Números inteiros

Sandro Marcos Guzzo

Cascavel - Pr
Agosto de 2013

1 Construção do conjunto dos números inteiros

O conjunto dos números inteiros, designado por $\mathbb{Z}$ será aqui construído a partir do conjunto nos números naturais. O conjunto dos números naturais será considerado

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$$

e dotado de duas operações $+$ e $\cdot$, ditas respectivamente adição (ou soma) e multiplicação (ou produto), sobre as quais incidem as seguintes propriedades para quaisquer $m, n, r \in \mathbb{N}$.

i) (Comutatividade de $+$) $m + n = n + m$,

ii) (Associatividade de $+$) $(m + n) + r = m + (n + r)$,

iii) (Existência de elemento neutro para $+$) $m + 0 = 0 + m = m$,

iv) (Lei do cancelamente para $+$) Se $a + m = a + n$ então $m = n$,

v) (Comutatividade de $\cdot$) $m \cdot n = n \cdot m$,

vi) (Associatividade de $\cdot$) $(m \cdot n) \cdot r = m \cdot (n \cdot r)$,

vii) (Existência de elemento neutro para $\cdot$) $m \cdot 1 = 1 \cdot m = m$,

viii) (Distributividade de $\cdot$ em relação a $+$) $m \cdot (n + r) = m \cdot n + m \cdot r$,

ix) $m \cdot n = 0$ se e somente se $m = 0$ ou $n = 0$,

x) (Lei do cancelamento para $\cdot$) Se $a \cdot m = a \cdot n$ e $a \neq 0$ então $m = n$.

O conjunto dos números naturais é também dotado de uma relação de ordem total. A notação $m < n$ significa que m precede n, ou que n sucede m, pela relação de ordem. Escrevemos $m \leq n$ para dizer que $m < n$ ou $m = n$. Mais precisamente, a relação é dada por

$$a \leq b \quad \Leftrightarrow \quad a + k = b, \quad \text{para algum} \quad k \in \mathbb{N},$$

e

$$a < b \quad \Leftrightarrow \quad a + k = b, \quad \text{para algum} \quad k \in \mathbb{N}^*.$$

Para mais detalhes sobre o conjunto totalmente ordenado dos números naturais, consulte uma construção (ou definição axiomática) deste conjunto.

A ideia da construção do conjunto dos números inteiros é definir um número inteiro como sendo a diferença entre dois números naturais. Assim, se $z \in \mathbb{Z}$ então $z = a - b$ para $a, b \in \mathbb{N}$. Dois problemas aqui ocorrem. Primeiro a diferença não é uma operação sobre o conjunto dos números naturais, e então para contornar isto, o número inteiro z será associado a um par (a, b) com $a, b \in \mathbb{N}$. A ideia é que este par represente o número $a - b$. O segundo problema é que, desta forma, um número inteiro z pode ser escrito de muitas maneiras como diferença de dois números naturais, e então temos que trabalhar com classes de equivalência.

Vamos aos detalhes técnicos desta construção. Considerando o conjunto $\mathbb{N} \times \mathbb{N}$, definimos a relação $\approx$ dada por

$$(a, b) \approx (x, y) \qquad \text{se, e somente se,} \qquad a + y = x + b.$$

Aqui, $+$ é a operação de adição de números naturais, sobre a qual incidem as propriedades citadas anteriormente. Vamos mostrar que $\approx$ é uma relação de equivalência. Dado qualquer $(a, b) \in \mathbb{N} \times \mathbb{N}$, temos claramente que $a + b = a + b$, donde $(a, b) \approx (a, b)$. A relação é então reflexiva. Sejam agora $(a, b), (x, y) \in \mathbb{N} \times \mathbb{N}$, tais que $(a, b) \approx (x, y)$. Da definição da relação temos que $a + y = x + b$ e claramente isto significa também que $x + b = a + y$ donde $(x, y) \approx (a, b)$. A relação é também simétrica. Agora, sejam $(a, b), (x, y), (m, n) \in \mathbb{N} \times \mathbb{N}$ tais que $(a, b) \approx (x, y)$ e $(x, y) \approx (m, n)$, isto é $a + y = x + b$ e $x + n = m + y$. Das propriedades da adição de números naturais, podemos deduzir que $a + y + n = (a + y) + n = (x + b) + n = (x + n) + b = (m + y) + b = m + y + b$. Pela lei do cancelamento de números naturais pela operação de adição, temos que $a + n = b + m$, donde $(a, b) \approx (m, n)$ e a relação é transitiva. Segue que $\approx$ e uma relação de equivalência sobre $\mathbb{N} \times \mathbb{N}$.

Consideremos o conjunto quociente de $\mathbb{N} \times \mathbb{N}$ pela relação $\approx$, isto é, o conjunto de todas as classes de equivalência determinadas pela relação $\approx$ em $\mathbb{N} \times \mathbb{N}$. Seja então

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{\approx} = \left\{ \overline{(a, b)}; \quad (a, b) \in \mathbb{N} \times \mathbb{N} \right\}.$$

O conjunto $\mathbb{Z}$ será, deste ponto em diante, chamado de conjunto dos números inteiros, e um elemento deste conjunto é um número inteiro, ou simplesmente um inteiro. Lembremos ainda que $\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N}; \quad (x, y) \approx (a, b)\}$, e como já sabemos,

$$\overline{(a, b)} = \overline{(x, y)} \quad \Leftrightarrow \quad (a, b) \in \overline{(x, y)} \quad \Leftrightarrow \quad (a, b) \approx (x, y) \quad \Leftrightarrow \quad a + y = x + b.$$

Definiremos em $\mathbb{Z}$ duas operações chamadas de adição (ou soma) e multiplicacão (ou produto) representadas respectivamente por $+$ e $\cdot$, e dadas por

$$\overline{(a, b)} + \overline{(x, y)} = \overline{(a + x, b + y)},$$

e

$$\overline{(a, b)} \cdot \overline{(x, y)} = \overline{(ax + by, ay + bx)}.$$

Aqui, estamos usando no segundo membro destas definições, a notação $+$ para designar a adição de números naturais, e a notação ax para designar a multiplicação $a \cdot x$ de números naturais.

Em primeiro lugar temos que verificar que a adição e a multiplicação de números inteiros estão bem definidas. Isto porque no primeiro membro da definição, temos uma classe $\overline{(a, b)}$ que é na verdade um conjunto de vários elementos relacionados entre si por $\approx$, enquanto no segundo membro temos os elementos a e b. Isto significa que usamos o par (a, b) como representante da classe $\overline{(a, b)}$, e precisamos ter certeza que esta escolha não afeta as operações.

