0$. Para o passo de indução é preciso usar a hipótese da indução, $a^n \equiv_m b^n$ e a hipótese da afirmação. Observe que $a^{n+1} = a \cdot (a^n)$. Agora, como $a \equiv_m b$, podemos usar o ítem (i), e obtemos da hipótese da indução que $a^{n+1} \equiv_m b^{n+1}$. ∎

A próxima observação é uma observação matemática.

Observação 2.6.5. *Sabemos que a estrutura algébrica $(\mathbb{Z}; +, \cdot, 0, 1)$ tem estrutura de anel comutativo com unidade. O conjunto quociente construido acima $\mathbb{Z}_m$, também tem a estrutura de anel comutativo com unidade, de seguinte maneira:*
Seja $(\mathbb{Z}_m; +_m, \cdot_m, \overline{0}, \overline{1})$, onde $\overline{0}$ e $\overline{1}$ são as classes de equivalência usuais, i.e., $\overline{0} = \{t \in \mathbb{Z} | \quad 0 \equiv_m t\}$ e $\overline{1} = \{t \in \mathbb{Z} | \quad 1 \equiv_m t\}$. Definimos a adição e o produto como segue:
$\overline{a} +_m \overline{b} := \overline{a + b}$ *e* $\overline{a} \cdot_m \overline{b} := \overline{a \cdot b}$.
Antes de podermos usar estas definições é preciso ter certeza que elas são boas definições, ou seja, que elas são independentes aos representantes, pois observe que estamos definido acima soma e produto de conjuntos! Matematicamente, é preciso fazer contas para mostrar a boa definição, ou seja, é preciso demonstrar que de $a \equiv_m b$ e $c \equiv_m d$, temos que, $(a + b) \equiv_m (c + d)$ e $(ab) \equiv_m (cd)$. Mas observe que esta conta já foi feita em proposição 2.6.4.
Agora podemos verificar os axiomas para um anel comutativo com unidade, cf. 1.3.11, (i) - (ix). Esta tarefa deixamos como exercício para o estudante interessado. ∎

Proposição 2.6.6. *Sejam $m \geq 2$ e $a, b, c \in \mathbb{Z}$ inteiros tais que $mdc(m; c) = 1$.*
Se $ac \equiv_m bc$, então, $a \equiv_m b$.

Demonstração: Sejam m, a, b e c como na hipótese da proposição. Seja $ac \equiv_m bc$, i.e., $m|(ac - bc)$. Assim, temos que $m|(c(a - b))$. Como agora $mdc(m; c) = 1$, temos que $m|(a - b)$, ou seja, $a \equiv_m b$. ∎

Exemplo 2.6.7. *(a) Vamos mostrar que $13|(4^{2n+1} + 3^{n+2})$, $\forall n \in \mathbb{N}$. Elaboramos uma prova por indução em n.*
O início da indução é feito para $n = 0$. Observe que precisamos mostrar que $13|(4^1 + 3^2)$, ou seja, $13|13$, o que é imediato.
No passo da indução temos a hipótese da indução: $13|(4^{2n+1} + 3^{n+2})$.
Vamos mostrar que $13|(4^{2(n+1)+1} + 3^{(n+1)+2})$.
Observe que $4^{2(n+1)+1} + 3^{(n+1)+2} = 4^{2n+3} + 3^{n+3} = 4^2 \cdot 4^{2n+1} + 3 \cdot 3^{n+2} = (13 + 3)4^{2n+1} + 3 \cdot 3^{n+2} =$

[3] Relembre da definição da união $\bigcup a := \{x | \quad \exists y \in a, x \in y\}$ feita em [5]

$13 \cdot 4^{2n+1} + 3(4^{2n+1} + 3^{n+2})$. *Agora é imediato que* $13|(13 \cdot 4^{2n+1})$ *e pela hipótese da indução temos que* $13|(4^{2n+1} + 3^{n+2})$. *Logo,* $13|(4^{2(n+1)+1} + 3^{(n+1)+2})$, *o que era para mostrar.* ∎

(b) Queremos saber qual é o resto da divisão de 5^{60} *por* 26. *É óbvio que não queremos calcular o valor de* 5^{60}. *De alguma maneira é para ter uma idéia. Sabemos pela divisão com resto que existem* q, r *inteiros únicos tais que* $5^{60} = 26q + r$, *onde* $0 \leq r < 26$. *Assim,* $26q = 5^{60} - r$, *ou seja,* $26|(5^{60} - r)$. *Isto significa que* $5^{60} \equiv_{26} r$.
Agora, observe que $5^2 = 25 \equiv_{26} -1$. *Pela proposição 2.6.4, temos que* $5^{60} = (5^2)^{30} \equiv_{26} (-1)^{30} = 1$. *Assim,* 5^{60} *tem resto* 1 *após a divisão por* 26.

(c) Queremos saber qual é o último algarismo da unidade de 3^{100}. *Também nesta vez não queremos e nem podemos calcular* 3^{100}. *Faremos um truque usando novamente congruências. Primeiramente, observe que um número natural* a *escrito na base decimal tem a forma* $a = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0$. *Assim, temos que* $a \equiv_{10} a_0$.
Logo, é preciso determinar o algarismo digamos $x \in \{0, 1, \ldots, 9\}$ *tal que* $3^{100} \equiv_{10} x$. *Observe que* $3^2 = 9 \equiv_{10} -1$. *Portanto, usando novamente 2.6.4,* $3^{100} = (3^2)^{50} \equiv_{10} (-1)^{50} = 1$, *ou seja, o último algarismo de* 3^{100} *é* 1.

(d) Queremos saber qual é o resto do número $t := 62 \cdot 10 \cdot 181^{40} \cdot 6^2$ *após a divisão por* 13. *Obviamente, queremos saber o menor resto positivo e também é* fora *de questão calcular o valor do número* t.
Vamos usar congruências e em especial 2.6.4. Observe que $62 \equiv_{13} -3$ *e* $10 \equiv_{13} -3$. *Por 2.6.4,* $62 \cdot 10 \equiv_{13} (-3)(-3) = 9$. *Agora* $6^2 = 36 \equiv_{13} (-3)$ *e portanto,* $62 \cdot 10 \cdot 6^2 \equiv_{13} 9 \cdot (-3) = -27 \equiv_{13} -1$.
Falta calcular o resto de 181^{40} *após a divisão por* 13. *Observe que* $13^2 = 169$. *Assim, temos que* $169 + 12 = 181 \equiv_{13} -1$, *pois* $13|(181 - (-1))$. *Logo,* $181^{40} \equiv_{13} (-1)^{40} = 1$. *Resumindo temos que* $t \equiv_{13} (-1) \cdot 1 = -1 \equiv_{13} 12$. *Ou seja, o resto de* t *após a divisão por* 13 *é* 12.

Na lista de exercícios têm mais exercícios par este assunto.

Em seguida queremos estabelecer alguns critérios de divisibilidade. Temos a seguinte

Observação 2.6.8. *Temos dois critérios simples para a divisibilidade de um inteiro por* 2 *e por* 5, *cujas demonstrações são deixadas na lista de exercícios. Seja* t *um inteiro.*
(a) $2|t$ *sse o último algarismo de* t *é divisível por* 2, *ou seja, é* $0, 2, 4, 6$ *ou* 8.
(b) $5|t$ *sse o último algarismo de* t *é* 0 *ou* 5.
Temos mais dois critérios para divisibilidade por 3 *e por* 11. *Seja* $a := a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$ *Então,*
(c) $3|a$ *sse* $3|(a_n + a_{n-1} + \ldots + a_1 + a_0$.
(d) $11|a$ *sse* $11|((-1)^n a_n + (-1)^{n-1} a_{n-1} + \ldots + (-1)^1 a_1 + (-1)^0 a_0 = \sum_{i=0}^{n} (-1)^i a_i$.

Demonstração: As demonstrações dos ítens (a) e (b) são relativamente simples e são deixados como exercício. Usaremos congruências para mostar os ítens (c) e (d). Para justificar (c), observe que $10 \equiv_3 1$. Assim, podemos demonstrar facilmente por indução em n - faça isso em exercício - que $10^n \equiv_3 1$, para todo $n \in \mathbb{N}$. Usando 2.6.4, temos que $a_n 10^n \equiv_3 a_n$, para qualquer $n \in \mathbb{N}$. Logo temos que

$$a = a_n 10^n + \ldots + a_1 \cdot 10^1 + a_0 \equiv_3 \sum_{i=0}^{n} a_i,$$

ou seja, existe $k \in \mathbb{Z}$ tal que $a = \sum_{i=0}^{n} a_i + 3k$. Agora observe que

$$3|a \quad \text{sse} \quad 3|(\textstyle\sum_{i=0}^{n} a_i + 3k) \quad \text{sse} \quad 3|\sum_{i=0}^{n} a_i,$$

o que era para justificar.
A demonstração de (d) é semelhante. Observe que $10 \equiv_{11} -1$.
Agora é fácil mostrar que para todo $n \in \mathbb{N}$, $10^n \equiv_{11} (-1)^n$ (exercício). Usando a proposição 2.6.4, obtemos que

$$a = a_n 10^n + \ldots + a_1 \cdot 10^1 + a_0 \equiv_{11} \sum_{i=0}^{n} (-1)^i a_i,$$

ou seja, existe $k \in \mathbb{Z}$ tal que $a = \sum_{i=0}^{n} (-1)^i a_i + 11k$. Agora observe que

$$11|a \quad \text{sse} \quad 11|(\textstyle\sum_{i=0}^{n} (-1)^i a_i + 11k) \quad \text{sse} \quad 11|\sum_{i=0}^{n} (-1)^i a_i,$$

o que era para justificar. ∎

2.7 O teorema chinês dos restos[4]

Nesta seção formulamos e demonstramos o *teorema chinês dos restos* qual de vez em quando tem aplicações em questões computacionais. É preciso alguns conceitos matemáticos para o tratamento deste teorema. Por isso, começamos com a seguinte definição. Em seguida, para facilitar tratamos sempre - mesmo somente escrevendo anel! - de *anéis comutativos com unidade*, cf. teorema 1.3.11, (i) - (ix).

Definição 2.7.1. *Sejam R e R' anéis comutativos com unidade e $f : R \to R'$ uma aplicação.*
(a) Dizemos que f é um **morfismo de anéis** *sse para quaisquer $r, s \in R$,*
(i) $f(r +_R s) = f(r) +_{R'} f(s)$ e (ii) $f(r \cdot_R s) = f(r) \cdot_{R'} f(s)$.
(b) Dizemos que f é um **isomorfismo de anéis** *sse f é morfismo de anéis e f é bijetiva. Neste caso, também dizemos que os anéis R e R' são isomorfos, i.e., $R \cong R'$.*

Observação 2.7.2. *(Anel produto) Sejam $n \geq 2$ um natural e $R_1, \ldots, R_n$ anéis. Consideremos o produto Cartesiano $R := R_1 \times \ldots \times R_n$ e observemos que R pode ser munido com estrutura de anel de seguinte maneira:*
Para quaisquer $t := (t_1, \ldots, t_n)$ e $s := (s_1, \ldots, s_n)$ elementos de R, definimos
$\cdot_R : R \times R \to R, (t; s) \mapsto t \cdot_R s := (t_1 \cdot_{R_1} s_1, \ldots, t_n \cdot_{R_n} s_n)$, *e*
$+_R : R \times R \to R, (t; s) \mapsto t +_R s := (t_1 +_{R_1} s_1, \ldots, t_n +_{R_n} s_n)$,
$1_R := (1_{R_1}, \ldots, 1_{R_n})$ *e* $0_R := (0_{R_1}, \ldots, 0_{R_n})$

Não é difícil de mostrar que $(R; +_R, \cdot_R, 0_R, 1_R)$ é de fato anel comutativo com unidade. Faça esta tarefa em exercício - isto está sendo feito coordenadas por coordenadas e não é difícil. ∎

Estamos agora em condições dar uma formulação do teorema chinês dos restos de 1247.

Teorema 2.7.3. *Sejam $m_i \geq 2$, onde $i \in \{1, \ldots, r\}$, naturais 2 a 2 primos entre si, i.e., $mdc(m_i; m_j) = 1$, para $i \neq j$. Seja $m := m_1 \cdot \ldots \cdot m_r$ o produto destes naturais.*
Então, os anéis $\mathbb{Z}_m := \mathbb{Z}/\mathbb{Z}_m$ e $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ são isomorfos.
O isomorfismo é dado pela aplicação, $\varphi : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}, \quad [t]_m \mapsto ([t]_{m_1}, \ldots, [t]_{m_r})$.

Demonstração: Sejam $m_1, \ldots, m_r$ 2 a 2 primos entre si e $m = m_1 \cdot \ldots \cdot m_r$. Vejamos que a aplicação dada por φ é um isomorfismo de anéis.

(i) φ é bem definida, pois: Observe que φ é definido para classes, assim é preciso mostrar que a definição é independente dos representantes, ou sejam $[t]_m = [s]_m$, então vejamos que $\varphi([t]_m) = \varphi([s]_m)$. De $[t]_m = [s]_m$ inferimos que $t \equiv_m s$, ou seja, $m|(t - s)$. Como $m_i|m$, para todo $i \in \{1, \ldots, r\}$, temos que $m_i|(t - s)$, ou seja, $t \equiv_{m_i} s$. Logo, temos que para todo i, $[t]_{m_i} = [s]_{m_i}$. Portanto, $\varphi([t]_m) = \varphi([s]_m)$ e assim φ é bem definida.

(ii) φ é morfismo de anéis, pois: É preciso verificar a definição 2.7.1, (a). Esta tarefa é simples e deixamos para o estudante em exercícios.

(iii) φ é sobrejetiva, pois: Observe que precisamos mostrar que para um $([t_1]_{m_1}, \ldots, [t_r]_{m_r}) \in \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ arbitrário, existe $[t]_m \in \mathbb{Z}_m$ tal que $\varphi([t]_m) = ([t_1]_{m_1}, \ldots, [t_r]_{m_r})$. Dividimos a prova em duas partes:
Primeira parte: Mostramos que qualquer $[e_i] := ([0]_{m_1}, \ldots, [0]_{m_{i-1}}, [1]_{m_i}, [0]_{m_{i+1}}, \ldots, [0]_{m_r})$, $i \in \{1, \ldots, r\}$, pertence a imagem de φ, i.e., $[e_i] \in im(\varphi)$. Para isso, é preciso determinar um número $u_i \in \mathbb{Z}$ tal que $u_i \equiv_{m_i} 1$ e $u_i \equiv_{m_j} 0$, para $i \neq j$. (observe que assim $\varphi([u_i]) = [e_i]$.)
Tomemos $z_i := \frac{m}{m_i}$. Observe que $z_i \in \mathbb{Z}$ e $mdc(z_i; m_i) = 1$, pois os m_i's são 2 a 2 primos entre si. Além disso, temos que $z_i \equiv_{m_j} 0$, para $i \neq j$. Como $mdc(z_i; m_i) = 1$, existem pelo teorema de Bézout constantes

[4]Esta seção pode ser omitida por leitores sem conhecimentos na teoria dos anéis. Na próxima seção vamos solucionar congruências lineares e a apartir destes sistemas de congruências

r_i e s_i tais que $z_i s_i + m_i r_i = 1$, ou seja, $z_i s_i = 1 - m_i r_i$, o que implica que $z_i s_i \equiv_{m_i} 1$.
Tomando $u_i := z_i s_i$ resolve a nossa questão, ou seja, $\varphi([z_i s_i]_m) = [e_i]$.
Segunda parte: Nesta parte usamos a primeira parte para mostrar que φ de fato é sobrejetiva. Tome $t_i \in \mathbb{Z}$ arbitrário e observe que $[e_i t_i] = ([0]_{m_1}, \ldots, [0]_{m_{i-1}}, [t_i]_{m_i}, [0]_{m_{i+1}}, \ldots, [0]_{m_r})$. Agora, defina $t := \sum_{i=1}^{r} t_i u_i$ e observe que $t \equiv_{m_i} t_i$. Portanto, temos que $\varphi([t]_m) = [t_1]_{m_1}, \ldots, [t_r]_{m_r})$, mostrando que φ é sobrejetiva.

(iv) φ é 1 a 1, pois: Como φ é sobrejetiva e em $\mathbb{Z}_m$ como em $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ temos m elementos, φ tem que ser injetiva. Concluimos que φ é bijetiva.

Os ítens (i) - (iv) mostram que φ é isomorfismo de anéis, e acabamos a prova. ∎

O teorema chinês dos restos com a sua demonstração fornece um método de solucionar sistemas de congruências, vejamos a próxima observação.

Observação 2.7.4. *São equivalentes:*
(a) O teorema chinês dos restos 2.7.3, e
(b) O sistema para $m_1, \ldots, m_r$ 2 a 2 primos entre si e $m = m_1 \cdot \ldots \cdot m_r$,

$$(*) \begin{cases} x \equiv_{m_1} t_1 \\ \vdots \\ x \equiv_{m_r} t_r \end{cases}$$

tem **única** *solução módulo m.*

Demonstração: Observe que para $t_1, \ldots, t_r \in \mathbb{Z}$ existe $t \in \mathbb{Z}$ tal que $\varphi([t]_m) = ([t_1]_{m_1}, \ldots, [t_r]_{m_r})$ pelo teorema 2.7.3. Assim, t é solução de $(*)$. Como φ é 1 a 1, existe único t módulo m, satisfazendo o sistema $(*)$. ∎

Exemplo 2.7.5. *Consideremos o seguinte sistema*

$$(*) \begin{cases} x \equiv_3 2 \\ x \equiv_4 3 \\ x \equiv_5 2 \end{cases}$$

Observe que os números $3, 4$ e 5 são 2 a 2 primos entre si e $3 \cdot 4 \cdot 5 = 60$. Pela observação anterior existe uma solução de $(*)$ e esta é única módulo 60. Para resolver o sistema $(*)$ usamos as construções da demonstração de 2.7.3.
Numa primeira parte resolvemos as equações
(i) $3r_1 + 20s_1 = 1$, *(ii)* $4r_2 + 15s_2 = 1$, *e* *(iii)* $5r_3 + 12s_3 = 1$.
Neste caso não precisamos fazer uso do algoritmo de Euclides, pois por tentativa obtemos que *(i)* $3 \cdot 7 + 20 \cdot (-1) = 1$, *(ii)* $4 \cdot 4 + 15 \cdot (-1) = 1$, *e* *(iii)* $5 \cdot 5 + 12 \cdot (-2) = 1$.
Assim, temos as constantes $u_1 = (-1) \cdot 20 = -20$, $u_2 = (-1) \cdot 15 = -15$ e $u_3 = (-2) \cdot 12 = -24$. Obtemos então para a solução $x = 2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24) = -133 \equiv_{60} -13 \equiv_{60} 47$.
Assim, observe que 47 é de fato solução de $(*)$, pois $47 \equiv_3 2$, $47 \equiv_4 3$ e $47 \equiv_5 2$. Pelo teorema 2.7.3 qualquer outra solução de $(*)$ é equivalente módulo 60 a 47. ∎

Observação 2.7.6. *Resolva os seguintes sistemas através do uso do teorema chinês do resto:*

$$(a) \begin{cases} x \equiv_3 1 \\ x \equiv_7 3 \\ x \equiv_5 2 \end{cases} \qquad (b) \begin{cases} x \equiv_3 2 \\ x \equiv_5 3 \\ x \equiv_7 2 \end{cases} \qquad (c) \begin{cases} x \equiv_6 5 \\ x \equiv_{11} 4 \\ x \equiv_7 3 \end{cases}$$

∎

2.8 Solução de congruências lineares

Queremos solucionar congruências lineares da forma seguinte, para $a, b \in \mathbb{Z}$ e $m \geq 2$:

$$ax \equiv_m b \qquad (*)$$

É possível reduzir congruências lineares para equações Diofantinas, cf. 2.5. Vamos esboçar este método sem elaborar os detalhes. Primeiramente, podemos mostrar que vale

Fato 1: A congruência $(*)$ tem solução sse $mdc(a, m)|b$.
Demonstração: Observe que temos as seguintes equivalências:
$ax \equiv_m b$ sse $m|(ax - b)$ sse $\exists y \in \mathbb{Z}$ tal que $ax + my = b$.
Aí, temos uma equação Diofantina equivalente e podemos usar resultados de 2.5. ∎

Agora podemos formular o seguinte

Teorema 2.8.1. *Sejam $a, b, m \in \mathbb{Z}$ com $m \geq 2$, $d := mdc(a, m)|b$. Escrevendo (usando Bézout) $d = ra + sm$ e $b = db_1$, temos que $ax \equiv_m b$ tem d soluções não congruentes 2 a 2 módulo m:*
$x_0 = rb_1, x_1 = rb_1 + \frac{1}{d}m, \ldots, x_{d-1} = rb_1 + \frac{d-1}{d}m$.

Demonstração: Sabemos pelo Fato 1 acima, que a congruência possui solução. Pelo teorema 2.5.4, sabemos calcular as soluções:
$x = rb_1 + \frac{m}{d}t$, $y = sb_1 - \frac{a}{d}t$, para $t \in \mathbb{Z}$. Portanto as soluções da congruência são da forma x.
Falta demonstrar que para $t := 0, 1, \ldots, d-1$ as soluções $x_0, x_1, \ldots, x_{d-1}$ como no enunciado satisfazem:
(i) qualquer outra solução é congruente a uma desssa, e
(ii) as soluções acima são 2 a 2 não congruentes.
Vejamos (i): Seja $x = x_0 + \frac{m}{d}t$ uma solução de $(*)$. Vamos dividir t por d e obtemos - pela divisão com resto: $t = qd + r'$, onde $0 \leq r' < d$. Aí, obtemos que

$$x = x_0 + \tfrac{m}{d}t = x_0 + \tfrac{m}{d}(qd + r') = x_0 + mq + \tfrac{m}{d}r' \equiv_m x_0 + \tfrac{m}{d}r',$$

mostrando (i).
Vejamos (ii). Considere $x_h = x_0 + \frac{h}{d}m$ e $x_k = x_0 + \frac{k}{d}m$, onde s.p.d.g. $0 \leq k \leq h < d$. Suponha que $x_h \equiv_m x_k$, então precisamos mostrar que $h = k$.
De $x_h \equiv_m x_k$, obtemos que $\frac{hm}{d} \equiv_m \frac{km}{d}$. Logo $m|(h-k)\frac{m}{d}$.
Escrevemos $m = dm_1$ e obervemos que de $0 \leq h - k < d$, $0 \leq (h-k)m_1 < dm_1 = m$. Porém, sabemos que $m|(h-k)m_1$ o que acarreta $h = k$. ∎.

Temos então o seguinte

Corolário 2.8.2. *Sejam $a, b, m \in \mathbb{Z}$ com $m \geq 2$ e $mdc(a, m) = 1$. Então a congruência $ax \equiv_m b$ tem sempre solução. Além disso, escrevendo $1 = ra + sm$, $x = rb$ é única solução módulo m.* ∎

Em seguida, vamos solucionar congruências lineares *sem* mencionar equações Diofantinas.

Denotamos $a = a_1 d$, $b = b_1 d$ e $m = m_1 d$, onde $mdc(a_1; m_1) = 1$.
Sabemos pelo Fato 1 que a congruência $(*)$ tem solução (inteira) sse $mdc(a, m)|b$. Temos agora

Lema 2.8.3. *Com as notações, $(*)$ é equivalente com $a_1 x \equiv_{m_1} b_1$.*

Demonstração: Como $d = mdc(a; m)$ existem constantes r, s inteiros tais que $d = ar + ms$. Cancelando $d \neq 0$ nos dois lados temos que $1 = a_1 r + m_1 s$.
Aí, observe que x solução de $(*)$ sse $m|(ax - b)$, ou seja $(m_1 d)|(d(a_1 x - b_1)$ sse $m_1|(a_1 x - b_1)$, ou seja, x é solução de $a_1 x \equiv_{m_1} b_1$. ∎

Denotamos então $a_1 x \equiv_{m_1} b_1$ por $(**)$, demonstramos

Lema 2.8.4. *Com as notações $(**)$ é equivalente com $x \equiv_{m_1} rb_1$, $(***)$.*

Demonstração: Vejamos $\Rightarrow$. Seja x solução de $(**)$. Observe que temos o seguinte: $ra_1 = 1 - sm_1 \equiv_{m_1} 1$. Assim, temos que $(ra_1 x) \equiv_{m_1} x$. Multiplicando $(**)$ por r, obtemos que $ra_1 x \equiv_{m_1} rb_1$. Como $\equiv_{m_1}$ é uma relação de equivalência, obtemos que $x \equiv_{m_1} rb_1$, ou seja x é solução de $(***)$.
Por outro lado, vendo $\Leftarrow$, seja x solução de $(***)$, i.e., $x \equiv_{m_1} rb_1$. Como $ra_1 \equiv_{m_1} 1$, temos que $ra_1 x \equiv_{m_1} rb_1$. Usando o fato de que $mdc(r; m_1) = 1$, a última equivalência é equivalente com $a_1 x \equiv_{m_1} b_1$. ■

Dos lemas 2.8.3, 2.8.4, temos a seguinte

Proposição 2.8.5. *Sejam $a, b, m \in \mathbb{Z}$ com $m \geq 2$, $d := mdc(a, m)|b$. Escrevendo (usando Bézout) $d = ra + sm$ e $a = da_1$, $b = db_1$ e $m = dm_1$ temos que*

$$ax \equiv_m b \quad sse \quad x \equiv_{m_1} rb_1.$$ ■

Observação 2.8.6. *Agora observe que a solução de $x \equiv_{m_1} rb_1$ é imediato dado por $x = rb_1 + m_1 t$, pois $m_1|(x - rb_1)$, ou seja, $x - rb_1 = tm_1$ para algum $t \in \mathbb{Z}$. Ou seja, as soluções são $x = rb_1 + \frac{m}{d}t$, para qualquer $t \in \mathbb{Z}$. Usando o teorema 2.8.1, podemos obter as soluções da forma*

$$x_0 = rb_1, x_1 = rb_1 + \tfrac{1}{d}m, \ldots, x_{d-1} = rb_1 + \tfrac{d-1}{d}m.$$

2 a 2 não congruentes módulo m. ■

Exemplo 2.8.7. *(a) Queremos solucionar $6x \equiv_4 14$.*
Sabemos que $mdc(6; 4) = 2$ e $2 = 1 \cdot 6 + (-1) \cdot 4$. Pelas observações anteriores, a congruência dada é equivalente com $x \equiv_2 7$, ou seja $x = 7 + 2t$, para $t \in \mathbb{Z}$, são as soluções da congruência.
(b) Seja $-3x \equiv_{15} 18$. Sabemos que $mdc(-3, 18) = 3$ divide 15. Logo a congruência linear possui solução. Escrevemos $3 = 4 \cdot (-3) + 1 \cdot 15$ temos que a congruência inicial é equivalente com $x \equiv_5 24$. As soluções 2 a 2 não congruentes módulo 15 desta congruência são as seguintes:
$x_0 = 24, x_1 = 29, x_2 = 34$. ■

Observação 2.8.8. *Resolva as seguintes congruências:*
(a) $25x \equiv_{29} 15$, *(b)* $5x \equiv_{26} 2$, *(c)* $140x \equiv_{301} 133$. ■

2.9 O Teorema chinês dos restos, revisto

O chinês Sun Tsu considerou no ano 300 d.C. - em seu livro *Livro sobre Aritmética* - se perguntou o seguinte problema:
Queremos determinar um número inteiro qual dividido por $3, 5$ e 7 tem os restos $2, 3$ e 2, respectivamente. Em nossa notação seria um número que satisfaz o seguinte sistema de congruências (lineares):

$$\begin{cases} x \equiv_3 2 \\ x \equiv_5 3 \\ x \equiv_7 2 \end{cases}$$

Ele determinou números *auxiliares*, 70, 21 e 15 e calculou $233 = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15$. Dividimos 233 pelo produto $3 \cdot 5 \cdot 7$, obtemos 23, e este número é menor solução positiva do nosso problema. Resultados deste tipo se tornaram conhecidos na Europa aparentemente somente por volta de 1850. Karl Friedrich Gauβ escreveu sobre estes problemas e suas soluções em *Disquisitiones Arithmeticae* em 1874.

Queremos determinar soluções gerais dos sistemas da forma

$$\begin{cases} a_1 x \equiv_{m_1} b_1 \\ a_2 x \equiv_{m_2} b_2 \\ \quad \vdots \\ a_3 x \equiv_{m_k} b_k \end{cases}$$

Observe que este sistema admite solução dado que cada uma das suas congruências admite solução, ou seja, $d_i := mdc(a_i, m_i)|b_i$, para todo $i \in \{1, \ldots, k\}$. Sabemos pela proposição 2.8.5 que cada congruência é equivalente a uma congruência da forma $x \equiv_{n_i} c_i$ com $n_i = \frac{m_i}{d_i}$, c_i adequado e $i \in \{1, \ldots, k\}$. Assim, obtemos um sistema equivalente dado em seguida:

$$(*) \begin{cases} x \equiv_{n_1} c_1 \\ x \equiv_{n_2} c_2 \\ \quad \vdots \\ x \equiv_{n_k} c_k \end{cases}$$

O teorema chinês dos restos nos dá uma possibilidade de solucionar tal sistema, no caso de $n_1, \ldots, n_k$ serem 2 a 2 primos entre si, i.e., $\forall i, j \in \{1, \ldots, k\}, \quad i \neq j \Rightarrow mdc(n_i, n_j) = 1$.

Teorema 2.9.1. *(Teorema chinês dos restos) Sejam $n_1, \ldots, n_k$ naturais 2 a 2 primos entre si. Sejam $c_1, \ldots, c_k$ inteiros quaisquer. O sistema de congruências $(*)$ admite única solução módulo $n := n_1 \cdot \ldots \cdot n_k$.*

Demonstração: Com as hipóteses, consideremos o sistema acima $(*)$. Seja $n := n_1 \cdot \ldots \cdot n_k$. Denotamos por $N_i := \frac{n}{n_i} \in \mathbb{Z}$, para qualquer $i \in \{1, \ldots, k\}$. Observe que $mdc(N_i, n_i) = 1$. Agora podemos determinar as constantes de Bézout r_i, s_i tais que $r_i N_i + s_i n_i = 1 \quad (+)$ e demonstramos o seguinte

Fato: O número $x_0 = \sum_{i=1}^{k} c_i r_i N_i$ é uma solução do sistema $(*)$.
Prova do Fato: Observe que primeiramente para $i, j \in \{1, \ldots, k\}$, se $i \neq j$ então $N_j \equiv_{n_i} 0$. Logo temos que $c_j r_j N_j \equiv_{n_i} 0$. Daí, é fácil ver que $\sum_{i=1}^{k} c_i r_i N_i \equiv_{n_i} c_i r_i N_i$. Das equações $(+)$, obtemos que $r_i N_i = 1 + s_i n_i \equiv_{n_i} 1$. Logo, obtemos que $x_0 \equiv_{n_i} c_i r_i N_i \equiv_{n_i} c_i$, mostrando que x_0 é de fato uma solução de $(*)$.

Falta verificar que x_0 é única solução de $(*)$ módulo n, ou seja, qualquer outra solução de $(*)$ é congruente a x_0 módulo n. Para isso, consideremos x outra solução de $(*)$. Então, para qualquer $i \in \{1, \ldots, k\}$, $x \equiv_{n_i} c_i$. Como $x_0 \equiv_{n_i} c_i$, temos que $x_0 \equiv_{n_i} x$, ou seja, $n_i|(x - x_0)$. Como i era arbitrário e os naturais $n_1, \ldots, n_k$ são 2 a 2 primos entre si, é preciso que $n|(x - x_0)$, terminando a demonstração. ∎

Exemplo 2.9.2. *Consideremos o seguinte sistema*

$$\begin{cases} 6x \equiv_4 2 \\ 2x \equiv_3 1 \\ 4x \equiv_7 2 \end{cases}$$

Em respeito da existência de soluções observemos que:
$d_1 = mdc(6, 4) = 2|2$,
$d_2 = mdc(2, 3) = 1|1$, *e*
$d_3 = mdc(4, 7) = 1|2$.
Sabemos que cada congruência possui solução. Agora, vamos transformar o sistema acima num sistema da forma $(*)$. Para isso, calculemos as constantes de Bézout, $2 = 1 \cdot 6 + (-1) \cdot 4$, $1 = (-1) \cdot 2 + 1 \cdot 3$ *e* $1 = 2 \cdot 4 + (-1) \cdot 7$. *Por 2.8.5, o sistema inicial é equivalente com o seguinte*

$$\begin{cases} x \equiv_2 1 \\ x \equiv_3 -1 \equiv_3 2 \\ x \equiv_7 4 \end{cases}$$

Podemos aplicar o teorema 2.9.1, pois $2, 3$ e 7 são primos entre si. Usando as técnicas da demonstração de teorema 2.9.1, obtemos que $n = 42$, $N_1 = 21$, $N_2 = 14$ e $N_3 = 6$. Obtemos as constantes de Bézout $r_1 = 1$, $r_2 = -1$ e $r_3 = -1$, respectivamente. Aí, a solução é dada por $x_0 = 11$, e sabemos que essa é única módulo 42. ∎

Observação 2.9.3. *O leitor interessado deve perguntar o que pode ser feito em casos em quais não podemos aplicar o teorema chinês? Nem sempre deve existir uma solução, porém um sistema da forma $(*)$ dada acima possui solução sse $\forall i \neq j$, $c_i \equiv_{mdc(n_i, n_j)} c_j$. Todas as soluções são neste caso congruentes módulo mmc dos $n_1, \ldots, n_k$.*

Consideremos o seguinte problema: Queremos achar o menor natural qual tem após a divisão por $2, 3, 4, 5$ *e* 6 *o resto* 1 *e qual é divisível por* 7*. O sistema de congruências não satisfaz as exigências do teorema chinês dos restos, porém podemos soluciona-lo da seguinte maneira: Podemos reunir as primeiras cinco exigências e obtemos que*

$$\begin{cases} x \equiv_{mmc(2,3,4,5,6)} 1 \equiv_{60} 1 \\ x \equiv_7 0 \end{cases},$$

qual sistema pode ser solucionado pelo teorema chinês. Cálcule!
Em alguns outros casos é possível determinar soluções transformando cada congruência numa equação Diofantina e procurar as soluções simultaneamente. Em livros sobre Teoria dos Números devem ter exemplos para este tipo de sistemas, em particular em [14] estão sendo tratados tais exemplos. ■

Capítulo 3

Conceitos báscios em ordens

Neste capítulo trabalhamos com ordem, e definimos três tipos de ordens. O conceito de ordem é importante para a computação, pois certos cálculos computacionais podem ser idealizados por funções preservando ordens, cf. 3.1.5. O conceito da álgebra de Boole, também pode ser introduzido puramente algébrica, sem mencionar uma ordem, porém a ordem existe de mesmo jeito - de fato as duas abordagens são equivalentes. Os assuntos desta seção podem ser encontrados também em [6], [12] e [15].

3.1 Pré-ordem, ordem parcial e ordem linear

Introduzimos três tipos de ordem, e usamos para a relação de ordem sempre o símbolo $\leq$, como é comum. Mas, observe que $\leq$ somente denota uma relação qual satisfaz alguns axiomas específicas para ordem, e não necessariamente tem algo a ver com a relação de *menor ou igual* entre números.

Definição 3.1.1. *Sejam P um conjunto não vazio e $\leq$ uma relação em P.*
(a) Dizemos que $(P;\leq)$ é uma **pré-ordem** *sse $\leq$ é reflexiva e transitiva.*
(b) Dizemos que $(P;\leq)$ é uma **ordem parcial** *sse $(P;\leq)$ é uma pré-ordem e $\leq$ é anti-simétrica, i.e., $\forall x, y \in P, x \leq y \ \& \ y \leq x \ \Rightarrow \ x = y$.*
(c) Dizemos que $(P;\leq)$ é uma **ordem linear** *ou* **conectada** *ou* **total** *sse $(P;\leq)$ é uma ordem parcial e $\leq$ é linear, i.e., $\forall x, y \in P, x \leq y \ \ ou \ \ y \leq x$.*

Temos alguns exemplos para vários tipos de ordens.