Sejam então (a,b) e $(\widetilde{a},\widetilde{b})$ representantes da mesma classe, bem como (x,y) e $(\widetilde{x},\widetilde{y})$, isto é, $(a,b) \approx (\widetilde{a},\widetilde{b})$ e também $(x,y) \approx (\widetilde{x},\widetilde{y})$. Da definição da relação temos que $a+\widetilde{b} = b+\widetilde{a}$ e também $x+\widetilde{y} = y+\widetilde{x}$. Segue que

$$(a+x)+(\widetilde{b}+\widetilde{y}) = (a+\widetilde{b})+(x+\widetilde{y}) = (\widetilde{a}+b)+(y+\widetilde{x}) = (\widetilde{a}+\widetilde{x})+(b+y),$$

donde $(a+x, b+y) \approx (\widetilde{a}+\widetilde{x}, \widetilde{b}+\widetilde{y})$, ou ainda, $\overline{(a+x,b+y)} = \overline{(\widetilde{a}+\widetilde{x},\widetilde{b}+\widetilde{y})}$. Então

$$\overline{(a,b)}+\overline{(x,y)} = \overline{(a+x,b+y)} = \overline{(\widetilde{a}+\widetilde{x},\widetilde{b}+\widetilde{y})} = \overline{(\widetilde{a},\widetilde{b})}+\overline{(\widetilde{x},\widetilde{y})},$$

e a adição está bem definida. Também, temos que

$$(a+\widetilde{b})x+(\widetilde{a}+b)y+\widetilde{a}(x+\widetilde{y})+\widetilde{b}(y+\widetilde{x}) = (\widetilde{a}+b)x+(a+\widetilde{b})y+\widetilde{a}(y+\widetilde{x})+\widetilde{b}(x+\widetilde{y}),$$

ou

$$ax+\widetilde{b}x+\widetilde{a}y+by+\widetilde{a}x+\widetilde{a}\widetilde{y}+\widetilde{b}y+\widetilde{b}\widetilde{x} = \widetilde{a}x+bx+ay+\widetilde{b}y+\widetilde{a}y+\widetilde{a}\widetilde{x}+\widetilde{b}x+\widetilde{b}\widetilde{y}.$$

Da lei do cancelamento para a adição de números naturais, resta que

$$ax+by+\widetilde{a}\widetilde{y}+\widetilde{b}\widetilde{x} = bx+ay+\widetilde{a}\widetilde{x}+\widetilde{b}\widetilde{y},$$

ou ainda,

$$(ax+by)+(\widetilde{a}\widetilde{y}+\widetilde{b}\widetilde{x}) = (\widetilde{a}\widetilde{x}+\widetilde{b}\widetilde{y})+(ay+bx),$$

e da definição da relação temos que,

$$\overline{(ax+by,ay+bx)} = \overline{(\widetilde{a}\widetilde{x}+\widetilde{b}\widetilde{y},\widetilde{a}\widetilde{y}+\widetilde{b}\widetilde{x})},$$

donde segue que,

$$\overline{(a,b)}\cdot\overline{(x,y)} = \overline{(ax+by,ay+bx)} = \overline{(\widetilde{a}\widetilde{x}+\widetilde{b}\widetilde{y},\widetilde{a}\widetilde{y}+\widetilde{b}\widetilde{x})} = \overline{(\widetilde{a},\widetilde{b})}\cdot\overline{(\widetilde{x},\widetilde{y})},$$

e a multiplicação também está bem definida.

Vamos agora mostrar propriedades importantes sobre as operações $+$ e $\cdot$ no conjunto $\mathbb{Z}$. Propriedades estas que fazem deste conjunto um anel de integridade.

Teorema 1.1. *A adição de números inteiros é associativa, isto é,*

$$\overline{(a,b)}+\Big(\overline{(x,y)}+\overline{(m,n)}\Big) = \Big(\overline{(a,b)}+\overline{(x,y)}\Big)+\overline{(m,n)},$$

para quaisquer $\overline{(a,b)},\overline{(x,y)},\overline{(m,n)} \in \mathbb{Z}$.

Prova. Dados então $\overline{(a,b)},\overline{(x,y)},\overline{(m,n)} \in \mathbb{Z}$, temos que

$$\begin{aligned}\overline{(a,b)}+\Big(\overline{(x,y)}+\overline{(m,n)}\Big) &= \overline{(a,b)}+\overline{(x+m,y+n)}\\ &= \overline{(a+(x+m),b+(y+n))} = \overline{((a+x)+m,(b+y)+n)}\\ &= \overline{(a+x,b+y)}+\overline{(m,n)} = \Big(\overline{(a,b)}+\overline{(x,y)}\Big)+\overline{(m,n)}.\end{aligned}$$

□

Teorema 1.2. *A adição é comutativa, isto é,*

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(x,y)} + \overline{(a,b)},$$

para quaisquer $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$.

Prova. Se $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$, então

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(a+x, b+y)} = \overline{(x+a, y+b)} = \overline{(x,y)} + \overline{(a,b)},$$

□

Teorema 1.3. *A adição admite um elemento neutro em* $\mathbb{Z}$*. De outra forma, existe um número inteiro, denotado por* 0*, e dito o elemento neutro para a operação de adição, tal que*

$$\overline{(a,b)} + 0 = 0 + \overline{(a,b)} = \overline{(a,b)},$$

para todo $\overline{(a,b)} \in \mathbb{Z}$.

Prova. Vamos mostrar a segunda igualdade da afirmação e a primeira igualdade será consequência da comutatividade da adição. Queremos encontrar um elemento $0 \in \mathbb{Z}$ que deve satisfazer a igualdade desejada. Como elemento do conjunto $\mathbb{Z}$, 0 é uma classe de equivalência. Desta forma, $0 = \overline{(x,y)}$ para algum par $(x,y) \in \mathbb{N} \times \mathbb{N}$. Vamos encontrar este par, ou algum par equivalente a este pela relação de equivalência $\approx$.