Exemplo 3.1.2. *(a) Consideremos $(\mathbb{Z};|)$. Observe que a relação $|$ de fato é uma relação de ordem, pois pela proposição 2.1.5, sabemos que $|$ é reflexiva e transitiva. Por outro lado $|$ não é relação anti-simétrica, pois temos que $2|(-2)$ e $(-2)|2$, mas $2 \neq (-2)$. Assim, $(\mathbb{Z};|)$ é somente uma pré-ordem. Em seguida, vejamos que toda pré-ordem induz uma ordem parcial por uma simples identificação.*
(b) Consideremos agora $(\mathbb{N};|)$. Então, também por 2.1.5, $(\mathbb{N};|)$ é uma pré-ordem. Mas neste caso temos para quaisquer $m, n \in \mathbb{N}$: para $n|m$ e $m|n$, temos que $|n| = |m|$, e como estamos nos naturais temos que $n = m$, mostrando que $|$ é anti-simétrica em $\mathbb{N}$. Logo, $(\mathbb{N};|)$ é uma ordem parcial. Porém $(\mathbb{N};|)$ não é uma ordem linear, pois para $2, 3 \in \mathbb{N}$, temos que $2 \not| 3$ nem $3 \not| 2$.
(c) Consideremos agora um conjunto arbitrário A e $(\mathcal{P}(A);\subseteq)$. Pela teoria de conjuntos ingênua, sabemos que a relação da inclusão $\subseteq$, é reflexiva, transitiva e também anti-simétrica. Assim, $(\mathcal{P}(A);\subseteq)$ é uma ordem parcial. Em caso de o conjunto A é vazio ou contém um só elemento, $(\mathcal{P}(A);\subseteq)$ é uma ordem linear (faça os detalhes).
(d) Consideremos $(\mathbb{N};\leq)$, onde $n \leq m$ sse $\exists k \in \mathbb{N}$ tal que $n + k = m$. Assim, podemos facilmente mostrar

(exercício) que $(\mathbb{N}; \leq)$ *é uma ordem linear.*
(e) Vamos elaborar um exemplo da lógica interessante: Seja L *uma linguagem da lógica proposicional clássica, veja [5], e denotamos por* $Form(L)$ *o conjunto das* L*-fórmulas. Definimos agora a relação* $\leq$ *em* $Form(L)$ *de seguinte maneira:*

$$\text{para } \varphi, \psi \in Form(L), \qquad \varphi \leq \psi \quad \text{sse} \quad (\varphi \to \psi) \text{ é uma tautologia.}$$

Assim, $(Form(L); \leq)$ *é uma pré-ordem. Vejamos isto de seguinte maneira: Primeiramente é imediato que* $\leq$ *é reflexiva, ou seja, para qualquer* $\varphi \in Form(L)$, $\varphi \leq \varphi$, *pois* $(\varphi \to \varphi)$ *é de fato uma tautologia. Sejam agora* φ, ψ *e* χ L*-fórmulas tais que* $\varphi \leq \psi$ *e* $\psi \leq \chi$. *Então, temos que* $(\varphi \to \psi)$ *e* $(\psi \to \chi)$ *são tautologias. Vamos mostrar que* $(\varphi \to \chi)$ *é tautologia. Observe que se* φ *tem valor de verdade* 1*, então precismaos mostrar que* χ *também tem valor* 1. *Mas, tendo* φ *valor* 1 *e sendo* $(\varphi \to \psi)$ *uma tautologia, é preciso que neste caso* ψ *tem valor* 1. *Sendo* $(\psi \to \chi)$ *uma tautologia, o valor de* χ *tem que ser* 1 *neste caso. Consequentemente,* $(\varphi \to \chi)$ *é uma tautologia e assim* $\varphi \leq \chi$. *Agora é fácil observar que* $\leq$ *não é anti-simétrica: Tome por exemplo as* L*-fórmulas* $(\neg(\neg(\varphi \to \varphi)))$ *e* $(\varphi \to \varphi)$. *É fácil ver que* $(\neg(\neg(\varphi \to \varphi))) \leq (\varphi \to \varphi)$ *e* $(\varphi \to \varphi) \leq (\neg(\neg(\varphi \to \varphi)))$ *- faça os detalhes! Mas obviamente* $(\neg(\neg(\varphi \to \varphi))) \neq (\varphi \to \varphi)$.
Logo, $(Form(L); \leq)$ *é somente uma pré-ordem.* ∎

Tendo em vista os últimos exemplos, podemos introduzir uma ordem parcial numa pré-ordem **sem** perder as informações importantes da pré-ordem dada, como mostra a seguinte proposição.

Proposição 3.1.3. *Toda pré-ordem induz uma ordem parcial.*

Demonstração: Seja $(P; \leq)$ uma pré-ordem, i.e., $\leq$ é reflexiva e transitiva. Vamos num primiero passo identificar os elementos $x, y \in P$ quais satisfazem $x \leq y$ e $y \leq x$. Neste caso, dizemos que $x \sim y$. $(*)$
Fato 1: $\sim$ é uma relação de equivalência em P.
Prova do fato 1: Em exercício, vamos mostrar que $\sim$ é reflexiva, simétrica e transitiva. Observe que a reflexividade e a transitividade seguem da hipótese que $\leq$ é reflexiva e transitiva. A própria definição de $\sim$ deixa $\sim$ simétrica.
Mostrado este fato, podemos considerar o conjunto quociente $[P]_\sim$. Neste conjunto quociente introduzimos a seguinte nova relação:

$$\text{para todo } [x], [y] \in [P]_\sim, \qquad [x] \leq^* [y] \quad \text{sse} \quad x \leq y.$$

Observe que esta definição é uma *boa definição*, ou seja, independente dos representantes. Sabemos que precisamos mostrar para

$$x, x', y, y' \in P, \text{ tais que } [x] = [x'] \text{ e } [y] = [y'] \qquad [x] \leq^* [y] \quad \text{sse} \quad [x'] \leq^* [y'].$$

Sejam $x, x', y, y' \in P$ dados como acima e tais que $[x] \leq^* [y]$. Daí, temos que $x' \leq x \leq y \leq y'$ e pela transitividade de $\leq$, obtemos que $x' \leq y'$. Assim, inferimos que $[x'] \leq^* [y']$. A outra direção é mostrada analogamente. Podemos então afirmar que a nossa definição dada acima é de fato uma boa definição. É fácil para mostrar que $([P]_\sim; \leq^*)$ é uma ordem parcial, finalizando a nossa demonstração. ∎

Exemplo 3.1.4. *(a) Reconsideremos o exemplo 3.1.2, (a), e sabemos que* $(\mathbb{Z}; |)$ *é uma pré-ordem. Aplicando o último resultado 3.1.3, esta pré-ordem* $|$ *induz uma ordem parcial e a demonstração nós dá o procedimento como fazer:*
Para $a, b \in \mathbb{Z}$*, definimos a seguinte relação* $\sim$*:*

$$a \sim b \qquad \text{sse} \qquad a|b \quad e \quad b|a.$$

Observe que $a \sim b$ *sse* $a = \pm b$. *Assim, temos que* $\mathbb{Z}/\sim := \{[a]_\sim | \quad a \in \mathbb{Z}\}$*, onde* $[a]_\sim := \{-a, +a\}$. *É fácil de estabelecer uma bijeção entre* $\mathbb{N}$ *e* $\mathbb{Z}/\sim$.
A ordem parcial induzida é a seguinte conforme a demonstração da proposição 3.1.3:

$$[a]_\sim |^* [b]_\sim \qquad \text{sse} \qquad a|b.$$

(b) Reconsideremos o exemplo 3.1.2, (a), e sabemos que $(Form(L); \leq)$ *é uma pré-ordem. De mesmo modo, cf. item (a), podemos aplicar as ideias da demonstração da proposição 3.1.3, e induzimos a seguinte*

ordem parcial:
$(Form(L)/\sim;\leq^*)$*, onde* $Form(L)/\sim := \{[\varphi]_\sim | \quad \varphi \in Form(L)\}$*, com* $[\varphi]_\sim := \{\psi \in Form(L) | \quad (\varphi \leftrightarrow \psi)$ *é uma tautologia* $\}$*. Além disso, temos a ordem parcial dado por:*

$$[\varphi]_\sim \leq^* [\psi]_\sim \qquad \textit{sse} \qquad (\varphi \to \psi) \textit{ é uma tautologia.}$$

Entenda todos os detalhes para estabelecer os resultados acima. ∎

Perguntamos quais aplicações entre ordens são de interesse a serem consideradas. Sabemos que em álgebra, consideremos aplicações quais são compatíveis com a estrutura da álgebra, por exemplo, na teoria dos grupos, consideremos morfismos de grupos, que preservam as operações do grupo, em teoria dos anéis, estas aplicações são chamadas morfismos de anéis, e estes preservam as operações dos anéis. Em nosso caso das ordens, vamos considerar aplicações quais preservam a ordem. Temos a seguinte

Definição 3.1.5. *Sejam* $(P;\leq_P)$ *e* $(Q;\leq_Q)$ *ordens parciais.*
Dizemos que a aplicação $f : P \to Q, p \mapsto f(p)$ **preserva ordem** *sse para todo* $p, p' \in P, \quad p \leq_P p'$*, então,* $f(p) \leq_Q f(p')$*.*

Observação 3.1.6 (Interpretação das aplicações preservando ordem)**.** *As aplicações entre ordens parciais imitam na teoria da computação cálculos quais não perdem informações, ou seja, se num certo estágio, sabemos que* $p \leq p'$*, i.e.,* p' *tem pelo menos tanta informação do que* p*, após um cálculo, ou após a aplicação de um certo algoritmo* f*, temos que* $f(p) \leq f(p')$*, i.e., o resultado* $f(p')$ *contêm pelo menos tanta informação do que* $f(p)$*. Assim, não perdemos nenhuma informação.*

Devido a proposição 3.1.3, vamos trabalhar em seguida na maioria dos casos com uma **ordem parcial**. Mesmo partindo somente de uma pré-ordem, sabemos que esta induz uma ordem parcial. Por outro lado, na teoria da ordem, ordens totais não tem muita aplicabilidade, pelo fato de que estes são muito específicas.

3.2 Produtos de Ordens

Queremos entender se e como é possível expandir ordens, no sentido que partindo de ordens parciais, é possível considerar o produto Cartesiano com uma certa ordem qual vem das ordens iniciais. Restringimo-nos para um número finito de ordens parciais e trabalhamos inicialmente com duas ordens parciais $(P;\leq_P)$ e $(Q;\leq_Q)$.

3.2.1 Ordem por coordenadas

Ordem por coordenadas para ordens parciais

Sejam $(P;\leq_P)$ e $(Q;\leq_Q)$ ordens parciais, cf definição 3.1.1. Consideremos agora o produto Cartesiano $P \times Q$, que é um conjunto definido como sendo $P \times Q := \{\langle x; y\rangle | \quad x \in P \quad \& \quad y \in Q\}$. Uma maneira natural de "ordenar" este conjunto $P \times Q$ é a seguinte, que chamamos de **ordem por coordenadas**:

$$\forall \langle p; q\rangle, \langle p'; q'\rangle \in P \times Q, \qquad \langle p; q\rangle \leq \langle p'; q'\rangle \quad \text{sse} \quad p \leq_P p' \quad \text{e} \quad q \leq_Q q'$$

Temos agora o seguinte

Fato 3.2.1. *Com as notações de cima,* $(P \times Q;\leq)$ *é uma ordem parcial.*

A demonstração é feita nos exercícios. É preciso verificar para a nova ordem $\leq$ em $P \times Q$, as condições da definição 3.1.1, (b), isto é, demonstrar que $\leq$ é reflexiva, antisimétrica e transitiva. Isto decorre do fato que $\leq_P$ e $\leq_Q$ têm estas propriedades. ∎

Considerando agora um número finito de ordens parciais $(P_1; \leq_1), \ldots, (P_n; \leq_n)$, para algum natural $n \geq 2$, podemos introduzir no produto Cartesiano $(P_1 \times \cdots \times P_n)$ a ordem por coordenada de maneira natural:
Para $\langle x_1, \ldots, x_n\rangle, \langle y_1, \ldots, y_n\rangle \in P_1 \times \cdots \times P_n$ definimos

$$\langle x_1, \ldots, x_n\rangle \leq \langle y_1, \ldots, y_n\rangle \qquad \text{sse} \qquad x_i \leq_i y_i,\ \forall i = 1, \ldots, n$$

A relação $\leq$ definido acima é de fato uma ordem parcial em $P_1 \times \cdots \times P_n$. Mostre isso ! Obtivemos então o seguinte resultado generalizando o Fato 3.2.1

Fato 3.2.2. *Com as notações de cima, $(P_1 \times \cdots \times P_n; \leq)$ é uma ordem parcial.* ∎

Ordem por coordenadas para ordens totais

Consideremos duas ordens totais $(P; \leq_P)$ e $(Q; \leq_Q)$, definidos cf. 3.1.1, (c), e munimos o produto Cartesiano $P \times Q$ com a ordem por coordenadas definida acima. Podemos nós perguntar se esta ordem é uma ordem total no produto. Já sabemos pelo visto anterior que a ordem por coordenadas é uma ordem parcial. Será que ela é uma ordem total? Infelizmente, a ordem por coordenadas não preserva a condição da linearidade. Dê um exemplo mostrando que o produto de duas ordens lineares não é mais linear. Observe que ordens finitas pequenas (com dois ou três elementos) já bastam para exibir este contra-exemplo.

3.2.2 Ordem lexicográfica

Com o resultado anterior, surge a pergunta qual relação proveniente de duas ordens pode manter a linearidade no produto Cartesiano de duas ordens totais? Sejam então $(P; \leq_P)$ e $(Q; \leq_Q)$ ordens totais, cf definição 3.1.1. Considerando o produto Cartesiano $P \times Q$ vamos bolar uma outra relação neste produto Cartesiano. Esta relação chamamos de ordem **lexicográfica** e denotamo-la por $\leq_{lex}$. O nome vem do simples fato que a ordem de uma biblioteca, ou de um dicionário vem desta ordem introduzida em seguinte:

$$\forall \langle p; q\rangle, \langle p'; q'\rangle \in P \times Q, \qquad \langle p; q\rangle \leq_{lex} \langle p'; q'\rangle \quad \text{sse} \quad p <_P p' \quad \text{ou} \quad p = p' \text{ e } q \leq_Q q' \qquad (*)$$

Relembre que definimos $<_P$ de seguinte maneira: Seja $(P; \leq_P)$ uma ordem qualquer, i.e., pré-ordem, ordem parcial ou ordem total, então dizemos que $p <_P p' \quad$ sse $\quad p \leq_P p'$ e $p \neq p'$. Podemos demonstrar que em caso de $(P; \leq_P)$ for ordem parcial, a relação $<_P$ em P é irreflexiva, i.e., $\neg(p <_P p)$, para todo $p \in P$, e é transitiva, i.e., $p <_P p'$ e $p' <_P p''$, implica que $p <_P p''$, para todo $p, p', p'' \in P$. (Exercício)

Agora, temos o seguinte

Fato 3.2.3. *Com as notações acima, $(P \times Q; \leq_{lex})$ é ordem total.*

Prova do Fato: Sejam $(P; \leq_P)$ e $(Q; \leq_Q)$ duas ordens totais. Precisamos demonstrar que a relação $\leq_{lex}$ atende a definição 3.1.1, (c), ou seja, que $\leq_{lex}$ é reflexiva, anti-simétrica, transitiva e total. Vejamos primeiramente que $\leq_{lex}$ é reflexiva. Para isso, seja $\langle p; q\rangle \in P \times Q$. Vamos mostrar que $\langle p; q\rangle \leq_{lex} \langle p; q\rangle$. Pela definição $(*)$, temos que $p \leq_P p$ e $q \leq_Q q$, pois $\leq_P$ e $\leq_Q$ são reflexivas. Logo, a definição $(*)$ é satisfeita, ou seja, $\leq_{lex}$ é reflexiva.
Vejamos então que $\leq_{lex}$ é anti-simétrica, i.e., sejam $\langle p; q\rangle, \langle p'; q'\rangle \in P \times Q$, tais que $\langle p; q\rangle \leq_{lex} \langle p'; q'\rangle$ e $\langle p'; q'\rangle \leq_{lex} \langle p; q\rangle$. Precisamos mostrar que $\langle p; q\rangle = \langle p'; q'\rangle$, ou seja, pelas propriedades de pares ordenadas, cf. [5], $p = p'$ e $q = q'$. Da hipótese $\langle p; q\rangle \leq_{lex} \langle p'; q'\rangle$, temos que $p <_P p' \quad$ ou $\quad p = p'$ e $q \leq_Q q'$. Pela outra hipótese, $\langle p'; q'\rangle \leq_{lex} \langle p; q\rangle$ temos que $p' <_P p \quad$ ou $\quad p' = p$ e $q' \leq_Q q$.
Assim, temos quatro casos, a saber:
Caso 1: $p <_P p'$ e $p' <_P p$. Porém, isto acarreta pela transitividade da relação $<_P$ que $p <_P p$, um absurdo.
Caso 2: $p <_P p'$ e $p' = p$ e $q' \leq q$, o que acarreta de imediato um absurdo, pois $p <_P p'$ implica $p \neq p'$.
Caso 3: $p = p'$ e $q \leq q'$ e $p' <_P p$, o que acarreta de modo análogo um absurdo, como em caso 2.