Queremos então que $\overline{(x,y)} + \overline{(a,b)} = \overline{(a,b)}$, para qualquer $\overline{(a,b)} \in \mathbb{Z}$. De outra forma, desejamos que $\overline{(a+x, b+y)} = \overline{(a,b)}$. Da definição de classe de equivalência, temos $(a+x, b+y) \approx (a,b)$ e da definição da relação, segue que x e y devem satisfazer $a+x+b = b+y+a$. Da lei do cancelamento da adição de números naturais, segue que $x = y$. Ou seja, $0 = \overline{(x,y)}$ é uma classe de equivalência, onde os representantes são pares ordenados com coordenadas iguais. De fato, dado qualquer $x \in \mathbb{N}$, e qualquer $\overline{(a,b)} \in \mathbb{Z}$, temos que $(a+x)+b = a+(b+x)$, donde $\overline{(a+x, b+x)} = \overline{(a,b)}$, e disto, temos

$$\overline{(x,x)} + \overline{(a,b)} = \overline{(a+x, b+x)} = \overline{(a,b)}.$$

Segue portanto que $0 = \overline{(x,x)}$ para qualquer $x \in \mathbb{N}$. Naturalmente o representante mais simples desta classe é o par $(0,0)$. Escolhemos então $0 = \overline{(0,0)}$, como sendo o elemento neutro do conjunto dos números inteiros para a adição. □

Teorema 1.4. *Todo número inteiro admite simétrico para a operação de adição. Isto é, para todo* $\overline{(a,b)} \in \mathbb{Z}$*, existe um elemento* $-\overline{(a,b)} \in \mathbb{Z}$*, chamado de elemento simétrico de* $\overline{(a,b)}$*, tal que*

$$\overline{(a,b)} + \left(-\overline{(a,b)}\right) = \left(-\overline{(a,b)}\right) + \overline{(a,b)} = 0.$$

Prova. Vamos mostrar apenas a última igualdade e a comutatividade da adição garantirá a primeira igualdade. Dado $\overline{(a,b)} \in \mathbb{Z}$, queremos encontrar $-\overline{(a,b)} = \overline{(x,y)} \in \mathbb{Z}$ que satisfaz $\overline{(x,y)} + \overline{(a,b)} = 0 = \overline{(0,0)}$. Mas isto é equivalente a $\overline{(x+a, y+b)} = \overline{(0,0)}$ que pela igualdade de classes de equivalência significa que $x+a = y+b$. Da definição da relação, esta última igualdade significa que $(x,y) \approx (b,a)$ e então $\overline{(x,y)} = \overline{(b,a)}$. Assim,

$$(-\overline{(a,b)}) + \overline{(a,b)} = \overline{(b,a)} + \overline{(a,b)} = \overline{(a+b, b+a)} = \overline{(0,0)} = 0.$$

Segue que todo elemento $\overline{(a,b)} \in \mathbb{Z}$ possui elemento simétrico para a operação de adição e este elemento simétrico é precisamente o elemento $\overline{(b,a)}$. □

Teorema 1.5. *A multiplicação de números inteiros é associativa, isto é,*

$$\overline{(a,b)} \cdot \left(\overline{(x,y)} \cdot \overline{(m,n)}\right) = \left(\overline{(a,b)} \cdot \overline{(x,y)}\right) \cdot \overline{(m,n)}.$$

para quaisquer $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$.

Prova. Suponha então $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ arbitrários. Então

$$\begin{aligned}
\overline{(a,b)} \cdot \left(\overline{(x,y)} \cdot \overline{(m,n)}\right) &= \overline{(a,b)} \cdot \overline{(xm+yn, xn+ym)} \\
&= \overline{(a(xm+yn)+b(xn+ym), a(xn+ym)+b(xm+yn))} \\
&= \overline{(axm+ayn+bxn+bym, axn+aym+bxm+byn)} \\
&= \overline{((ax+by)m+(ay+bx)n, (ax+by)n+(ay+bx)m)} \\
&= \overline{(ax+by, ay+bx)} \cdot \overline{(m,n)} = \left(\overline{(a,b)} \cdot \overline{(x,y)}\right) \cdot \overline{(m,n)}.
\end{aligned}$$

□

Teorema 1.6. *A multiplicação é distributiva em relação à adição, isto é,*

$$\overline{(a,b)} \cdot \left(\overline{(x,y)} + \overline{(m,n)}\right) = \overline{(a,b)} \cdot \overline{(x,y)} + \overline{(a,b)} \cdot \overline{(m,n)},$$

e

$$\left(\overline{(x,y)} + \overline{(m,n)}\right) \cdot \overline{(a,b)} = \overline{(x,y)} \cdot \overline{(a,b)} + \overline{(m,n)} \cdot \overline{(a,b)},$$

para quaisquer $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$.

Prova. Vamos mostrar a distributividade à esquerda e a distributividade à direita seguirá de forma análoga. Suponha dados arbitrários $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$. Então,

$$\begin{aligned}
\overline{(a,b)} \cdot \left(\overline{(x,y)} + \overline{(m,n)}\right) &= \overline{(a,b)} \cdot \overline{(x+m, y+n)} \\
&= \overline{(a(x+m)+b(y+n), a(y+n)+b(x+m))} \\
&= \overline{(ax+am+by+bn, ay+an+bx+bm)} \\
&= \overline{(ax+by, ay+bx)} + \overline{(am+bn, an+bm)} \\
&= \overline{(a,b)} \cdot \overline{(x,y)} + \overline{(a,b)} \cdot \overline{(m,n)}.
\end{aligned}$$

□

O leitor atento dirá que poderíamos ter primeiro demonstrado a comutatividade do produto para garantir a distributividade à direita no teorema anterior. O detalhe é que o que fizemos até agora garante que a terna ordenada $(\mathbb{Z}, +, \cdot)$ é um anel. Não é necessária a comutatividade do produto para garantir isto. Assim que mostrarmos a comutatividade do produto o anel se tornará um anel comutativo.

Teorema 1.7. *A multiplicação é comutativa em* $\mathbb{Z}$*, isto é,*

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(x,y)} \cdot \overline{(a,b)},$$

para quaisquer $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$.

Prova. Sejam então $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$ arbitrários. Temos que

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(ax+by, ay+bx)} = \overline{(xa+yb, ya+xb)} = \overline{(x,y)} \cdot \overline{(a,b)}.$$

□

Teorema 1.8. *A multiplicação admite elemento neutro em $\mathbb{Z}$. Em outras palavras, $\mathbb{Z}$ possui unidade, isto é, existe um numero inteiro, representado por* 1*, tal que*

$$1 \cdot \overline{(a,b)} = \overline{(a,b)} \cdot 1 = \overline{(a,b)},$$

para qualquer $\overline{(a,b)} \in \mathbb{Z}$.

Prova. Vamos encontrar um elemento $1 = \overline{(x,y)} \in \mathbb{Z}$ de forma que $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)}$, para qualquer $\overline{(a,b)} \in \mathbb{Z}$. Da igualdade desejada, $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)}$, temos que, $\overline{(xa+yb, xb+ya)} = \overline{(a,b)}$. Da definição de classe de equivalência, $(xa+yb, xb+ya) \approx (a,b)$ e da definição da relação segue que x e y devem satisfazer

$$ax + by + b = a + bx + ay. \tag{1}$$

Esta última igualdade norteia a busca do elemento unidade $\overline{(x,y)}$. Vamos considerar três casos exclusivos.

Caso 1: $a = b$. Neste caso, $\overline{(a,b)} = \overline{(0,0)} = 0 \in \mathbb{Z}$ e então

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(0,0)} \cdot \overline{(x,y)} = \overline{(0x+0y, 0y+0x)} = \overline{(0,0)} = \overline{(a,b)},$$

para qualquer escolha do elemento $\overline{(x,y)} \in \mathbb{Z}$.

Caso 2: $a > b$. Neste caso, da relação de ordem do conjunto dos números naturais existe $n \in \mathbb{N}^*$ tal que $a = b + n$. Substituindo a na igualdade (1), temos $(b+n)x + by + b = (b+n) + bx + (b+n)y$, e pela lei do cancelamento de números naturais para a adição segue que $nx = n + ny$, ou ainda $nx = n(1+y)$. Agora como $n \in \mathbb{N}^*$ então pela lei do cancelamento de números naturais não nulos para o produto, temos $x = y + 1$.

Caso 3: $a < b$. Existe então $n \in \mathbb{N}^*$ tal que $a + n = b$ e substituindo isto na igualdade (1), temos $ax + (a+n)y + (a+n) = a + (a+n)x + ay$. Novamente, pela lei do cancelamento de números naturais para a adição, temos $ny + n = nx$ e do cancelamento de números não nulos para o produto, vem $y + 1 = x$.

Os três casos nos mostram que o número inteiro $1 = \overline{(x,y)} \in \mathbb{Z}$ procurado é $\overline{(y+1,y)}$. De fato, para qualquer $\overline{(a,b)} \in \mathbb{Z}$,

$$\overline{(y+1,y)} \cdot \overline{(a,b)} = \overline{((y+1)a+yb, (y+1)b+ya)} = \overline{(ya+a+yb, yb+b+ya)} = \overline{(a,b)}.$$

Claro que o representante mais simples da classe $\overline{(y+1,y)}$ é o elemento $\overline{(1,0)}$ e deste ponto em diante, a unidade do conjunto $\mathbb{Z}$ é entendida como sendo o elemento $\overline{(1,0)} \in \mathbb{Z}$.

A igualdade $\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(a,b)}$ é garantida pela comutatividade da multiplicação.

□

Desta forma a terna ordenada $(\mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade.

Teorema 1.9. *O conjunto $\mathbb{Z}$ não possui divisores próprios de 0, isto é, se $\overline{(a,b)} \cdot \overline{(x,y)} = 0$ então $\overline{(a,b)} = 0$ ou $\overline{(x,y)} = 0$.*

Prova. Sejam $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$, tais que $\overline{(a,b)} \cdot \overline{(x,y)} = 0 = \overline{(0,0)}$, e suponha que $\overline{(a,b)} \neq \overline{(0,0)}$. Consequentemente $a \neq b$. Temos então que $\overline{(ax+by, bx+ay)} = \overline{(0,0)}$, e então $(ax+by, bx+ay) \approx (0,0)$. Da definição da relação, segue que $ax+by = bx+ay$. Como $a \neq b$, restam ainda dois casos exclusivos.

Caso 1: $a < b$. Existe então $k \in \mathbb{N}^*$, tal que $a + k = b$, e usando este fato temos que $ax+(a+k)y = (a+k)x+ay$, e pela lei do cancelamento de números naturais para a adição, vem $ky = kx$. Esta por sua vez, pela lei do cancelamento de números naturais não nulos para a multiplicação nos leva a $y = x$, isto é, $\overline{(x,y)} = \overline{(0,0)} = 0$.

Caso 2: $b < a$. Neste caso $a = b+k$ para algum $k \in \mathbb{N}^*$. Substituindo em $ax+by = bx+ay$, chegamos a $(b+k)x + by = bx + (b+k)y$ e pelas mesmas leis de cancelamento citadas no caso 1, temos também que $x = y$. Segue aqui também que $\overline{(x,y)} = \overline{(0,0)} = 0$. □

Este último teorema garante que o conjunto $\mathbb{Z}$ é um anel de integridade, dito anel de integridade dos números inteiros. O conjunto dos números inteiros não é um corpo, e portanto este é o ponto máximo que podemos chegar no sentido da estrutura algébrica deste conjunto. Contudo ainda mostraremos a lei do cancelamento de elementos não nulos para a multiplicação.

Teorema 1.10. *Se $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ tais que $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)} \cdot \overline{(m,n)}$ e $\overline{(a,b)} \neq \overline{(0,0)}$ então $\overline{(x,y)} = \overline{(m,n)}$.*

Prova. Suponha então $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ satisfazendo $\overline{(a,b)} \neq \overline{(0,0)}$, e portanto $a \neq b$, e também $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)} \cdot \overline{(m,n)}$. Segue desta última igualdade que

$$\overline{(ax+by, ay+bx)} = \overline{(am+bn, an+bm)},$$

ou ainda

$$ax + by + an + bm = ay + bx + am + bn. \tag{2}$$

Como $a \neq b$ vamos ainda considerar dois casos exclusivos.

Caso 1: $(a < b)$. Neste caso $a + k = b$ para algum $k \in \mathbb{N}^*$. Logo temos de (2) que

$$ax + ay + ky + an + am + km = ay + ax + kx + am + an + kn,$$

e da lei do cancelamento para a soma de números naturais, temos $k(y+m) = k(x+n)$ e usando a lei do cancelamento para o produto de números naturais não nulos, segue que $y + m = x + n$ ou ainda $(x,y) \approx (m,n)$ e isto significa que $\overline{(x,y)} = \overline{(m,n)}$.