Caso 4: $p = p'$ e $q \leq_Q q'$ e $p' = p$ e $q' \leq_Q q$. Como a relação $\leq_Q$ é anti-simétrica, temos que $q = q'$, ou seja, este caso mostra que $p = p'$ e $q = q'$.
Observe que com as hipóteses acima, os primeiros três casos não podem entrar. Assim, a relação $\leq_{lex}$ é de fato anti-simétrica.
Deixamos as demonstrações que $\leq_{lex}$ é transitiva e total como tarefas em exercícios. ∎

De modo semelhante como em seção 3.2.1, podemos generalizar ou estender a ordem lexicográfica para um número finito n de ordens totais:
Sejam $(P_1; \leq_1), \ldots, (P_n; \leq_n)$, para algum natural $n \geq 2$, podemos introduzir no produto Cartesiano $(P_1 \times \cdots \times P_n)$ a ordem lexicográfica de maneira natural:
Para $\langle x_1, \ldots, x_n \rangle, \langle y_1, \ldots, y_n \rangle \in P_1 \times \cdots \times P_n$ definimos

$$\begin{aligned}
&\langle x_1, \ldots, x_n \rangle \leq_{lex} \langle y_1, \ldots, y_n \rangle \qquad \text{sse} \\
&\quad x_1 <_1 y_1, \text{ ou} \\
&\quad x_1 = y_1 \text{ e } x_2 <_2 y_2, \text{ ou} \\
&\quad \ldots \text{ , ou} \\
&\quad x_1 = y_1, \ldots, x_{n-1} = y_{n-1} \text{ e } x_n <_n y_n, \text{ ou} \\
&\quad x_1 = y_1, \ldots, x_n = y_n \qquad (**)
\end{aligned}$$

A relação $\leq_{lex}$ definida acima é de fato uma ordem total em $P_1 \times \cdots \times P_n$. Mostre isso ! Obtivemos então o seguinte resultado generalizando o Fato 3.2.1.

Fato 3.2.4. *Com as notações de cima, $(P_1 \times \cdots \times P_n; \leq_{lex})$ é uma ordem total.* ∎

Observação 3.2.5. *A ordem introduzida no Fato anterior é a ordem que ordena uma biblioteca, como também um dicionário. Elabore a definição matemática correta em todos os detalhes para uma biblioteca ou dicionário. É claro que os conjuntos P_i, $i = 1, \ldots, n$ são todos iguais e denotam o alfabeto $\{a, b, c, \ldots, x, y, z\}$ da língua em consideração. Um valor para n de 30 deveria dar para um dicionário em português (existe uma palavra em português com mais de trinta letras?). Qual é a ordem am cada P_i?* ∎

3.3 O princípio da dualidade

Falando de ordem, sempre temos a priori duas ordens, a partir de uma dada. Vejamos isso em mais detalhes. Somente formulamos as idéias para ordens parciais, porém observemos que os comentários a seguir também valem para pré-ordem e ordens totais. Seja $(P; \leq_P)$ uma ordem parcial. De maneira natural podemos introduzir uma ordem *oposta*, $\leq_P^{op}$ no conjunto P:

$$\forall p, q \in P \qquad p \leq_P^{op} q \quad \text{sse} \quad q \leq_P p \qquad (*)$$

A demonstração do seguinte Fato é simples e faz parte dos exercícios:

Fato 3.3.1. *Seja $(P; \leq_P)$ uma ordem parcial. Então, $(P; \leq_P^{op})$ é uma ordem parcial.* ∎

Os argumentos para provar este fato, vêm das propriedades de uma ordem parcial. O último Fato, nós dá além de uma *nova* ordem no conjunto P, vários novos resultados. Isto segue facilmente do seguinte princípio da dualidade:
Consideremos uma linguagem L da lógica de primeira ordem com igualdade e um símbolo de relação $\leq$. Acima desta relação temos os três axiomas dados na definição 3.1.1, (b), isto é, $\leq$ é reflexiva, anti-simétrica e transitiva. Nesta linguagem L podemos formar por recursão as nossas L-fórmulas φ, cf. [5]. Dizemos que esta linguagem é a linguagem da teoria das ordens. Temos agora:

Príncipio da dualidade: Seja φ uma L-fórmula da linguagem da teoria das ordens. Consideremos agora a L-fórmula, φ^{op} qual é obtida de φ, substituindo $\leq$ por $\leq^{op}$. Se soubermos que φ é um teorema, então, φ^{op} também é um teorema na teoria das ordens. ∎

A demonstração deste princípio faz parte da lógica matemática, e é elaborado por *indução sobre a complexidade das L-fórmulas*. Vamos omitir esta demonstração, pelo fato de que precisaríamos alguns conceitos da lógica matemática, qual não conhecemos.
Temos alguns teoremas na teoria das ordens parciais, por exemplo, na seção anterior, vimos que dadas duas ordens parciais, o produto é uma ordem parcial, se consideremos a ordem por coordenadas. Pelo princípio da dualidade, temos um teorema qual não precisamos mais demonstrar – aplicando o princípio da dualidade –, afirmando que a ordem por coordenadas também dá uma ordem parcial, considerando a ordem $\leq^{op}$. No decorrer dos assuntos abordados sobre ordens neste capítulo como no próximo, obtemos mais teoremas desta natureza. Sempre quando isso acontece, mencionamos o princípio da dualidade.

3.4 Diagrama de Hasse

Nesta seção, vejamos que ordens parciais **finitas** podemos desenhar ou melhor representar através de um gráfico. Descrevemos as condições para podermos desenvolver gráficos para ordens parciais, e chamamo-los de **diagramas de Hasse**. Começamos com a seguinte

Definição 3.4.1. *Sejam $(P; \leq_P)$ uma ordem parcial e $x, y \in P$. Dizemos que x* **cobre** *y, y é* **coberto** *por x, $y \multimap_P x$, sse $y <_P x$ e para todo $z \in P$ tal que $y \leq_P z$ e $z \leq_P x$, temos que $y = z$ ou $z = x$.*
Neste caso, também dizemos que x é sucessor imediato de y.

Observação 3.4.2. *Seja $(P; <_P)$ uma ordem parcial. Então, $(P; \multimap_P)$ é irreflexiva. Esta relação é transitiva?* ∎

Com a noção de *cobertura* em elementos de uma ordem parcial P, podemos caracterizar uma diagrama de Hasse na próxima

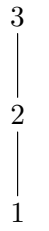
Definição 3.4.3. *Seja $(P; <_P)$ uma ordem parcial finita. Um* **diagrama de Hasse** *para $(P; \leq_P)$ construimos de seguinte maneira:*

(i) cada elemento de P corresponde a um ponto no diagrama,

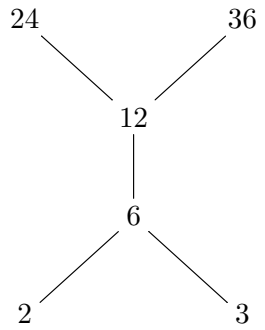
(ii) para elementos $x, y \in P$ tais que $x \leq_P y$, desenhemos o ponto para x em baixo de y, e

(iii) para elementos $x, y \in P$ tais que $x \multimap_P y$, desenhemos uma linha de x para y, ou seja, conectemos x com y.

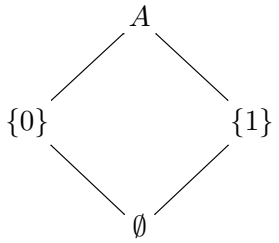
Exemplo 3.4.4. *(a) Consideremos a ordem total $\leq_{\mathbb{N}}$ nos naturais sobre o conjunto $\{1, 2, 3\}$, ou seja, consideremos uma cadeia de três elementos. Podemos usando a definição 3.4.3, elaborar o diagrama de Hasse para esta cadeia de três elementos e obtemos:*



(b) Consideremos o conjunto $A := \{2, 3, 6, 12, 24, 36\}$ com a ordem da divisibilidade $|$. O seu diagrama de Hasse é a seguinte:



(c) Consideremos o conjunto $A := \{0, 1\}$ e a ordem parcial $(\mathcal{P}(A); \subseteq)$. Obtemos o seguinte diagrama de Hasse:



Como exercício, desenhe os diagramas de Hasse de $(\mathcal{P}(A); \subseteq)$, em caso de $A := \emptyset$ e $A := \{0, 1, 2\}$. Também desenhe para $2 := \{0, 1\}$ com $0 \leq 1$, o diagrama da ordem produto $(2^2; \leq)$ e $(2^3; \leq)$, onde $\leq$ denota a ordem por coordenadas introduzida em 3.2.1. ∎

Questão 3.4.5. *É possível desenhar os diagramas de Hasse do exemplo 3.4.4, considerando a ordem oposta! Exibe os diagramas!*

3.5 Alguns elementos especiais em ordens parciais

Nesta seção, queremos introduzir alguns elementos especiais importantes em ordens parciais, como maior, menor, maximal e minimal. Vejamos em seguida que nem sempre elementos especiais vão existir.

Definição 3.5.1. *Seja $(P; \leq_P)$ uma ordem parcial.*
(a) Dizemos que $x \in P$ é **menor (ou primeiro) elemento** *de P sse para todo $p \in P$, $\quad x \leq_P p$.*

(b) Dizemos que $x \in P$ é **maior (ou último) elemento** *de P sse para todo $p \in P$, $\quad p \leq_P x$.*

Observação 3.5.2. *(a) Observe que pelo princípio da dualidade, cf. 3.3, temos a seguinte equivalência: Sejam $(P; \leq_P)$ uma ordem parcial e $x \in P$,*

$$x \text{ é maior elemento em } (P; \leq_P) \quad \text{sse} \quad x \text{ é menor elemento em } (P; \leq_P^{op}).$$

(b) Existem ordens parciais quais não tem elemento menor e/ou elemento maior. Dê exemplos!
(c) Os elementos menor e maior são únicos, caso existirem.

Demonstração: Vamos somente demonstrar o ítem (c), deixando os primeiros dois ítens como exercício. Sejam $t, s \in P$ dois elementos menores. Vamos demonstrar que $t = s$. Como t é menor elemento, temos que

$$\forall p \in P, \quad t \leq_P p, \text{ e em particular } t \leq_P s \quad .$$

Como s é menor elemento temos pela mesma razão que $s \leq_P t$, e aplicando a propriedade da anti-simetria, é preciso que $t = s$, terminando a prova. Usando o princípio da dualidade temos como resultado adicional que também o maior elemento, caso exista, é único. ∎

Notação 3.5.3. *Em ordens, denotamos caso existirem, o menor elemento por $\bot$ e o maior elemento por $\top$. Estas notações vem da lógica matemática, onde $\bot$ denota o* **falso***, e o $\top$ denota a* **tautologia***. Em alguns livros, encontramos também 0 para menor elemento e 1 para maior elemento.*

Exemplo 3.5.4. *Reconsideremos o exemplo 3.4.4, perguntamos sobre o elemento especial, menor e maior, introduzidos em 3.5.1.*
(a) Em conjunto $\{1,2,3\}$ com a ordem $\leq_N$ temos que 1 é o menor elemento e 3 é o maior elemento.
(b) Reconsiderando $(A;|)$ de 3.4.4 (b), vejamos que nesta ordem não temos menor nem maior elemento. Para o caso de um possível menor elemento, observemos que os candidatos são 2 e 3, porém estes dois elementos não são comparáveis na ordem da divisibilidade $|$, i.e., $2 \not| 3$ e $3 \not| 2$. Logo, não existe menor elemento. A mesma argumentação se aplica para um possível maior elemento.
(c) Reconsiderando $(\mathcal{P}(A);\subseteq)$ de 3.4.4 (c), vejamos que nesta ordem temos menor e maior elemento, a saber $\emptyset$ é o menor elemento e A é o maior elemento.
(d) Consideremos o ítem (b) novamente e definimos $B := A \cup \{1\}$, então é fácil ver que 1 é menor elemento, enquanto o maior elemento não existe. ∎

Definição 3.5.5. *Seja $(P;\leq_P)$ uma ordem parcial.*
(a) Dizemos que $x \in P$ é **elemento minimal** *de P sse para todo $p \in P$, $\quad p \leq_P x \ \rightarrow \ x = p$.*
(b) Dizemos que $x \in P$ é **elemento maximal** *de P sse para todo $p \in P$, $\quad x \leq_P p \ \rightarrow \ x = p$.*

Deixamos a demonstarção da próxima observação como exercício.

Observação 3.5.6. *(a) Observe que pelo princípio da dualidade, cf. 3.3, temos a seguinte equivalência: Sejam $(P;\leq_P)$ uma ordem parcial e $x \in P$,*

$$x \text{ é elemento maximal em } (P;\leq_P) \quad \text{sse} \quad x \text{ é elemento minimal em } (P;\leq_P^{op}).$$

(b) Existem ordens parciais quais não tem elemento minimal e/ou elemento maximal. Dê exemplos!
(c) Os elementos minimal e maximal não são únicos, caso existirem. ∎

Exemplo 3.5.7. *Reconsideremos o exemplo 3.4.4, perguntamos sobre o elemento especial, minimal e maximal, introduzidos em 3.5.5.*
(a) Em conjunto $\{1,2,3\}$ com a ordem $\leq_{\mathbb{N}}$ temos que 1 é o elemento minimal e 3 é o elemento maximal.
(b) Reconsiderando $(A;|)$ de 3.4.4 (b), vejamos que nesta ordem temos dois elementos maximais. Os elementos maximais são 24 e 36, pois estes verificam a definição 3.5.5. Logo, 24 e 36 são os elementos maximais em A. Pela mesma argumentação vejamso que 2 e 3 são os elementos minimais em A.
(c) Reconsiderando $(\mathcal{P}(A);\subseteq)$ de 3.4.4 (c), vejamos que nesta ordem os elementos minimal e maximal são menor e maior elemento, respectivamente, a saber $\emptyset$ é o menor elemento e A é o maior elemento.
(d) Consideremos o ítem (b) novamente e definimos $B := A \cup \{1\}$, então é fácil ver que 1 é elemento minimal, enquanto os elementos maximais continuam sendo os mesmos, 24 e 36. ∎

Capítulo 4

Introdução à teoria dos reticulados

Nesta seção, queremos introduzir o conceito de reticulado via ordem e demonstrar alguns conceitos básicos acerca de reticulados. O conceito de reticulado pode ser definida também *algebricamente* e vejamos que as duas abordagens, uma vez via ordem, outra vez, via álgebra, tem o mesmo conceito como resultado. Reticulados são ordens parciais especiais, ou seja, são ordens parciais com propriedades interessantes, e reticulados acontecem em várias áreas da matemática, como da ciência da computação. Estes assuntos são abordados na literatura, veja por exemplo, [6], [8], [11] e [12].

4.1 Barreiras superiores e inferiores

Para podermos entender estas ordens específicas, chamados de *reticulados* precisamos esclarecer barreiras superior e inferior, o que faremos na próxima

Definição 4.1.1. *Sejam $(P; \leq_P)$ uma ordem parcial e $Q \subseteq P$ um subconjunto de P.*
(a) Dizemos que $x \in P$ é uma **barreira superior para** *Q sse $\forall y \in Q, \quad y \leq_P x$.*

(b) Dizemos que $x \in P$ é uma **barreira inferior para** *Q sse $\forall y \in Q, \quad x \leq_P y$.*

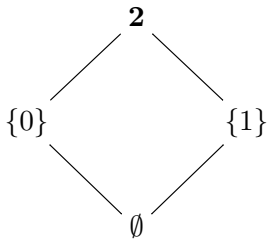
Observação 4.1.2. *(a) Observe que os conceitos (a) e (b) da última definição 4.1.1 são* **duais** *no sentido do nosso princípio da dualidade, cf. 3.3.*
(b) Na definição 4.1.1 anterior, tomando $Q := P$, os conceitos (a) e (b), coincidem com **maior** *e* **menor** *elementos, cf. 3.5.1, respectivamente.*
(c) É claro que barreiras superiores, como inferiores não necessariamente sempre existem, nem são em caso da existência únicos, ou seja, podem existir mais do que uma barreiras superiores como inferiores para um subconjunto B de P dado.

Demonstração: fica como exercício. ∎

Questão 4.1.3. *Considerando a definição 4.1.1, esta faz sentido para $Q := \emptyset$? Caso afirmativo, quais são as barreiras superiores de $\emptyset$, e quais as inferiores?*

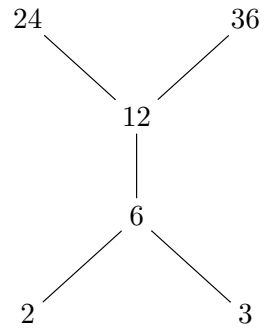
Vejamos um exemplo que trata os conceitos novos de 4.1.1:

Exemplo 4.1.4. *(a) Consideremos $\mathbf{2} := \{0, 1\}$ e a ordem parcial $(\mathcal{P}(\mathbf{2}); \subseteq)$. Pelo exemplo 3.4.4, temos o seguinte diagrama de Hasse:*



Considerando $Q \subseteq \mathcal{P}(\mathbf{2})$, definido como $Q := \{\{0\}; \mathbf{2}\}$, podemos calcular
(i) as barreiras superiores de Q, e obtemos que somente $\mathbf{2}$ é barreira superior de Q, e
(ii) as barreiras inferiores de Q, e obtemos que somente $\emptyset, \{0\}$ são as barreiras inferiores de Q.

(b) Considerando o exemplo 3.4.4, (b), temos o conjunto $A := \{2, 3, 6, 12, 24, 36\}$ com a ordem da divisibilidade $|$. O seu diagrama de Hasse é a seguinte:



Considerando $Q \subseteq A$, definido como $Q := \{2, 3, 6\}$, podemos calcular
(i) as barreiras superiores de Q, e obtemos que os elementos $6, 12, 24$ e 36 são barreiras superiores de Q, e
(ii) as barreiras inferiores de Q, e obtemos que não temos nenhuma barreira inferior de Q em A.

(c) Consideremos então a ordem linear $\mathbb{N}; \leq_{\mathbb{N}})$, onde $\mathbb{N}$ denota a ordem usual de menor ou igual entre naturais. O diagrama de Hasse é uma cadeia infinita.
Consideremos então $Q := \mathbb{N} \setminus \{0, 1, 2\}$, e determinamos que não temos barreira superior para Q em $\mathbb{N}$. Não é difícil de verificar que $0, 1$ e 2 são as barreiras inferiores de Q.