Caso 2: $(a > b)$. Agora $b+k = a$ para algum $k \in \mathbb{N}^*$, e com isto em (2) obtemos a igualdade

$$bx + kx + by + bn + kn + bm = by + ky + bx + bm + km + bn,$$

e das leis do cancelamento segue (como no caso 1) que $y+m = x+n$ e portanto $\overline{(x,y)} = \overline{(m,n)}$.
□

Como complemento para esta seção, iremos ainda definir uma ordem total no anel de integridade $(\mathbb{Z}, +, \cdot)$. Dados $\overline{(a,b)}$ e $\overline{(x,y)}$ em $\mathbb{Z}$, definimos a relação $\leq$ por

$$\overline{(a,b)} \leq \overline{(x,y)} \qquad \text{se e somente se} \qquad a+y \leq x+b,$$

sendo que ao dizer $a+y \leq x+b$ nos referimos à relação de ordem do conjunto dos naturais. Desta forma, usando a definição de ordem do conjunto dos números naturais, podemos escrever

$$\overline{(a,b)} \leq \overline{(x,y)} \qquad \text{se e somente se} \qquad a+y+k = x+b \quad \text{para algum} \quad k \in \mathbb{N}.$$

Vamos mostrar que esta relação é uma relação de ordem total no conjunto $\mathbb{Z}$. Primeiro claro que precisamos mostrar que $\leq$ está bem definida. Isto se deve ao fato de que estamos trabalhando com classes de equivalência e precisamos mostrar que se $\overline{(a,b)} \leq \overline{(x,y)}$ isto não deve depender dos representantes (a,b) e (x,y) escolhidos para cada classe. Sejam então $\overline{(a,b)} = \overline{(\widetilde{a},\widetilde{b})}$ e $\overline{(x,y)} = \overline{(\widetilde{x},\widetilde{y})}$, isto é, $(a,b) \approx (\widetilde{a},\widetilde{b})$ e $(x,y) \approx (\widetilde{x},\widetilde{y})$, e da definição da relação, $a+\widetilde{b} = \widetilde{a}+b$ e $x+\widetilde{y} = \widetilde{x}+y$. Assim,

$$\begin{aligned}
\overline{(a,b)} \leq \overline{(x,y)} \quad &\Leftrightarrow \quad a+y+k = x+b, \quad \text{para algum} \quad k \in \mathbb{N}. \\
&\Leftrightarrow \quad (a+\widetilde{b})+(\widetilde{x}+y)+k = x+b+\widetilde{b}+\widetilde{x}, \quad \text{para algum} \quad k \in \mathbb{N}. \\
&\Leftrightarrow \quad (\widetilde{a}+b)+(x+\widetilde{y})+k = x+b+\widetilde{b}+\widetilde{x}, \quad \text{para algum} \quad k \in \mathbb{N}. \\
&\Leftrightarrow \quad \widetilde{a}+\widetilde{y}+k = \widetilde{b}+\widetilde{x}, \quad \text{para algum} \quad k \in \mathbb{N}. \\
&\Leftrightarrow \quad \overline{(\widetilde{a}+\widetilde{b})} \leq \overline{(\widetilde{x}+\widetilde{y})}.
\end{aligned}$$

Vamos agora provar que $\leq$ é uma relação de ordem total no conjunto $\mathbb{Z}$. Como $a+b = b+a$, para quaisquer $a, b \in \mathbb{N}$, então temos que $\overline{(a,b)} \leq \overline{(a,b)}$, e a relação é reflexiva.

Dados agora, $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$, com $\overline{(a,b)} \leq \overline{(x,y)}$ e $\overline{(x,y)} \leq \overline{(a,b)}$ temos, da definição da relação, que $a+y+k = x+b$ e $x+b+r = a+y$ para algum $k, r \in \mathbb{N}$. Mas assim, $x+b = a+y+k = x+b+r+k$ e da lei do cancelamento para a adição de naturais, temos que $0 = r+k$. Mas esta igualdade somente pode ser cumprida em $\mathbb{N}$ se $r = k = 0$. Desta forma $a+y = x+b$ e da definição da relação $\approx$ temos que $(a,b) \approx (x,y)$ o que significa que $\overline{(a,b)} = \overline{(x,y)}$ e a relação é antissimétrica.

Se $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$, com $\overline{(a,b)} \leq \overline{(x,y)}$ e $\overline{(x,y)} \leq \overline{(m,n)}$, então da definição da relação temos que $a+y+k = x+b$ e $x+n+r = m+y$ para algum $k, r \in \mathbb{N}$. Mas assim, $m+b+x = m+a+y+k = x+n+r+a+k$. Da lei do cancelamento de naturais para a adição, temos que $m+b = a+n+(r+k)$. Como $(r+k) \in \mathbb{N}$ então segue que $\overline{(a,b)} \leq \overline{(m,n)}$. Temos a transitividade da relação, que é portanto uma relação de ordem.

Para provar que a relação é de ordem total, sejam $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$. Então para os números naturais $(a+y)$ e $(x+b)$, como a relação $\leq$ é uma relação de ordem total em $\mathbb{N}$, temos que $a+y \leq x+b$ ou $x+b \leq a+y$, donde

$$\overline{(a,b)} \leq \overline{(x,y)} \qquad \text{ou} \qquad \overline{(x,y)} \leq \overline{(a,b)},$$

e a relação de ordem é total.

2 Divisibilidade no conjunto dos números inteiros

Embora tenhamos construído o conjunto dos números inteiros como classes de pares ordenados de $\mathbb{N} \times \mathbb{N}$, vamos agora denotar um número inteiro apenas por uma letra minúscula (como estamos habituados). Dentro desta nova notação para números inteiros, consideramos que,

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

é ordenado, e dotado de (pelo menos) duas operações, chamadas de adição e de multiplicação, representadas respectivamente por $+$ e $\cdot$, as quais possuem as seguintes propriedades (mostradas na seção anterior):

i) $a + (b + c) = (a + b) + c$,

ii) $a + b = b + a$,

iii) $a + 0 = 0 + a = a$,

iv) $a + (-a) = (-a) + a = 0$,

v) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

vi) $a \cdot (b + c) = a \cdot b + a \cdot c$,

vii) $a \cdot b = b \cdot a$,

viii) $1 \cdot a = a \cdot 1 = a$,

ix) Se $(a \cdot b) = 0$, então $b = 0$ ou $a = 0$,

x) Se $a \cdot b = a \cdot c$, e $a \neq 0$, então $b = c$,

para quaisquer números inteiros a, b e c. A operação de multiplicação (ou produto) será subentendida quando apresentados dois números inteiros sem qualquer sinal separando-os. Isto significa que ab será entendido como $a \cdot b$, para quaisquer inteiros a e b.

Definição 2.1. Dados dois números inteiros a e $b \neq 0$, dizemos que b divide a, ou equivalentemente, que a é divisível por b, se existir algum número k, inteiro também, e unicamente determinado, de forma que $a = b \cdot k = bk$, e representamos este fato escrevendo $b|a$. O número a é ainda chamado de múltiplo de b e b é chamado de divisor de a.

Note que esta definição é resumida na condição

$$b|a \qquad \Leftrightarrow \qquad a = bk = kb, \quad \text{para algum} \quad k \in \mathbb{Z}.$$

Se isto não acontecer, isto é, nao existir tal número inteiro k, que satisfaz $a = bk$, então dizemos que b não divide a, ou que a não é múltiplo de b, e representamos este fato escrevendo $b \nmid a$.