Observe que os diagramas de Hasse de fato podem facilitar a procura das barreiras. ∎

Com estes preliminários, podemos introduzir o importante conceito de supremo e infimo na próxima definição.

Definição 4.1.5. *Sejam $(P; \leq_P)$ uma ordem parcial e $Q \subseteq P$ um subconjunto de P.*
(a) Dizemos que $x \in P$ é **menor barreira superior para** *Q, ou equivalentemente, o* **supremo** *de Q, $\sup Q$, $\bigvee Q$, sse*

(i) x é barreira superior para Q, e

(ii) entre todas as barreiras superiores de Q, x é a menor, ou seja, $\forall y \in P,$ se y for barreira superior de Q, então $x \leq_P y$.

(b) Dizemos que $x \in P$ é **maior barreira inferior para** *Q, ou equivalentemente, o* **infimo** *de Q, $\inf Q$, $\bigwedge Q$, sse*

(i) x é barreira inferior para Q, e

(ii) entre todas as barreiras inferiores de Q, x é a maior, ou seja, $\forall y \in P,$ se y for barreira inferior de Q, então $y \leq_P x$.

Temos uma observação parecida de 4.1.2 formulada em

Observação 4.1.6. *(a) Observe que os conceitos (a) e (b) da última definição 4.1.1 são* **duais** *no sentido do nosso princípio da dualidade, cf. 3.3: (a) é o dual de (b) e (b) é o dual de (a).*
(b) Na definição 4.1.1 anterior, tomando $Q := P$, os conceitos (a) e (b), coincidem com **menor** *e* **maior** *elementos, cf. 3.5.1, respectivamente.*
(c) É claro que supremo, como infimo não necessariamente sempre existem, porém em caso da existência de cada um, eles são únicos.

Demonstração: como exercício. ∎

Reconsideremos o exemplo 4.1.4 e perguntamos sobre possíveis supremos e infimos:

Exemplo 4.1.7. *(a) Consideremos $\mathbf{2} := \{0, 1\}$ e a ordem parcial $(\mathcal{P}(\mathbf{2}); \subseteq)$ com o diagrama de Hasse dado anteriormente. Considerando $Q \subseteq \mathcal{P}(\mathbf{2})$, definido como $Q := \{\{0\}; \mathbf{2}\}$, podemos calcular*
(i) o supremo de Q, $\sup Q$, e obtemos que $\sup Q = \mathbf{2}$, e
(ii) o infimo de Q, $\inf Q$, e obtemos que $\inf Q = \{0\}$.

(b) Considerando o exemplo 3.4.4, (b), temos o conjunto $A := \{2, 3, 6, 12, 24, 36\}$ com a ordem da divisibilidade $|$ e o diagrama de Hasse dado anteriormente. Considerando $Q \subseteq A$, definido como $Q := \{2, 3, 6, 12\}$, queremos calcular
(i) o supremo de Q, $\sup Q$, porém $\sup Q$ não existe, e
(ii) o infimo de Q, $\inf Q$, qual também não existe.
Observe que o supremo de Q não existe, pois as barreiras superiores de Q, a saber, 24 e 36, não são comparáveis, e consequentemente, não pode existir uma menor barreira, enquanto o infimo de Q não existe, pois não existe nenhuma barreira inferior de Q em A, e logo não pode existir uma maior.

(c) Consideremos então a ordem linear $(\mathbb{N}; \leq_{\mathbb{N}})$, onde $\mathbb{N}$ denota a ordem usual de menor ou igual entre naturais. O diagrama de Hasse para esta ordem é uma cadeia infinita.
Consideremos então $Q := \mathbb{N} \setminus \{0, 1, 2\}$, e temos que não existe $\sup Q$ em $\mathbb{N}$, porém temos o infimo de Q, dado por $\inf Q = 2$. ∎

Definição 4.1.8. *Seja $(P; \leq_P)$ uma ordem parcial.*
(a) Dizemos que P é limitado superiormente sse existe maior elemento em P, cf. 3.5.1.

(b) Dizemos que P é limitado inferiormente sse existe menor elemento em P, cf. 3.5.1.

(c) Dizemos que P é limitado sse P é limitado superior e inferiormente.

A seguinte observação é simples para demonstrar:

Observação 4.1.9. *Seja $(P; \leq_P)$ uma ordem parcial. São equivalentes:*
(a) P é limitado, e b) P tem barreiras superior e inferior. ∎

Vamos comparar os conceitos importantes em ordens e seus duais quais introduzimos nesta seção e em 3.5 na seguinte tabela:

$\leq$	$\leq^{op}$
elemento maior	elemento menor
elemento maximal	elemento minimal
barreira superior	barreira inferior
supremo	infimo
limitado superiormente	limitado inferiormente

A leitura da tabela é feito de seguinte modo: Se numa ordem parcial com a ordem $\leq$, temos um elemento maior, este é menor na ordem $\leq^{op}$, ou também, se uma ordem $(P; \leq_P)$ é limitada superiormente, então $(P; \leq_P^{op})$ é limitado inferiormente.

O próximo resultado é importante e será usado sem mencionar em seguida.

Proposição 4.1.10. *Seja A um conjunto arbitrário e consideremos a ordem parcial $(\mathcal{P}(A); \subseteq)$. Seja $B \subseteq \mathcal{P}(A)$ então temos que*
(a) $\inf(B) = \bigcap B := \{x \in A| \quad \forall y(y \in B \ \rightarrow \ x \in y)\}$, *e*
(b) $\sup B = \bigcup B := \{x \in A| \quad \exists y(y \in B \ \& \ x \in y)\}$.

Demonstração: Vamos mostrar o ítem (a) e deixamos (b) como exercício.[1] Consideremos a ordem parcial $(\mathcal{P}(A); \subseteq)$ e um subconjunto $B \subseteq \mathcal{P}(A)$. Obviamente precisamos verificar 4.1.5, (b).
Primeira parte: Mostramos que $\bigcap B$ é de fato uma barreira inferior de B, ou seja, $\bigcap B \subseteq y, \forall y \in B$. Agora, tome $x \in \bigcap B$, então, $x \in y \ \forall y \in B$. Logo, $\bigcap B$ é barreira inferior de B.
Segunda parte: Mostramos que $\bigcap B$ é maior barreira inferior de B. Para isso, seja $z \in \mathcal{P}(A)$ uma barreira inferior de B, isto é, $z \subseteq y, \forall y \in B$. Precisamos mostrar que $z \subseteq \bigcap B$. Tome $w \in z$, então como $z \subseteq y$, $\forall y \in B$, temos que $w \in y, \forall y \in B$. Mas assim, $w \in \bigcap B$, e portanto, $z \subseteq \bigcap B$. ∎

4.2 Reticulados via ordem

Nesta seção introduzimos ordens parciais especiais, os reticulados, como também semi-reticulados.

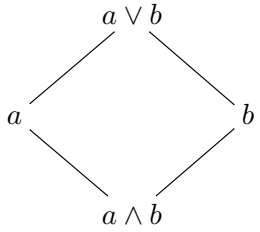
Definição 4.2.1. *Seja $(P; \leq_P)$ uma ordem parcial.*
(a) Dizemos que P é um **semi-reticulado** *sse para cada dois elementos de P, existe o infimo deles em P, i.e., $\forall a, b \in P$, existe $\inf\{a; b\} \in P$, em notação $(a \wedge b) \in P$.*

(b) Dizemos que P é um $\vee$- **semi-reticulado** *sse para cada dois elementos de P, existe o supremo deles em P, i.e., $\forall a, b \in P$, existe $\sup\{a; b\} \in P$, em notação $(a \vee b) \in P$.*

(c) Dizemos que P é um **reticulado** *sse para cada dois elementos de P, existe supremo e infimo deles em P, i.e., $\forall a, b \in P$, existem $(a \wedge b), (a \vee b) \in P$.*

(d) Dizemos que P é um **reticulado limitado** *sse P é reticulado e $(P; \leq_P)$ é limitado, cf. 4.1.8.*

Observação 4.2.2. *(a) Seja $A \neq \emptyset$ uma família de conjuntos fechados por interseção e união*[2]*. Então, A é um reticulado.*
(b) Uma ordem linear sempre tem estrutura de reticulado.
(c) Existem ordens parciais quais não são reticulados.
(d) Sejam $(P; \leq_P)$ um reticulado e $a, b \in P$. Então temos que $a, b \leq_P a \vee b$ e $a \wedge b \leq_P a, b$. Temos o seguinte diagrama de Hasse:



Demonstração: Os primeiros dois ítens são demonstrados em exercícios. No exemplo 3.4.4, (b), não existe $\sup\{24; 36\}$, e assim $A := \{2, 3, 6, 12, 24, 36\}$ com a ordem parcial | não é um reticulado, verificando (c). O ítem (d) é trivial, pois pela definição de supremo, temos que $a, b \leq_P a \vee b$, e pelo princípio da dualidade, $a \wedge b \leq_P a, b$, mostrando (d). ∎

[1] Observe que ítem (b) segue também do princípio da dualidade. Faça estes detalhes!

[2] Relembre que uma família $A := \{a_i\}_{i \in I}$ de conjuntos é fechado por união e interseção sse $\forall J \subseteq I$, $\bigcup_{j \in J} a_j \in A$ e $\bigcap_{j \in J} a_j \in A$.

Exemplo 4.2.3. *(a) Seja A um conjunto e consideremos a ordem parcial $(\mathcal{P}(A);\subseteq)$. Como $\mathcal{P}(A)$ é fechado por união e interseção $(\mathcal{P}(A);\subseteq)$ é um reticulado. Além disso, este reticulado tem menor e maior elemento: Observe que $\emptyset \subseteq B$ e $B \subseteq A$, $\forall B \subseteq A$. Assim, $\emptyset$ é menor elemento e A é maior elemento em $\mathcal{P}(A)$.*

(b) Consideremos $(\mathbb{N};\leq_{\mathbb{N}})$ e $(\mathbb{Z};\leq_{\mathbb{Z}})$, onde as ordens $\leq_{\mathbb{N}}$ e $\leq_{\mathbb{Z}}$ são as ordens de menor ou igual natural nos naturais e inteiros, respectivamente. Sabemos que estas ordens são lineares e por observação 4.2.2, temos então reticulados. $\mathbb{N}$ é limitado inferiormente pelo elemento 0, porém é fácil ver que não temos em nenhum destes reticulados elemento maior, como em $\mathbb{Z}$ não tem nem elemento menor.

(c) Consideremos $(\mathbb{N}^*;|)$, onde $\mathbb{N}^* := \mathbb{N}\setminus\{0\}$. Sabemos que a divisibilidade $|$ em $\mathbb{N}^*$ é uma ordem parcial. Podemos perguntar, se $(\mathbb{N}^*;|)$ tem estrutura de reticulado? Temos o seguinte

Fato 4.2.4. *Sejam $m,n\in\mathbb{N}^*$. Então, $\inf\{m;n\} = mdc(m;n)$ e $\sup\{m;n\} = mmc(m;n)$.*

Prova do Fato: Sejam $m,n\in\mathbb{N}^*$. Sabemos pela teoria dos números que $mdc(m;n)$ existe em $\mathbb{N}^*$. Denotamos este mdc por $d := mdc(m;n)$ e mostramos que d satisfaz definição 4.1.5, (b). Para isso, sabemos por proposição 2.3.6, que $d|m$ e $d|n$, mostrando que d é barreira inferior de m e n. Também por 2.3.6, temos que para qualquer $d'\in\mathbb{N}^*$ tal que $d'|m$ e $d'|n$, temos que $d'|d$. Mas esta exigência é exatamente a propriedade de d é maior barreira entre as barreiras inferiores. Logo, $\inf\{m;n\} = mdc(m;n)$.
Usando o princípio da dualidade e a definição 2.3.13, temos que $\sup\{m;n\} = mmc(m;n)$, terminando a demonstração do Fato.

Usando 4.2.4, concluimos que $(\mathbb{N}^*;|)$ é um reticulado. Observemos que este reticulado é limitado inferiormente, pois para todo $n\in\mathbb{N}^*$, temos que $1|n$, mostrando que 1 é menor elemento. Por outro lado, não existe um maior elemento em $\mathbb{N}^*$. ∎

Observação 4.2.5. *É imediato que sendo $(P;\leq_P)$ um reticulado, cf. 4.2.1, então $(P;\leq_P^{op})$ também é um reticulado. O diagrama de Hasse para $(P;\leq_P^{op})$, é obtido do diagrama para $(P;\leq_P)$, simplesmente "virando o diagrama de cabeça para baixo".* ∎

Em seguida, mostramos algumas propriedades dos supremo e infimo em reticulados. Estas propriedades são importantes e podem ser usados em considerações futuras.

Lema 4.2.6. *Sejam $(P;\leq_P)$ um reticulado um $x,y,z\in P$ elementos. Então,*
$(R_{0\wedge})$ $(x\wedge x)=x$ *e* $(R_{0\vee})$ $(x\vee x)=x$.
$(R_{1\wedge})$ $x\wedge y = y\wedge x$ *e* $(R_{1\vee})$ $x\vee y = y\vee x$.
$(R_{2\wedge})$ $(x\wedge y)\wedge z = x\wedge(y\wedge z)$ *e* $(R_{2\vee})$ $(x\vee y)\vee z = x\vee(y\vee z)$.
$(R_{3\wedge})$ $x = x\wedge(x\vee y)$ *e* $(R_{3\vee})$ $x = x\vee(x\wedge y)$.

Observação 4.2.7. *(i) Dizemos a propriedade mencionada em $(R_{0\wedge})$ é que $\wedge$ é idempotente. Analogamente, em $(R_{0\vee})$, $\vee$ é idempotente.*
(ii) Dizemos a propriedade mencionada em $(R_{1\wedge})$ é que $\wedge$ é comutativo. Analogamente, em $(R_{1\vee})$, $\vee$ é comutativo.
(iii) Dizemos a propriedade mencionada em $(R_{2\wedge})$ é que $\wedge$ é associativo. Analogamente, em $(R_{2\vee})$, $\vee$ é associativo.
(iv) Dizemos a propriedade mencionada em $(R_{3\wedge})$ e em $(R_{0\vee})$ é lei da **absorção**.
(v) Obviamente, $(R_{j\wedge})$ e $(R_{j\vee})$, para $j=0,1,2,3$, são conceitos duais, cf 3.3. ∎

Demonstração do Lema 4.2.6: Sejam $(P;\leq_P)$ um reticulado um $x,y,z\in P$ elementos. Pela última observação temos da validade de $(R_{j\wedge})$ a validade de $(R_{j\vee})$, para qualquer $j=0,1,2,3$. Assim, somente precisamos mostrar $(R_{j\wedge})$, para todo $j=0,1,2,3$. Começando com $(R_{1\wedge})$: Observe que $x\wedge x\leq_P x$, pela definição do infimo. Por outro lado, temos pela reflexividade de $\leq_P$, que $x\leq_P x$. Logo, x é barreira inferior de x. Porém $x\wedge x$ é maior barreira inferior de x, e consequentemente, $x\leq_P x\wedge x$. Pela anti-simétria de

$\leq_P$, temos que $x = x \wedge x$.
Usando a observação 4.2.2, temos que $x \wedge y \leq_P x, y$. Assim, $x \wedge y$ é barreira inferior de y e x, porém $y \wedge x$ é maior barreira inferior de y e x. Portanto, $x \wedge y \leq_P y \wedge x$. Analogamente, mostramos que $y \wedge x \leq_P x \wedge y$. Pela anti-simetria, $x \wedge y = y \wedge x$, verificando $(R_{1\wedge})$.
Vejamos então $(R_{2\wedge})$. Observe que $(x \wedge y) \wedge z \leq_P x \wedge y \leq_P x, y$ e $(x \wedge y) \wedge z \leq_P z$. Portanto $(x \wedge y) \wedge z$ é barreira inferior de y e z. Sendo $y \wedge z$ maior barreira superior, precisamos ter $(x \wedge y) \wedge z \leq_P y \wedge z$. Por outro lado, $(x \wedge y) \wedge z$ é barreira inferior de $y \wedge z$ e x, o que implica que $(x \wedge y) \wedge z \leq_P x \wedge (y \wedge z)$. De modo analogo, mostramos que $x \wedge (y \wedge z) \leq_P (x \wedge y) \wedge z)$, o que acarreta pela anti-simetria a igualdade e portanto $(R_{2\wedge})$.
Resta mostrar a absorção. A desigualdade $x \wedge (x \vee y) \leq_P x$ é imediato. Por outro lado, temos que $x \leq_P x$ e $x \leq_P x \vee y$. Assim, x é barreira inferior de x e $x \vee y$. Como $x \wedge (x \vee y)$ é maior entre as barreiras, é preciso que $x \leq_P x \wedge (x \vee y)$. Pela anti-simetria temos novamente a igualdade e assim estabelecemos a lei da absorção. ∎

O próximo resultado conecta o conceito de ordem com os conceitos de infimo e supremo. Este lema é importante e pode ser aplicado em questões envolvendo ordem e supremo ou infimo.

Lema 4.2.8. *(Lema da Conexão) Sejam $(P; \leq_P)$ um reticulado um $x, y \in P$ elementos. Então são equivalentes:*

$$\textit{(a) } x \leq_P y, \quad \textit{(b) } x = x \wedge y \quad \textit{e} \quad \textit{(c) } y = x \vee y.$$

Demonstração: Com as hipóteses do lema, sejam $(P; \leq_P)$ um reticulado e $x, y \in P$ elementos.
$\underline{(a) \Rightarrow (b)}$: Seja $x \leq_P y$. Observe que $x \leq_P x$, e por hipótese, $x \leq_P y$, o que implica ($x \wedge y$ é o infimo!) $x \leq_P x \wedge y$. Como sempre temos que $x \wedge y \leq_P x$, cf 4.2.2, e assim $x = x \wedge y$.
$\underline{(b) \Rightarrow (c)}$: Seja agora $x = x \wedge y$. Fazemos uso do lema 4.2.6 e calculemos
$x \vee y = (x \wedge y) \vee y =_{(R_{1\vee})} y \vee (x \wedge y) =_{(R_{1\wedge})} y \vee (y \wedge x) =_{(R_{3\vee})} y$.
$\underline{(c) \Rightarrow (a)}$: Seja $y = y \vee x$. Então temos que $x \leq_P (x \vee y) = y$, por 4.2.2. ∎

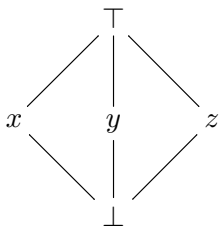
Introduzimos em seguida reticulados de grande importância na teoria, que satisfazem as leis de distributividade.

Definição 4.2.9. *Seja $(P; \leq_P)$ um reticulado. Dizemos que $(P; \leq_P)$ é* **distributivo** *sse $\forall x, y, z \in P$ temos que*
(i) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, e
(ii) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Observação 4.2.10. *(a) Em definição 4.2.9, temos que (i) e (ii) são logicamente equivalentes.*
(b) Existem reticulados não distributivos.

Demonstração: Vejamos o ítem (a) e somente que (ii) implica (i). A parte (i) implica (ii) fica como exercício – observe que uma aplicação do princípio da dualidade também mostra (i) implica (ii), supondo mostrado (ii) implica (i). Usando a hipótese, eventualmente comutatividade e associatividade ccomo as leis da absorção $(R_{3\wedge})$ e $(R_{3\vee})$ obtemos que
$(x \wedge y) \vee (x \wedge z) = [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] = x \wedge [(x \wedge y) \vee z] = x \wedge [z \vee (x \wedge y)] = x \wedge [(z \vee x) \wedge (z \vee y)] = x \wedge (y \vee z)$, mostrando o ítem (i).

Para o ítem (b) exibimos um reticulado importante em forma de diagrama de Hasse qual não é distributivo: O primeiro diagrama representa o reticulado $M3$:



É fácil a verificação que este reticulado não é distributivo. Tome x, y, z conforme o diagrama e observe que $x \wedge y = \bot = x \wedge z$. Por outro lado, $y \vee z = \top$ e $x \wedge (y \vee z) = x \wedge \top = x >_P \bot = (x \wedge y) \vee (x \wedge z)$, mostrando que não vale 4.2.9, (i). Observemos ainda que este reticulado $M3$ ocorre, por exemplo, visto o conjunto das partições de um conjunto de três elementos como reticulado. Outro reticulado não distributivo é chamado de $N5$ e devemos introduzi-lo em aula. A diferença grande de $M3$ e $N5$ é devido ao fato que $M3$ é modular, enquanto $N5$ não o é. ∎

Vimos então que existem reticulados quais não são distributivos, porém todo reticulado sempre satisfaz as desigualdades distributivas mencionadas no próximo

Lema 4.2.11. *Seja $(P; \leq_P)$ um reticulado. Então temos para todo $x, y, z \in P$,*
(a) $(x \wedge y) \vee (x \wedge z) \leq_P x \wedge (y \vee z)$, e (b) $x \vee (y \wedge z) \leq_P (x \vee y) \wedge (x \vee z)$.

Demonstração: Observe que os dois ítens são duais pelo princípio da dualidade. Assim, somente precisamos mostrar o ítem (a), pois (b) segue da dualidade. Sejam para isso $x, y, z \in P$ elementos de P. Observe que $x \wedge y \leq_P y \leq_P x \vee y$, como também $x \wedge z \leq_P z \leq_P y \vee z$, mostrando que $y \vee z$ é barreira superior de $(x \wedge y)$ e $(x \wedge z)$. Como o supremo entre esses dois é a menor barreira superior temos que e $(x \wedge y) \vee (x \wedge z) \leq_P y \vee z$. Porém é imediato, cf. 4.2.2 que $(x \wedge y)$ e $(x \wedge z)$ são barreiras superiores de x, e portanto $(x \wedge y) \vee (x \wedge z) \leq_P x$. Logo, $(x \wedge y) \vee (x \wedge z)$ é barreira inferior de x e $y \vee z$. Sendo o infimo destes dois a maior barreira, temos que $(x \wedge y) \vee (x \wedge z) \leq_P x \wedge (y \vee z)$, mostrando a primeira desigualdade distributiva. ∎

A questão de "quando um reticulado é distributivo" foi respondido por G. Birkhoff:

Teorema 4.2.12 (Birkhoff)**.** *Seja A um reticulado. São equivalentes:*
(a) A é distributivo,
(b) A não contém subreticulado (cf. 4.4.1) isomorfo (i.e., com a mesma estrutura de) $M3$ ou $N5$. ∎

Uma demonstração pode ser encontrada no livro de Davey e Priestley, [6] e temos que fazer algumas contas para mostrar (b) implica (a), sendo (a) implica (b) demonstrado facilmente pela contra-positiva. ∎

4.3 Reticulados via álgebra

Nesta seção definimos reticulados usando o conceito de álgebra, e mostramos que as duas definições de reticulados são equivalentes. Começamos com a noção de álgebra.

Definição 4.3.1. *Dizemos que $\mathfrak{A} := (A; \{f_j\}_{j \in I})$ é uma* **álgebra** *sse o conjunto A, chamado de* **suporte** *ou* **domínio** *é não vazio e para cada $j \in I$, f_j é uma operação n_j-ária em A, i.e., $f_j : A^{n_j} \to A$ é função.*

Exemplo 4.3.2. *(a) Consideremos $\mathfrak{N} := (\mathbb{N}; +_{\mathbb{N}}, 0_{\mathbb{N}})$. Então temos uma álgebra, pois sabemos que $\mathbb{N} \neq \emptyset$. Aém disso, a constante $0_{\mathbb{N}}$ é uma função 0-ária, i.e., $0_{\mathbb{N}} : \mathbb{N}^0 := \{\star\} \to \mathbb{N}, 0_{\mathbb{N}}(\star) := 0$. O símbolo $+_{\mathbb{N}}$ é seguinte função binária: $+_{\mathbb{N}} : \mathbb{N}^2 \to \mathbb{N}, \langle m; n\rangle \mapsto +_{\mathbb{N}}(\langle m; n\rangle) := m + n$.*

(b) Consideremos $\mathfrak{Z} := (\mathbb{Z}; +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}})$, então temos a álgebra dos números inteiros tratados em capítulo 1. Demonstre em detalhe que de fato temos uma álgebra.

(c) Consideremos uma linguagem L da lógica proposicional, [5], sabemos como gerar as L-fórmulas $\varphi \in Form(L)$. Porém podemos ver matematicamente $Form(L)$ como a seguinte álgebra:
Seja $\mathfrak{F} := (Form(L); \wedge_L, \to_L, \vee_L, \neg_L, \bot_L, \top_L)$, onde as operações $\wedge_L, \vee_L$ e $\to_L$ são binárias, $\neg_L$ é unário e as operações $\bot_L, \top_L$ são 0-árias. As definições das operações são simplesmente dados pelos conectivos lógicos. Por exemplo, temos que
$\bot_L : From(L)^0 \to Form(L), \star \mapsto \bot_L(\star) := \bot$, *onde* $From(L)^0 := \{\star\}$.
$\top_L : From(L)^0 \to Form(L), \star \mapsto \top_L(\star) := \top$.

$\neg_L : From(L) \to Form(L), \varphi \mapsto \neg_L(\varphi) := \neg(\varphi)$.
$\wedge_L : From(L)^2 \to Form(L), \langle\varphi;\psi\rangle \mapsto \wedge_L(\langle\varphi;\psi\rangle) := \varphi \wedge \psi$.
$\vee_L : From(L)^2 \to Form(L), \langle\varphi;\psi\rangle \mapsto \vee_L(\langle\varphi;\psi\rangle) := \varphi \vee \psi$.
$\to_L$: $From(L)^2 \to Form(L), \langle\varphi;\psi\rangle \mapsto \to_L (\langle\varphi;\psi\rangle) := \varphi \to \psi$.

(d) Dê exemplos para outras álgebras! Pense em noções matemáticas e observe que existem muitas álgebras: espaço vetorial, semi-grupo, monóide, grupo, anel etc. ∎

O alvo é introduzir uma definição de um tipo de álgebra que é um reticulado, ou seja, satisfaz as exigências de reticulado estabelecido em definição 4.2.1. Temos a seguinte

Definição 4.3.3. *Dizemos que uma álgebra $\mathfrak{L} := (A; \wedge_A, \vee_A)$, onde as operações $\wedge_A$ e $\vee_A$ são binárias e satisfazem os oito axiomas $(R_{j\wedge})$ e $(R_{j\vee})$, para $j = 0, 1, 2, 3$, dados em lema 4.2.6, é um* **reticulado**.

Proposição 4.3.4. *As definições 4.2.1 e 4.3.3 definem o mesmo conceito, ou seja, são equivalentes.*

Demonstração: Vamos fazer a demonstração em duas partes.

Primeira parte: Seja $(P; \leq_P)$ um reticulado conforme definido em 4.2.1. Vamos mostrar que $(P; \leq_P)$ satisfaz as condições da definição 4.3.3. Conforme o lema 4.2.6 valem as condições da definição 4.3.3 e esta parte é demonstrada.

Segunda parte: Seja $\mathfrak{L} := (A; \wedge_A, \vee_A)$ a álgebra dada na definição 4.3.3 satisfazendo os oito axiomas $(R_{j\wedge})$ e $(R_{j\vee})$, para $j = 0, 1, 2, 3$ dados em lema 4.2.6. Denotamos as operações binárias da álgebra simplesmente por $\wedge$ e $\vee$. É preciso verificar as condições da definição 4.2.1. Para isso, precisamos inicialmente introduzir uma relação de ordem parcial. Usando o Lema da Conexão, 4.2.8, definimos

$$x \leq_A y, \quad \text{sse}_{def} \quad x = x \wedge y \quad \text{sse}_{Fato}{}^{3} \quad y = x \vee y. \qquad (*)$$

Com a definição acima, temos o seguinte
Fato 1: $(A; \leq_A)$ é uma ordem parcial.
Prova do Fato 1: Sabemos que por $(R_{0\wedge})$ para $x \in A$, $x = x \wedge x$. Logo pela definição $(*)$, $x \leq_A x$, mostrando que a ordem é reflexiva. Sejam agora $x, y \in A$ tais que, $x \leq_A y$ e $y \leq_A x$, então temos que $x = x \wedge y$ e $y = y \wedge x$. Usando $(R_{1\wedge})$, obtemos que $x = y$, mostrando a anti-simetria. Para verificar a transitividade, sejam $x, y, z \in A$ tais que, $x \leq_A y$ e $y \leq_A z$, i.e., $x = x \wedge y$ e $y = y \wedge z$. Usando $(R_{2\wedge})$, obtemos que $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, mostrando que $x \leq_A z$, terminando a prova do primeiro Fato.

Falta mostrar que as operações $\wedge$ e $\vee$ são o infimo e supremo, respectivamente. Temos
Fato 2: Para todo $x, y \in A$, $\quad x \wedge y = \inf\{x, y\} \quad$ e $\quad x \vee y = \sup\{x, y\}$.
Prova do Fato 2: Somente vamos mostrar que $x \wedge y = \inf\{x, y\}$, sendo a segunda parte deste fato análoga, usando a segunda parte da definição $(*)$ acima (Exercício). Para isso, precisamos verificar as condições da definição 4.1.5. Primeiramente, vejamos que $x \wedge y$ é barreira inferior de x e y. Observe que $(x \wedge y) \wedge x = x \wedge (y \wedge x) = x \wedge (x \wedge y) = (x \wedge x) \wedge y = x \wedge y$, onde usamos $(R_{2\wedge})$, $(R_{1\wedge})$ e $(R_{0\wedge})$. Com isso, temos que $x \wedge y \leq_A x$. Analogamente, podemos mostrar que $x \wedge y \leq_A y$. Assim, $x \wedge y$ é barreira inferior para x e y. Falta ver que esta barreira é a maior possível. Para isso, consideremos uma barreira inferior $z \in A$ de x e y, i.e., $z \leq_A x$ e $z \leq_A y$. Então temos pela definição $(*)$ acima: $z = z \wedge x$ e $z = z \wedge y$. Precisamos mostrar que $z = z \wedge (x \wedge y)$. Usando as hipóteses e as condições $(R_{1\wedge})$ e $(R_{2\wedge})$, obtemos que $z = z \wedge x = (z \wedge y) \wedge x = z \wedge (y \wedge x) = z \wedge (x \wedge y)$, terminado a prova da primeira parte deste Fato.

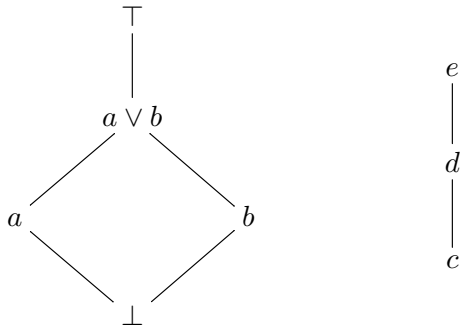
Usando os fatos 1 e 2 acima demonstrados temos que $(A, \leq_A)$ é um reticulado definido conforme a definição 4.2.1. ∎

Observação 4.3.5. *Podemos mostrar (cf. exercício) que as leis da absorção $(R_{3*}$ implicam as leis da idempotência (R_{0*}).* ∎

[3] Para mostrar este Fato, use a lei da absorção.

Definição 4.3.6. *Sejam $(A; \leq_A)$ e $(B; \leq_B)$ reticulados e $f : A \to B$ uma aplicação.*
Dizemos que f é **(homo-)morfismo de reticulados** *sse$_{def}$ f preserva infimo e supremo, i.e., para todo $x, y \in A$, temos que $f(x \wedge y) = f(x) \wedge f(y)$ e $f(x \vee y) = f(x) \vee f(y)$.*

Exemplo 4.3.7. *(a) Sejam dados os reticulados A e B seguintes*



e a aplicação $f : A \to B$ definida como sendo $f(\bot) = f(a) = c$, $f(b) = f(a \vee b) = d$ e $f(\top) = e$. Então esta aplicação é um morfismo de reticulados e preserva ordem (cf. 3.1.5). Verifique!

(b) Considerando os mesmos reticulados A e B acima, e definindo uma aplicação $g : A \to B$, como sendo $g(\bot) = c$, $g(a) = g(b) = d$ e $g(a \vee b) = g(\top) = e$, vejamos que g preserva ordem, porém não é morfismo de reticulados: Observe que $g(a \wedge b) = g(\bot) = c$ e $g(a) \wedge g(b) = d \wedge d = d$, mas $c < d$. ∎

Temos a seguinte

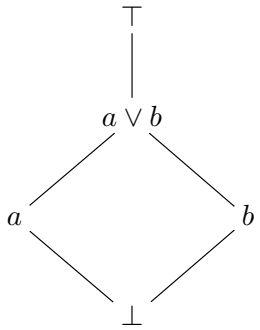
Observação 4.3.8. *(a) Um morfismo entre reticulados sempre preserva ordem.*
(b) Não vale a reciproca do ítem (a). ∎

4.4 Subreticulado e reticulado produto

Definição 4.4.1. *Sejam A um reticulado visto como álgebra, cf. 4.3.3 e $B \subseteq A$ não vazio.*
Dizemos que B é **subreticulado de** *A sse$_{def}$ para todo $a, b \in B$, $a \wedge_A b, \quad a \vee_A b \in B$.*

Observação 4.4.2. *(a) Observe que em caso de B é subreticulado de A, então B é um reticulado com os supremos e infimos calculados em A.*
(b) Todo subconjunto de A com um só elemento é subreticulado.
(c) Toda cadeia num reticulado é um subreticulado. ∎

Exemplo 4.4.3. *Consideramos o reticulado A do exemplo 4.3.7:*



Consideremos o subconjunto $B := \{\bot, a, b, \top\} \subseteq A$ de A. Assim, mesmo sendo B por sua vez um reticulado, B **não** *é subreticulado de A, pois temos que $a \vee_A b \neq \top = a \vee_B b$, ou seja, o supremo entre a e b calculado em B e em A não coincidem.* ∎

Em seguida, introduzimos o produto de dois reticulados. É fácil ver que a definição pode ser generalizada se para um produto finito de reticulados.

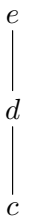
Definição 4.4.4. *Sejam $(A; \leq_A)$ e $(B; \leq_B)$ reticulados cf. 4.2.1.*
Dizemos que $(A \times B; \leq)$ é o **reticulado produto** *de A e B, onde $\leq$ denota a ordem por coordenadas em $A \times B$ introduzido em 3.2.1.*

Observação 4.4.5. *(a) Em seção 3.2.1 demonstramos que a ordem $\leq$ em $A \times B$ é de fato uma ordem parcial. Para completar o raciocínio que a definição anterior de fato dá uma estrutura de reticulado é preciso saber quem são supremo e infimo. Para isso, mostramos que os supremo e infimo é calculado simplesmente por coordenadas ou seja, podemos demonstrar que $\forall \langle a_1; b_1\rangle, \langle a_2; b_2\rangle \in A \times B$,*

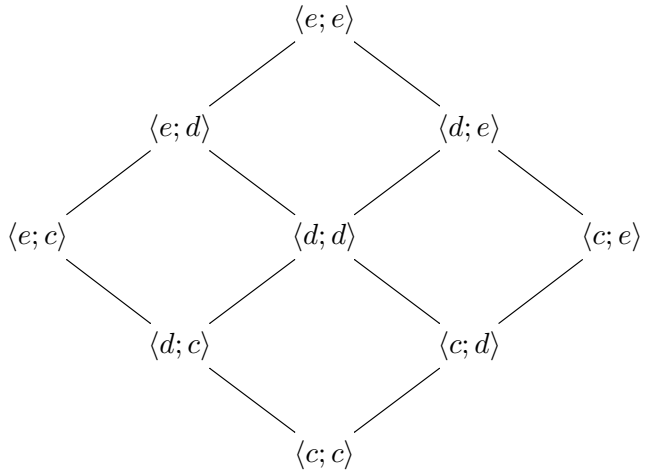
$$\langle a_1; b_1\rangle \vee_{A\times B} \langle a_2; b_2\rangle = \langle a_1 \vee_A a_2; b_1 \vee_B b_2\rangle, \quad \textit{e} \quad \langle a_1; b_1\rangle \wedge_{A\times B} \langle a_2; b_2\rangle = \langle a_1 \wedge_A a_2; b_1 \wedge_B b_2\rangle,$$

Faça os detalhes!