Na definição anterior, exigimos que $b \neq 0$, pois se tivéssemos $b = 0$, então a igualdade $a = bk = 0k = 0$, só ficaria válida para $a = 0$. Mas por outro lado, se $a = 0$,

então o número k não fica unicamente determinado. Em outros termos, dizemos que 0 não divide ninguém. Desta forma, sempre que usarmos a expressão $b|a$ estaremos supondo implicitamente que b é não nulo, exatamente como a definição pede. Mas note também que nada impede de que a seja zero, pois sendo assim, para qualquer b não nulo, a igualdade $0 = a = bk$, faz $k = 0$ unicamente determinado. Por isso, dizemos que qualquer número inteiro (não nulo) divide 0, ou ainda, 0 é múltiplo de qualquer número inteiro (não nulo).

Observe ainda, que se $b|a$, e a é diferente de 0 então devemos ter obrigatoriamente que $|b| \leq |a|$.

Teorema 2.1 (Algoritmo da divisão de Euclides). *Dados dois números inteiros* a *e* $b \neq 0$, *então existem únicos* $q, r \in \mathbb{Z}$, *chamados respectivamente de quociente e resto da divisão Euclidiana, tais que,*

$$a = qb + r \quad \textit{com} \quad 0 \leq r < |b|.$$

Prova. Primeiro mostraremos que existem os números q e r. Também, se $b|a$ então a igualdade fica cumprida para $r = 0$. Vamos considerar então que b não divide a, ou que a não é múltiplo de b. Vamos considerar dois casos.

Caso 1: $(b > 0)$. Neste caso, observemos o conjunto dos múltiplos de b, que é,

$$M_b = \{\ldots, (-k)b, (-k+1)b, \ldots, -3b, -2b, -b, 0, b, 2b, 3b, \ldots, kb, (k+1)b, \ldots\}.$$

Como a não é múltiplo de b, então a está entre dois múltiplos consecutivos de b, isto é, $qb < a < (q+1)b$, e temos $qb < a < qb + b$ ou equivalentemente, $0 < a - qb < b$. Tomando $r = a - qb$ temos que $a = qb + (a - qb) = qb + r$, e como $0 < a - qb < b$, vem $0 < r < b = |b|$.

Caso 2: $(b < 0)$. Neste caso, o conjunto dos múltiplos de b agora é

$$M_b = \{\ldots, (k)b, (k-1)b, \ldots, 3b, 2b, b, 0, -b, -2b, -3b, \ldots, (-k)b, (-k-1)b, \ldots\},$$

e como a não é múltiplo de b, da mesma forma que no caso 1, a deve estar entre dois múltiplos consecutivos de b, ou seja, $qb < a < (q-1)b$, e então, $qb < a < qb - b$ ou equivalentemente $0 < a - qb < -b$. Tomando $r = a - qb$, temos que $a = qb + (a - qb) = qb + r$, e já que $0 < a - qb < -b$, então $0 < r < -b = |b|$.

Agora mostraremos que os números q e r são únicos. Suponhamos então q_1, q_2, r_1 e r_2 tais que $a = q_1b + r_1 = q_2b + r_2$. Então $(q_1 - q_2)b = r_2 - r_1$ com $0 \leq r_1, r_2 < |b|$. Isto significa que $b|(r_2 - r_1)$. Mas note que também $-b < r_2 - r_1 < b$, e como o único múltiplo de b estritamente entre $-b$ e b é 0, temos que $r_2 - r_1 = 0$, donde segue que $r_2 = r_1$.

Com $(r_2 - r_1) = 0$ temos que $(q_1 - q_2)b = 0$ e como $b \neq 0$ segue que $(q_1 - q_2) = 0$, donde também $q_1 = q_2$. □

Um fato importante, é que se $b|a$ e somente neste caso, então o número r da igualdade $a = qb + r$ é igual a zero. A próxima proposição reune algumas propriedades a respeito da divisibilidade de números inteiros.

Proposição 2.2. *Se* a, b *e* c *são números inteiros arbitrários, então valem as seguintes propriedades:*

i) $a|a$,

ii) Se $a|b$ *e* $b|a$, *então* $a = \pm b$,

iii) Se $a|b$ *e* $b|c$, *então* $a|c$,

iv) Se $(ac)|(bc)$ *então* $a|b$,

v) Se $a|b$ *e* $a|c$, *então* $a|(bx + cy)$ *para quaisquer* $x, y \in \mathbb{Z}$,

vi) Se $a|b$ *e* $c|d$, *então* $(ac)|(bd)$.

Prova. A condição (i) é imediata pois $a = 1 \cdot a$. Para provar (ii), suponha que $a|b$ e que $b|a$. Então $b = ma$ e $a = nb$, para algum $m, n \in \mathbb{Z}$. Desta forma, $b = ma = m(nb) = (mn)b$, e como $b \neq 0$ então $1 = mn$. Mas isto só será possível se $m = n = \pm 1$, donde $a = \pm b$. Para provar (iii), suponhamos $a|b$ e $b|c$. Então temos que, $b = am$ e $c = bn$ com $m, n \in \mathbb{Z}$. Desta forma $c = bn = (am)n = a(mn)$ e como $(mn) \in \mathbb{Z}$, temos que $a|c$. Para provar (iv) suponha que $(ac)|(bc)$, e então $bc = kac$ para algum $k \in \mathbb{Z}$. Como ac é não nulo, então a e c são não nulos, e da lei do cancelamento para elementos não nulos no produto, $b = ka$ para algum $k \in \mathbb{Z}$ donde $a|b$. Para provarmos (v), suponha que $a|b$ e $a|c$. Temos assim, $b = am$ e $c = an$ com $m, n \in \mathbb{Z}$. Para quaisquer $x, y \in \mathbb{Z}$, temos que $(bx + cy) = (am)x + (an)y = a(mx) + a(ny) = a(mx + ny)$, e como $(mx + ny) \in \mathbb{Z}$, segue que $a|(bx + cy)$. Para a última afirmação, suponha $a|b$ e $c|d$. Então $b = am$ e $d = cn$, para $m, n \in \mathbb{Z}$. Então $(bd) = (ma)(nc) = (mn)(ac)$, e como $mn \in \mathbb{Z}$, segue que $(ac)|(bd)$. Isto finaliza esta demonstração. □

Dados dois números inteiros a e b, consideremos o conjunto dos múltiplos de a, dado por,

$$M_a = \{ka; \quad k \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \pm 3a, \pm 4a, \dots\},$$

e o conjunto dos múltiplos de b dado por

$$M_b = \{kb; \quad k \in \mathbb{Z}\} = \{0, \pm b, \pm 2b, \pm 3b, \pm 4b, \dots\}.$$

É bastante claro que estes conjuntos possuem elementos em comum (além de 0). Os elementos $\pm ab$ são elementos de M_a e também de M_b e um deles deve ser positivo. Ao menor elemento, positivo (não nulo portanto), comum aos dois conjuntos M_a e M_b, isto é, o menor número inteiro positivo, múltiplo ao mesmo tempo de a de b, chamaremos de mínimo múltiplo comum entre a e b, e representaremos por $\text{mmc}(a, b)$. Se algum dos números a ou b for igual a zero, e somente neste caso, então definimos $\text{mmc}(a, b) = 0$. É um fato também que $a| \text{mmc}(a, b)$ e $b| \text{mmc}(a, b)$.