(b) Dado o diagrama de Hasse de dois reticulados, podemos imediatamente exibir o diagrama para o reticulado produto, como no exemplo em baixo. Temo dado o reticulado C que é uma cadeia de três elementos e com o seguinte diagrama de Hasse



Então o reticulado produto $C \times C$ tem o seguinte diagrama:



■

4.5 Reticulados especiais

Introduzimos em seguida alguns reticulados especiais, ou seja, reticulados quais têm alguma(s) propriedade(s) a mais do que os reticulados tratados até então. Começamos com

Definição 4.5.1. *Seja $(A; \leq_A)$ um reticulado.*
Dizemos que A é **completo** *sse_{def} para qualquer subconjunto $S \subseteq A$, existe $\bigvee S$ e $\bigwedge S$.*

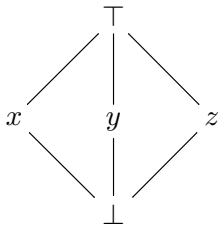
Observação 4.5.2. *(a) Observe que um reticulado completo é sempre limitado, porém não vale a recíproca.*
(b) Existe um método de emergir qualquer reticulado num reticulado completo. Este método é um generalização das cortes de Dedekind para a introdução dos números reais, a partir dos racionais. Chamamos este método para reticulados de Dedekind-MacNeille e este pode ser encontrado em [6]. ∎

Antes de exibir exemplos introduzimos ainda

Definição 4.5.3. *Seja $(A; \leq_A)$ um reticulado limitado.*
(a) Seja $a \in A$ um elemento. Dizemos que a é **complementado** *sse_{def} existe $b \in A$ tal que $a \vee b = \top$ e $a \wedge b = \bot$. Dizemos que este b é um* **complemento** *de a. Em caso de b ser o único complemento de a, denotamo-lo por $\neg a$.*
(b) Dizemos que A é **complementado** *sse_{def} A é limitado e todo elemento de A é complementado.*

Observação 4.5.4. *(a) Observe que num reticulado, um elemento a pode ter nenhum, exatamente um ou mais do que um complemento.*
(b) O conceito de "ser complemento de" é simétrica.

Demonstração: Para o ítem (a), considere o reticulado da cadeia C de três elementos dado na observação 4.4.5, por $c \leq d \leq e$. O elemento d não possui complementado. Consideremos porém o elemento c, então e é complemento de c.
Para ver que podemos ter mais do que um complementado, consideremos o reticulado não distributivo $M3$, cf. 4.2.10, dado pelo diagrama



Assim podemos calcular sem maiores problemas que para x, os elementos y e z satisfazendo as condições de serem complementos de x. O ítem (b) é trivial. ∎

Temos o seguinte resultado qual demonstramos em exercícios:

Lema 4.5.5. *Seja A um reticulado distributivo. Então, todo elemento a complementado de A possui único complemento qual denotamos por $\neg a$.* ∎

Exemplo 4.5.6. *(a) Consideremos o reticulado $M3$. É imediato que $M3$ é um reticulado completo, cf. 4.5.1, pois ele é finito. Vimos que $M3$ não é distributivo, porém complementado.*

(b) Consideremos a cadeia $(\mathbb{N}; \leq_{\mathbb{N}})$, onde $\leq_N$ é a ordem linear em $\mathbb{N}$. Assim, este reticulado não é completo, pois considere o conjunto de todos os primos denotado por $P \subseteq \mathbb{N}$. Sabemos pela teoria dos números e da demonstração da existência de um número infinito de primos, que não pode existir o supremo de P, i.e., $\bigvee P$. Existe $\bigwedge P$? O reticulado é complementado? (Dica: Para responder isso, basta obter um elemento que não tem complemento.) O reticulado é distributivo? Veja resultados obtidos anteriormente para responder as perguntas.

(c) Seja agora A um conjunto arbitrário. Sabemos que $(\mathcal{P}(A); \subseteq)$ é um reticulado completo. Pela proposição 4.1.10, sabemos como calcular supremo e infimo de qualquer subconjunto de $\mathcal{P}(A)$. Como as leis distributivas valem para conjuntos, o reticulado é distributivo. Além disso, o reticulado é complementado, pois dado $X \subseteq A$, sabemos que $X \cap (A \setminus X) = \emptyset$ e $X \cup (A \setminus X) = A$. Usando o Lema 4.5.5, o complementado é único e podemos denotar por A^c. Na próxima seção, vejamos que este reticulado é muito especial: distributivo, complementado e completo. ∎

4.6 Álgebra de Boole e um teorema do ponto fixo

Nesta seção falamos de algumas propriedades das álgebras de Boole e demonstramos o teorema do ponto fixo de Tarski para reticulados completos.

Definição 4.6.1. *Dizemos que um reticulado distributivo, complementado (e completo) é uma* **álgebra de Boole (completa)**.

Observação 4.6.2. *(a) É possível defnir o conceito de álgebra de Boole via álgebra. Assim uma álgebra de Boole é dada por* $\mathfrak{B} := (B; \vee, \wedge, \neg, \bot, \top)$ *satisfazendo os seguintes axiomas:*

(i) $(B; \wedge, \vee)$ *é um reticulado, i.e., conforme 4.3.3.*

(ii) $\mathfrak{B}$ *é limitado, i.e.,* $\forall b \in B$, $\bot \wedge b = \bot$ *e* $\top \vee b = \top$.

(iii) $\mathfrak{B}$ *é distributivo, i.e. cf. 4.2.9.*

(iv) $\mathfrak{B}$ *é complementado, i.e.* $\forall b \in B$, $b \vee (\neg b) = \top$ *e* $b \wedge (\neg b) = \bot$.

As definições 4.6.1 e a de cima são equivalentes, ou seja, definem o mesmo conceito. (Faça os detalhes em exercício).

(b) Observemos que as abreviações para as operações numa álgebra de Boole lembrem de conectivos lógicos, e isto não é de mera coincidência. Álgebras de Boole formam modelos para lógica clássica e podemos interpretar de fato os conectivos lógicos pelas operações numa álgebra de Boole, . 4.6.5. ∎

Exemplo 4.6.3. *(a) Reconsideremos o reticulado introduzido em 4.5.6 (c), é fácil ver que* $(\mathcal{P}(A); \subseteq)$ *é uma álgebra de Boole.*

(b) Consideremos agora o seguinte conjunto $FC(X) := \{A \subseteq X | \quad A$ *e finito ou* A *é cofinito* $\}$*, onde dizemos que* A *é cofinito sse*$_{def}$ $X \setminus A$ *é finito. Assim,* $(FC(X); \subseteq)$ *forma uma álgebra de Boole. Em exercício, vamos mostrar que* $(FC(\mathbb{N}); \subseteq)$ *é uma álgebra de Boole.*

(c) Consideremos a ordem linear $\mathbf{2} := \{0, 1\}$*, onde* $0 \leq 1$*. É fácil para verificar que* $(\mathbf{2}; \leq)$ *é uma álgebra de Boole. Esta álgebra de Boole é isomorfa a* $(\mathcal{P}(\{\emptyset\}); \subseteq)$.
Para um natural $n \in N$*, seja* $\mathbf{2}^n := \mathbf{2} \times \cdots \times \mathbf{2}$ *com a ordem* $\leq_n$ *definida por coordenadas, cf. 3.2.1, i.e.,*
$\forall \langle x_1, \ldots, x_n \rangle, \langle y_1, \ldots, y_n \rangle \in \mathbf{2}^n, \quad \langle x_1, \ldots, x_n \rangle \leq_n \langle y_1, \ldots, y_n \rangle \quad$ *sse* $\quad x_i \leq y_i, \quad \forall i = 1, \ldots, n.$

Então, $(\mathbf{2}^n; \leq_n)$ *é uma álgebra de Boole. Verifique os detalhes e mostre que esta álgebra de Boole é isomorfa a álgebra dada por* $(\mathcal{P}(A); \subseteq)$*, onde* A *é um conjunto com* n *elementos.* ∎

Observação 4.6.4. *Um resultado importante de M. Stone é que qualquer álgebra de Boole é isomorfa a uma subalgebra de uma álgebra das partes de algum conjunto. O exemplo anterior mostra que existe de fato uma álgebra de Boole qual não é da forma "partes de algum conjunto".*
Observe que podemos demonstrar que $FC(\mathbb{N})$ *tem um número infinito* **enumerável** *de elementos. Cantor mostrou além disso o conjunto das partes* $\mathcal{P}(\mathbb{N})$ *é não enumerável. Sabemos que em caso de o conjunto* A *ser finito,* $\mathcal{P}(A)$ *é finito. Com o resultado de Cantor sabemos em caso de* A *ser infinito enumerável,* $\mathcal{P}(A)$ *é infinito* **não** *enumerável. Por isso, a álgebra de Boole* $FC(\mathbb{N})$ *não pode ser isomorfa a uma álgebra de Boole da forma* $\mathcal{P}(A)$*, para algum conjunto* A*.* ∎

A próxima observação conecta lógica, ordem e conjuntos.

Observação 4.6.5. *Podemos identificar as seguintes operações em lógica matemática, teoria dos conjuntos e teoria das ordens conforme a tabela em baixo:*

lógica	*conjuntos*	*ordens*
$\rightarrow$	$\subseteq$	$\leq$
$\leftrightarrow$	$=$	$=$
1*, verdade*	*conjunto uiversal*	$\top$*, maior elemento*
0*, absurdo*	$\emptyset$*, conjunto vazio*	$\bot$*, menor elemento*
$\wedge$*, conjunção*	$\cap$*, interseção*	$\wedge$*, infimo*
$\vee$*, disjunção*	$\cup$*, união*	$\vee$*, supremo*
$\neg$*, negação*	$(\cdot)^c$*, complemento em conjuntos*	$\neg$*, elemento complementado*
$\forall$*, para todo, quantificador universal*	$\bigcap$*, interseção geral*	$\bigwedge$*, infimo geral*
$\exists$*, existe, quantificador existêncial*	$\bigcup$*, união geral*	$\bigvee$*, supremo geral.*

■

O último teorema é uma versão do teorema de ponto fixo de Tarski-Knaster. A importância deste teorema é que na computação teórica, cf. 3.1.6, podemos modelar um calculo computacional através de uma aplicação preservando ordem de um reticulado completo em si mesmo. O teorema agora diz que existe um ponto fixo desta aplicação, o que é equivalente a dizer que a computação de fato chega a um fim, oiu seja, ela pára.

Teorema 4.6.6 (Tarski-Knaster)**.** *Sejam $(A;\leq)$ um reticulado completo e $f : A \rightarrow A$ uma aplicação preservando ordem, cf. 3.1.5. Então a aplicação f tem um ponto fixo, i.e., $\exists x \in A$ tal que $f(x) = x$.*

Demonstração: Com as hipóteses, consideremos $\mathcal{F} := \{x| \quad x \in A \ \& \ x \leq f(x)\}$.
Como $\bot \leq f(\bot)$ e $\bot \in A$, temos que $\mathcal{F} \neq \emptyset$. Além disso, é claro que $\mathcal{F} \subseteq A$, e sendo A um reticulado completo temos que $\bigvee \mathcal{F}$ existe em A. Agora observe que pela definição do supremo

$$\forall y \in \mathcal{F}, \qquad y \leq \bigvee \mathcal{F}$$

Como f preserva ordem e $y \in \mathcal{F}$, temos para todo $y \in \mathcal{F}$ que $\quad y \leq f(y) \leq f(\bigvee \mathcal{F})$.

Assim, $f(\bigvee \mathcal{F})$ é uma barreira superior de $\mathcal{F}$. Como $\bigvee \mathcal{F}$ é o supremo de $\mathcal{F}$, é preciso que $\bigvee \mathcal{F} \leq f(\bigvee \mathcal{F})$. Logo, temos que

$$f(\bigvee \mathcal{F}) \leq f(f(\bigvee \mathcal{F})).$$

Ou seja, $f(\bigvee \mathcal{F}) \in \mathcal{F}$, o que implica que $f(\bigvee \mathcal{F}) \leq \bigvee \mathcal{F}$.

Com isso temos que $f(\bigvee \mathcal{F}) = \bigvee \mathcal{F}$. Aí, $\bigvee \mathcal{F}$ é o ponto fixo de f. ■

Observação 4.6.7. *Podemos demonstrar que o conjunto de todos os pontos fixos da aplicação f do Teorema de Knaster-Tarski, denotado por $Fix(f) := \{x \in A| \quad f(x) = x\}$, forma um reticulado completo.* ■

Apendix: Criptografia RSA

Nesta seção queremos explicar o método de criptografia *RSA*[4] usado desde os anos 1970 até hoje (ano 2018) na transmissão de dados secrétos. Usamos entre outros fontes principalmente [16] nesta seção. Esta criptografia se baseia na fatoração de primos, ou seja, usa o fato de que um produto de dois primos suficientemente grandes - mais tarde explicamos este *suficientemente grande* - não podem ser fatorados em tempo habil, por um programa de computação.

Troca de chave

Até os anos 1970, achava-se que para podermos mandar uma mensagem secréta para uma outra pessoa *sempre* é preciso uma *troca de chave*:
A pessoa A quer mandar uma mensagem para a pessoa B. Para isso, é preciso que a pessoa A codifica a sua mensagem em símbolos que ninguém pode entender **sem** o uso de uma *chave*. A transmite esta mensagem para B e aí, B precisa para a decodificação da mensagem esta chave, ou seja, B precisa algum método para poder entender a mensagem de A. Estamos supondo que uma transmissão pessoal não é viável, por causa de custos. Por exemplo, pense na compra de mercadorias via internet, quantas transmissões secrétas são efetuadas a cada hora! Ou pense em internet-banking, os correntistas precisam acessar a sua conta, e nenhuma terceira pessoa pode saber das transações!

Uma distribuição de chave nos leva ao seguinte paradóxo:

Para duas pessoas trocarem um segredo é preciso ter trocado um segredo antes.

Ou seja, para duas pessoas trocarem informações secretamente é preciso que eles trocam primeiramente uma chave de digamos *decodificação*. Para uma troca de chave teríamos pelo menos duas possibilidades, porém não practicáveis: A troca pessoal das chaves geraria muitos custos, pensando nos exemplos acima feitos. Uma troca de chave usando uma terceira pessoa seria por outro lado muito arriscado no sentido de fraude, nem falar dos custos também. Durante muito tempo cientistas pensaram neste problema, pois a criptografia é de interesse desde muito tempo. Transmitir mensagens secrétas sempre era de grande interesse. Infelizmente, muitas vezes a criptografia é usada em tempos de guerra, que basicamente marcam a existência de toda a humanidade.

Uma possibilidade de solucionar esta troca de chaves é que *não* é preciso uma troca de chaves. Vejamos o seguinte modelo:
Pensamos numa caixa em qual a pessoa A coloca a mensagem secréta e depois a tranca com um cadeado. Agora manda esta caixa para a pessoa B. A pessoa B coloca o seu cadeado na caixa, e manda de volta a caixa para A. A então tira o seu cadeado, e na caixa resta somente o cadeado de B. Observe que a caixa ainda está trancada! Porém B tem a chave e pode abri-la, após A ter mandado de volta para B .

Este modelo mostra que aparentemente é possível uma transmissão de segredos **sem** uma troca de cha-

[4] A criptografia RSA é chamada pelos iniciais das três cientistas que a desenvolveram em 1977, a saber, Ronald Rivest, Adi Shamir e Leonard Adleman.

ves! Um problema deste modelo é a inversão das decodificações, quais vejamos logo em seguida. Até aos anos 1970, era um *paradigma* ou seja, era *o axioma* da criptografia que uma troca de chaves é sempre preciso. O modelo acima elaborado parece que contradiz ao axioma.

Vejamos agora o problema acima mencionado da inversão das decodificações. Para isso, usamos a seguinte notação: Seja M a mensagem a ser transmitida, a chave-cadeado de A denotado por a. Aí, a pessoa A manda Ma para a pessoa B, onde Ma quer dizer que a mensagem M foi munida com o cadeado a da pessoa A. A pessoa B manda agora Mab para a pessoa A de volta. Agora A destrava o seu cadeado fazendo a^{-1} e manda para B a mensagem $Maba^{-1}$. Agora B tira o seu cadeado e obtém $Maba^{-1}b^{-1}$. O problema que temos então que em geral $M \neq Maba^{-1}b^{-1}$. Por quê?

Podemos pensar num exemplo simples de dia e dia: sapatos e meias. Observe que é preciso sempre vestir meias antes dos sapatos, porém na hora de chegar em casa, é preciso tira antes os sapatos e depois as meias. Neste caso o modelo acima não vai funcionar: A coloca meia, e B coloca sapato, porém com o sapato *não* consigo tira a meia. Um outro exemplo, pode ser gerado com facilidade.