Apresentamos a seguir a definição formal de $\text{mmc}(a, b)$.

Definição 2.2. Dados dois inteiros a e b ambos não nulos, dizemos que o número natural m é o mínimo múltiplo comum entre a e b, e escrevemos $m = \text{mmc}(a, b)$, se

a) $a|m$ e $b|m$,

b) Se $a|n$ e $b|n$, para algum outro $n \in \mathbb{Z}$, então $m|n$.

Se a ou b forem iguais a zero, então definimos $mmc(a, b) = 0$.

Dados dois números inteiros a e b, consideremos o conjunto dos divisores de a, dado por,

$$D_a = \{\pm 1, \pm a_1, \pm a_2, \pm a_3, \ldots, \pm a\},$$

e o conjunto dos divisores de b, dado por,

$$D_b = \{\pm 1, \pm b_1, \pm b_2, \pm b_3, \ldots, \pm b\}.$$

Estes conjuntos também possuem elementos em comum. O número 1 é um elemento que pertence aos dois conjuntos simultaneamente. Ao maior elemento, comum aos dois conjuntos D_a e D_b, isto é, o maior número inteiro, divisor ao mesmo tempo de a e de b, chamaremos de máximo divisor comum entre a e b, e representamos por $mdc(a, b)$. Se os números a e b forem iguais a zero, e somente neste caso, definimos $mdc(a, b) = 0$. Claramente temos que $mdc(a, b)|a$ e $mdc(a, b)|b$.

Além disso, é fato também que $mdc(a, b) \geq 0$. A definição formal de $mdc(a, b)$, é a que segue.

Definição 2.3. Dados dois inteiros a e b não simultaneamente nulos, dizemos que o natural d é o máximo divisor comum entre a e b, e representamos por $d = mdc(a, b)$, se

i) $d|a$ e $d|b$,

ii) Se $n|a$ e $n|b$, para algum outro $n \in \mathbb{Z}$, então $n|d$.

Se $a = b = 0$ então definimos $mdc(a, b) = 0$.

Definição 2.4. Um número natural p, não nulo e diferente de 1 é dito um número primo se o conjunto D_p, de seus divisores inteiros, é o conjunto

$$D_p = \{\pm 1, \pm p\}.$$

Observe que se exigíssemos que um número natural é primo se e somente se o conjunto de seus divisores possuir exatamente 4 elementos, então não precisaríamos pedir que p fosse não nulo e diferente de 1. Podemos estender esta definição de números primos para todo número inteiro. Neste caso números negativos também podem ser considerados números primos, desde que possuam exatamente 4 divisores distintos.

Definição 2.5. Dois números inteiros a e b, são ditos primos entre si, se (e somente se), $mdc(a, b) = 1$.

Proposição 2.3. *Se a e b são números inteiros, então existem m e n inteiros também, tais que* $mdc(a, b) = ma + nb$.

Prova. No caso em que $a = b = 0$, então $mdc(a, b) = 0$, e a igualdade é satisfeita com $m = n = 0$. No caso em que apenas um dos números, digamos a, é não nulo, temos que $mdc(a, 0) = a$ e a igualdade fica satisfeita com $m = n = 1$.

Consideremos agora o caso em que a e b são ambos não nulos. Seja $d = mdc(a, b)$. Considere S o conjunto de números positivos da forma $xa + yb$, isto é,

$$S = \{xa + yb; \qquad x, y \in \mathbb{Z}, \quad xa + yb > 0\}.$$

Este conjunto não é vazio, pois sabemos que a ou $-a$, e também b ou $-b$, estão em S. Mas sendo S um conjunto de valores positivos deve haver um destes valores que é o menor entre eles. Tomemos $k = \min\{S\} > 0$. Como $k \in S$, então $k = ma + nb$ para algum $m, n \in \mathbb{Z}$. Como $d|a$ e também $d|b$ temos pela condição (v) da proposição 2.2 que $d|(ma+nb)$, e então $d|k$. Por outro lado, afirmamos que $k|a$, pois caso contrário ($k \nmid a$), existiriam $q, r \in \mathbb{Z}$, de tal forma que $a = qk + r$, com $0 < r < k$, e assim, $r = a - qk = a - q(ma + nb) = a - qma - qnb = (1 - qm)a - (qn)b$.

Desta forma, $r > 0$ e $r \in S$, com $r < k$, contradizendo o fato de que $k = \min\{S\}$. Sendo assim, ocorre de fato que $k|a$. Um processo análogo mostrará que $k|b$ também. Segue que k é um divisor comum entre a e b. Então da condição (ii) da definição de mdc temos que $k|d$. Como $d|k$ segue que $k = \pm d$ mas como ambos devem ser positivos, temos que $k = d$, isto é $mdc(a, b) = d = k = ma + nb$. □

Corolário 2.4. *Sejam a e b números inteiros não nulos. Então a e b são primos entre si, se e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Prova. Se a e b são primos entre si então a proposição anterior garante a igualdade desejada.