Exemplo:
Consideramos que as pessoas A e B codificam o alfabeto de seguinte maneira, onde o ç deve ser identificado com o c:

pessoa	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	h	f	s	u	g	t	a	k	v	d	e	o	y	j	b	p	n	x	w	c	q	r	i	m	z	l
B	c	p	m	g	a	t	n	o	j	e	f	w	i	q	b	u	r	y	h	x	s	d	z	k	l	v

Agora transmite a mensagem: "M:= venha hoje a noite", e vejamos que $M \neq Maba^{-1}b^{-1}$. ■

Nos anos 1970, os cientistas americanos Whitfield Diffie, Martin Hellman e Ralph Merkle trabalharam numa pesquisa sobre a criptografia. Foram eles que descobriram que uma troca de chave não precisa ser efetuado sempre. Além disso, esses pesquisadores procuraram um método de trocar eventuais chaves sem riscos. Para isso, eles pensaram em funções bijetivas que podemos calcular facilmente, porém as suas inversas são difícil de calcular. Nos seus estudos, eles descobriram funções modulares da seguinte forma:
Seja $\mathbb{Z}_7^* := \mathbb{Z}_7 \setminus \{0\}$ e

$$f : \mathbb{Z}_7^* \to \mathbb{Z}_7^*, x \mapsto f(x) := 3^x mod 7.$$

A inversa desta função é relativamente difícil de calcular, aumentando os valores de 3 para 453, e de 7 para 21997, por exemplo. Faça o exemplo, esta função podemos chamar de *one way*: É relativamente fácil de calcular $453^x mod 21997$ para qualquer x, porém é problemático achar o valor x tal que $453^x mod 21997 = 5787$. Com estas funções é uma troca de chaves finalmente possível sem nenhum risco.

Para o entendimento o que é uma função one way, pense na mixtura de cores: Misturamos as cores azul e amarelo, obtemos a cor verde. Porém, não é possível obter as cores amarelo e azul da cor verde de volta. Isto quer dizer função *one way*. Vejamos o seguinte

Exemplo:
Damos um exemplo com valores pequenos! Na prática, é preciso aumentar os valores. Pessoa A escolhe $\alpha = 3$, e deixa sob segredo. A pessoa B, escolhe $\beta = 6$ e deixa sob segredo. As pessoas A e B trocam publicamente os números 7 e 11. Aí, A calcula $7^3 mod 11$ e B $7^6 mod 11$. Obtemos uma vez $7^3 \equiv_{11} 2$ e da outra vez $7^6 \equiv_{11} 4$.

O resultado de A chamamos de a, e A manda $a = 2$ para B. O resultado de B é b, e B manda $b = 4$ para A. Esta troca de mensagens seria o passo problemático, porém neste caso os números a e b podem ser feitos públicos.

Agora A calcula $b^\alpha mod 11$ e B calcula $a^\beta mod 11$ e obtemos em nosso caso:

$$b^\alpha \equiv_{11} 4^3 \equiv_{11} 9 \quad \text{e} \quad a^\beta \equiv_{11} 2^6 \equiv_{11} 9.$$

Como α é chave pessoal e secréto de A, ninguém além de A pode calcular o valor 9. O mesmo vale para

o caso de B. E olhe só: Assim, conseguimos trocar a chave! E trocamos a chave *sem* encontro pessoal ou mediante de terceiros. ■

Porém ainda não foi resolvido o método da transmissão da mensagem. Assim Diffie desenvolveu o método da codificação *asimétrica*. Até o momento as codificações eram todas *simétricas*, no sentido que para a decodificação é preciso a chave *inversa* da codificação, ou seja em símbolos, A faz a e B para decodificar faz a^{-1}. O método asimétrico, é diferente no sentido de que A pode codificar a mensagem em a, porém não consegue mais decodificá-lo - porém não precisa necessariamente pois sabe a sua mensagem a! B tem a chave para decodificar e pode ler a mensagem. Temos então a diferença entre chave *codificar* e chave *decodificar*. Diffie teve estas idéias e já as idéias eram revolucionárias na área da criptografia, mesmo não tendo funções quais satifazem estas exigências.

Resumindo a idéia da criptografia asimétrica é que A tem a sua chave de codificar, e esta pode ser *público*, além de A ter a chave de decodificar, e esta seria *secréto*. O mesmo ocorre para B. Com isso, podemos aumentar os números de pessoas quais querem trocar mensagens privadas. Cada uma tem chave pública, em geral um número que pode ser colocado numa lista tipo telefônica, e junto tem o número da decodificação. Assim, se alguém quer mandar uma mensagem para A, somente codifica com a chave pública de A, e somente A pode decodificá-la via chave secréta.

A grande vantagem é que não é mais preciso uma troca de chaves!

No verão de 1975, Diffie publicou as suas idéias, e começou a procura da função one way. Assim, o campo da criptografia foi revolucionado completamente, embora até 1976, não era achado este tipo de função.

A criptografia RSA

Com os problemas acontecendo exemplificado anteriormente, os pesquisadores procuraram uma codificação *asimétrica*, ou seja, uma função bijetiva que cumpre estas exigências. No Massachusettes Institute of Technology (MIT), dois pesquisadores da computação Ron Rivest, Adi Shamir e o matemático Leonard Adleman estavam procurando funções one way. Em abril de 1977, Ron Rivest descobriu uma tal função e os três pesquisadores conseguiram elaborar a criptografia chamada de **RSA**. A idéia principal é uma função *one way* baseada nas funções modulares. Vamos explicar o método em detalhe.

Em seguida, chamamos N a variável desta função. Alguém querendo usar uma criptografia, pode escolher o seu valor N - qual claramente tem que satisfazer algumas condições, quais vejamos logo. Em **RSA** usamos uma chave pública, i.e., uma chave qual é aberta e conhecida, o número N. Além desta chave temos também a chave particular, i.e., uma chave qual precisamos manter em segredo. A chave particular está sendo usada para decodificar a mensagem. Vejamos os detalhes de **RSA**:

- Escolhemos dois números primos distintos p e q, quais são relativamente próximos e calculamos a chave pública $N := pq$. Os primos são grandes[5] e mantidos em segredo.
- O número $N = pq$, facilita o cálculo da função de Euler de N,[6] $\varphi(N)$. Podemos demonstrar que $\varphi(pq) = (p-1)(q-1)$, para primos p e q.
- Escolhemos então um número e tal que $1 < e < \varphi(N)$ e $mdc(e; \varphi(N)) = 1$. Esta escolha do número e garante que e é inversível módulo $\varphi(N)$, ou seja, que existe d tal que $ed \equiv_{\varphi(N)} 1$.

[5]Em 2008, o comprimento de $RSA-2048$, $2048 = 2^{11}$, era um número N com mais ou menos 617 dígitos dezimais, i.e., $N \sim 2^{2^{11}}$, e era suficiente para a garantia da segurança da criptografia. Caso este número pode ser quebrado ou fatorado, é preciso aumentar para $RSA-4096$ e $N \sim 2^{2^{12}}$.

[6]A função φ de Euler de um número natural N não nulo é a quantidade dos números entre 1 e N, quais são relativamente primos com N. Desta definição é imediato que se p for número primo, $\varphi(p) = p-1$.

- Calculemos o número d tal que $1 < d < \varphi(N)$ e $d \cdot e \equiv_{\varphi(N)} 1$. Para o cálculo de d usamos o algoritmo de Euclides, pois observe que $d \cdot e \equiv_{\varphi(N)} 1$ é equivalente com $de + k\varphi(N) = 1$, para algum $k \in \mathbb{Z}$.

Retornamos ao nosso problema inicial, i.e., a pessoa A quer mandar uma mensagem secréta para a pessoa B. Assim, escolhe de uma lista a chave pública de B, digamos N. Agora, observe que a pessoa B sabe a fatoração de N em dois primos p e q. Estes primos são as chaves particulares de B, junto com o número d, que B pode calcular apartir de $\varphi(N)$. Sendo N suficientemente grande, como mencionado acima, ninguém pode fatorar este números em produto de primos, também os computadores não podem fatorar N em tempo razoável. A pessoa A toma número público e conforme o ítem acima. A quer mandar a mensagem qual deve ser um número m tal que $m < N$. A mensagem m é secréta. Agora A calcula m^e manda $c \equiv_N m^e$ para a pessoa B. O cálculo de c pode ser feita via exponenciação rápida, explicado em seguida. Agora A informa B do número c via telefone, por exemplo. Observe que c não é secréto, pode ser transmitido publicamente.

A pessoa B tem por sua vez a fatoração de N, informação que nem A tem, ou seja, uma informação secréta. Com a fatoração, B pode calcular o número d, qual permite saber a mensagem original m de A. Podemos demonstrar que

Fato 1: $m \equiv_N c^d \equiv_N (m^e)^d$.

Vamos justificar este Fato. Para isso, é preciso o uso do *pequeno teorema de Fermat*.

Pequeno Teorema de Fermat
Sejam $a, p \in \mathbb{Z}$ tais que $p \geq 2$ um primo e $mdc(a; p) = 1$. Então $a^{p-1} \equiv_p 1$.[7]

Prova do Fato 1: Observe que a segunda igualdade é imediata. Sabemos agora que $de \equiv_{\varphi(N)} 1$, com $\varphi(N) = (p-1)(q-1)$. Daí, temos que $de = 1 + k \cdot \varphi(N)$, para algum $k \in \mathbb{Z}$. Logo obtemos que

$$(m^e)^d = m^{ed} = m^{1+k\varphi(N)} = m(m^{k(p-1)(q-1)}) = m(m^{(p-1)})^{k(q-1)} = m(m^{(q-1)})^{k(p-1)}.$$

Temos então dois casos, a saber
Primeiro caso: $mdc(q; m) = 1$. Então, temos pelo pequeno Teorema de Fermat que $m^{q-1} \equiv_q 1$. Daí, $(m^{(q-1)})^{k(p-1)} \equiv_q 1$. Logo $m^{ed} \equiv_q m$.
Segundo caso: $mdc(q; m) \neq 1$, i.e., como q é primo é preciso que $q|m$. Assim, existe $t \in \mathbb{Z}$ tal que $m = tq$, o que implica que $m \equiv_q 0$. Portanto

$$m(m^{(q-1)})^{k(p-1)} \equiv_q 0 \equiv_q m.$$

Assim, em ambos os casos, obtemos que $m^{ed} \equiv_q m$, ou seja, m^{ed} nos devolve a mensagem secréta m.

Analogamente, podemos elaborar os casos idênticos para o primo p, e obtemos também $m^{ed} \equiv_p m$. Como os primos eram escolhidos distintos e como $p|(m^{ed} - m)$ e $q|(m^{ed} - m)$, temos pelo teorema de Euclides 2.3.8 que $pq|(m^{ed} - m)$, ou seja,

$$N|(m^{ed} - m), \text{ isto é, } m^{ed} \equiv_N m$$

Logo, o fato está demonstrado. ∎

Assim, B recupera a mensagem m. Observe que A não tem informações para fazer estes cálculos, nenhuma outra pessoa além de B pode saber a mensagem m, após a codificação.

Repetindo, temos as chaves públicas, N e e, além das chaves particulares p, q e d. Assim, a transmissão de mensagens secrétas funciona. Cada pessoa tem números públicos N e e, além de números secrétos, p, q e d. Tendo em vista este método de criptografia, entendemos também, porque a ciência está interessado em números primos grandes. Usando um certo código também é fácil de entender que uma mensagem nada mais é do que um número natural.

[7] Para um prova deste teorema, consulte por exemplo [14].

Exponenciação rápida

Em seguida vejamos como calcular de modo rápido $c^d mod\, N$. O método qual explicamos está sendo chamado de *exponenciação rápida*. Em casos, em quais o pequeno teorema de Fermat não é aplicável, podemos usar este método. Sejam dados os númros naturais b, e e m e queremos calcular $b^e mod\, m$. Procedemos em três passos:

- Inicialmente escrevemos o número e em base 2, isto é, $e = \sum_{i=0}^{k} e_i 2^i$, onde $e_i \in \{0, 1\}$, cf. capítulo 2.
- Calculemos então $b^{2^i} mod\, m$, para todo $i \in \{0, \ldots, k\}$. Para este cálculo, usamos o fato de que
$$b^{2^{i+1}} = b^{2^i \cdot 2} = (b^{2^i})^2.$$
- Observemos agora que
$$b^e = b^{(\sum_{i=0}^{k} e_i 2^i)} = \prod_{i=0}^{k} b^{e_i 2^i} = \prod_{i=0, e_i \neq 0}^{k} b^{2^i}.$$

Vejamos o seguinte exemplo: Queremos calcular $6^{73} mod\, 100$. Não podemos aplicar os teorema de Euler e de Fermat. Também não temos outro *truque* para solucionar. Porém a exponencição rápida nós permite um cálculo rápido. Seguimos como explicado acima, e calculamos 73 na base 2. Um cálculo simples $73 = 2^6 + 2^3 + 1$. Agora precisamos calcular $6^{(2^i)} mod\, 100$, para $i \in \{1, \ldots, 6\}$.
$6^2 = 36$, $6^{(2^2)} = (6^2)^2 = 36^2 \equiv_{100} -4$,
$6^{(2^3)} = (6^{2^2})^2 \equiv_{100} (-4)^2 \equiv_{100} 16$,
$6^{(2^4)} = (6^{2^3})^2 \equiv_{100} 16^2 \equiv_{100} 56$,
$6^{(2^5)} = (6^{2^4})^2 \equiv_{100} 56^2 \equiv_{100} 36$,
$6^{(2^6)} = (6^{2^5})^2 \equiv_{100} 36^2 \equiv_{100} -4$.

Pelo terceiro passo, sabemos que
$6^{73} = \prod_{i=0, e_i \neq 0}^{6} 6^{2^i} = 6^1 \cdot 6^{(2^3)} \cdot 6^{(2^6)} = 6 \cdot 16 \cdot (-4) \equiv_{100} 16$.

Observe que o cálculo de $6^{73} mod\, 100$ necessitou oito multiplicações, além da transferência de 73 em base 2. Calculando $6^{73} = 6 \cdot 6 \cdot \ldots \cdot 6$ precisaria de 72 multiplicações, além do calculo módulo 100. A pior estratégia é calcular 6^{73} - este número tem 57 dígitos! - e depois calcular módulo 100.

A segurança de RSA

Falamos então um pouco da *segurança* do **RSA**. Observe que a fatoração de um natural em primos é uma tarefa muito difícil, em caso de números grandes do tipo $RSA - 2048$, i.e., o número tem $2^{(2^{11})}$ bytes impossível, até hoje. Um computador *quantico* poderia talvez resolver este problema, porém até agora tal computador não existe. Um computador quantico basicamente pode executar cálculos paralelos, em vez de calcular em sequência.

Observe que o cálculo para transmitir uma mensagem, ou seja, de codificar é uma tarefa simples, pois exige somente o cálculo de potências módulo N. O mesmo é a tarefa de decodificar! A quebra do código é basicamente impossível, porem por sorte pode ser descoberta a fatoração de N. O seguinte fato mostra que a fatoração de N e o cálculo de $\varphi(N)$ tem dificuldades equivalentes. Relembre que precisamos $\varphi(N)$ para calcular o número d inverso multiplicativo de e.

Fato 2:
Seja dado um número **RSA** N, i.e., N é produto de dois primos distintos. São equivalentes:

(a) o cálculo de $\varphi(N)$, e

(b) a fatoração de N em produtos de primos.

Prova do Fato 2. Supondo válido (b), sabemos a fatoração de $N = p \cdot q$. Pela definição da função de Euler é fácil ver que podemos calcular $\varphi(N) = (p-1)(q-1)$.
Supondo válido (a), sabemos o valor de $\varphi(N)$. Como $N = pq$, mesmo não sabendo os valores de p e q, sabemos que $\varphi(N) = (p-1)(q-1)$. Agora, observe que

$$N + 1 - \varphi(N) = pq + 1 - (p-1)(q-1) = pq + 1 - pq - 1 + p + q = p + q. \qquad (*)$$

Por outro lado, temos que

$$\sqrt{(p+q)^2 - 4n} = \sqrt{(p-q)^2} = |p-q|. \qquad (**)$$

S.p.d.g. podemos supor que $p > q$, e temos que $|p-q| = p-q$. De $(*)$ e $(**)$, temos que

$$p = \tfrac{1}{2}((p+q) + (p-q)) \quad \text{e} \quad q = \tfrac{1}{2}((p+q) - (p-q)).$$

Assim, podemos calcular p e q. ■

Referências Bibliográficas

[1] E. Alencar Filho, **Introdução à teoria dos números**, Editora Nobel, São Paulo, 1975.

[2] A.B. Alfonso, H.A. Feitosa e H.L. Nascimento, **Teoria dos conjuntos: sobre a fundamentação da matemática e a construção dos conjuntos númericos**, Editora Ciência Moderna, Rio de Janeiro, 2011.

[3] S. F. Barker, **Filosofia da matemática**, Zahar Editores, Rio de Janeiro, 1969.

[4] P. Blauth Menezes, **Matemática discreta para computação e informática**, Editora Bookman, 3. edição, Porto Alegre, 2010.

[5] A.B.M. Brunner: **Notas de aula para matemática discreta I**, Impresso de pdf, julho de 2013.

[6] B.A. Davey e H.A. Priestley, **Introduction to Lattices and Order**, Cambridge University Press, Cambridge, second edition, 2002.

[7] H.B. Enderton, **Elements of Set Theory**, Academic Press, New York, 1977.

[8] J. L. Gersting, **Fundamentos matemáticos para a ciência da computação**, Editora LTC, Rio de Janeiro, 2001.

[9] P.R. Halmos, **Teoria ingênua dos conjuntos**, Editora Ciência Moderna, Rio de Janeiro, 2001.

[10] A. Hefez: **Elementos de aritmática**, Textos Universitários, Sociedade Brasileira de Matemática (SBM), 2005.

[11] L. Lovász, J. Pelikán e K. Vesztergombi, **Discrete mathematics**, Springer, New York, 2003.

[12] F. Miraglia: **Teoria dos conjuntos, um mínimo**, EDUSP, São Paulo, 1991.

[13] J.P. de Oliveira Santos: **Introdução à teoria dos números**, IMPA, Rio de Janeiro, 2003.

[14] C. Polcino Milies e S. Pitta Coelho: **Números - uma introdução à matemática**, Editora USP, 1998.

[15] E.R. Scheinerman, **Matemática discreta - uma introdução**, Editora Thomson, São Paulo, 2003.

[16] S. Singh, **Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet**, dtv, München, 2001.

[17] S. Singh, **O último teorema de Fermat**, Editora Record, São Paulo e Rio de Janeiro, 1997.