Suponha então que existem $m, n \in \mathbb{Z}$ tais que $am+bn = 1$. Seja $mdc(a, b) = d > 0$. Então, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = dk_1$ e $b = dk_2$. Nestes termos, $dk_1m + dk_2n = 1$, ou ainda, $d(k_1m + k_2n) = 1$, e portanto d é um divisor (positivo) de 1. Segue que $d = 1$. □

Lema 2.5. *Se a, b e c são números inteiros, com a e b primos entre si, e além disso, $a|c$ e $b|c$, então $(ab)|c$.*

Prova. Do corolário 2.4, existem números inteiros m e n tais que $1 = ma + nb$. Então temos que $(ma+nb)c = c$, ou ainda, $m(ac)+n(bc) = c$. Ora, $a|c$ e então do item (iv) da proposição 2.2, $(ab)|(bc)$, e como $b|c$, também temos que $(ab)|(ac)$. Do item (v) da mesma proposição temos que $(ab)|(m(ac) + n(bc))$, ou seja, $(ab)|c$. □

Lema 2.6. *Sejam a e b dois números inteiros, com $d = mdc(a, b)$. Então se existem $m, n \in \mathbb{Z}$ tais que $a = md$ e $b = nd$, temos que m e n são primos entre si, ou seja, $mdc(m, n) = 1$.*

Prova. Suponha que $k = mdc(m, n)$, então k é divisor de m e n, isto é $m = m_1k$ e $n = n_1k$, e assim $a = md = m_1kd$, e $b = nd = n_1kd$, mostrando que kd é divisor comum de a e de b. Mas como d é o máximo entre os divisores comuns de a e b, da definição de máximo divisor comum, devemos ter $kd|d$. Do item (iv) da proposição 2.2 temos $k|1$, donde $k = \pm 1$. Mas devendo ser $k \geq 0$, segue que $k = 1$. □

Teorema 2.7. *Para quaisquer a e b inteiros, tem-se $|ab| = mmc(a, b) \cdot mdc(a, b)$.*

Prova. Se $a = 0$, ou $b = 0$, então a igualdade é óbvia pois $\text{mmc}(a, b) = 0$, e também $ab = 0$. Suponha agora $a \neq 0$ e $b \neq 0$. Como $\text{mdc}(a, b)$ e $\text{mmc}(a, b)$ são ambos positivos, então é suficiente verificar a expressão para a e b também positivos. Assim, suponha $a > 0$ e $b > 0$, e consequentemente $m = \text{mmc}(a, b) > 0$, e $d = \text{mdc}(a, b) > 0$. Então $d|a$, $d|b$ e também $d|ab$, isto é, $a = k_1 d$, $b = k_2 d$, $ab = k_3 d$ para algum $k_1, k_2, k_3 \in \mathbb{Z}$, e mais ainda, k_1, k_2 e k_3 são positivos, e do lema 2.6, k_1 e k_2 são primos entre si. Temos então que $k_3 d = ab = (k_1 d)(k_2 d) = k_1 k_2 dd$, e como $d \neq 0$ temos $k_3 = k_1 k_2 d$. Segue que $k_3 = ak_2 = bk_1$. Desta forma, k_3 é um múltiplo comum entre a e b, e assim $m \leq k_3$, pois m é o mínimo entre os múltiplos comuns de a e b. Por outro lado, $d|a$ e $a|m$, então $d|m$, isto é, $m = m_0 d$ para algum $m_0 \in \mathbb{Z}$ positivo. Então, de $a|m$ temos $(k_1 d)|(m_0 d)$, e de $b|m$ temos $(k_2 d)|(m_0 d)$, e assim, $k_1|m_0$ e também $k_2|m_0$. Sendo k_1 e k_2 primos entre si, então do lema 2.5, $(k_1 k_2)|m_0$, e então $(k_1 k_2 d)|(m_0 d)$, ou seja, $k_3|m$, e assim, $k_3 \leq m$. Concluimos que $k_3 = m$, e portanto $ab = k_3 d = md = \text{mmc}(a, b) \cdot \text{mdc}(a, b)$. □

Corolário 2.8. *Se a e b são dois números inteiros primos entre si, então* $\text{mmc}(a, b) = |ab|$.

3 Congruência módulo m

O que vamos apresentar agora é um dos exemplos mais importantes de classes de equivalência, chamado conjunto das classes de equivalência $\mathbb{Z}$ módulo m. Consideremos o conjunto dos números inteiros,

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}.$$

Escolhemos um inteiro arbitrário $m \geq 2$, e definimos em $\mathbb{Z}$ a relação $\approx$ dada por

$$x \approx y \qquad \text{se e somente se} \qquad m|(x - y).$$

É comum escrever $x \equiv y (\text{mod } m)$ para dizer que $m|(x - y)$. A expressão $x \equiv y \,(\text{mod } m)$ deve ser lida como: "x é congruente a y módulo m", ou ainda, "x é equivalente a y módulo m".

Vamos verificar agora que esta relação é uma relação de equivalência sobre o conjunto dos números inteiros. Primeiro temos que $m|0$ e então $m|(x - x)$ para todo $x \in \mathbb{Z}$, logo, $x \approx x$ para todo $x \in \mathbb{Z}$, isto é, $\approx$ e reflexiva. Suponha agora $x \approx y$, e então, $m|(x-y)$. Do item (v) da proposição 2.2, $m|(k(x-y))$ para qualquer inteiro k. Em particular $m|((-1)(x-y))$, ou ainda, $m|(y - x)$. Desta forma, $y \approx x$, mostrando que $\approx$ é simétrica. Também, sejam $x, y, z \in \mathbb{Z}$ com $x \approx y$ e $y \approx z$, isto é, $m|(x - y)$ e $m|(y - z)$. Então temos do item (v) da proposição 2.2 que $m|(k_1(x - y) + k_2(y - z))$ para quaisquer $k_1, k_2 \in \mathbb{Z}$. Em particular, $m|((x - y) + (y - z))$, isto é, $m|(x - z)$ e temos portanto $x \approx z$, mostrando a transitividade de $\approx$. Desta forma $\approx$ é de fato uma relação de equivalência.

Observe que dizer que $x \approx y$, ou equivalentemente $m|(x-y)$, significa que os restos da divisão euclidiana de x e de y por m, são iguais. De fato, do algoritmo de Euclides, temos que existem q_1, q_2, r_1 e r_2 tais que $x = q_1 m + r_1$ e $y = q_2 m + r_2$, com $0 \leq r_1, r_2 < m$. Como

$m|(x-y)$ então $m|[(q_1-q_2)m+(r_1-r_2)]$. Como m divide uma soma, e divide uma das parcelas desta soma, então obrigatoriamente, m divide a outra parcela desta soma também. Isto é, $m|(r_1-r_2)$ ou (r_1-r_2) é múltiplo de m. Como $0 \leq r_1, r_2 < m$ então $-m < r_1 - r_2 < m$. Mas sendo (r_1-r_2) múltiplo de m, e o único múltiplo de m entre $-m$ e m é 0, então $r_1 - r_2 = 0$, ou ainda, $r_2 = r_1$, provando a nossa afirmação. A recíproca e obviamente verdadeira, isto é, se os restos r_1 e r_2 são iguais, então $(x-y) = (q_1m + r_1) - (q_2m - r_2) = (q_1 - q_2)m$ e então $m|(x-y)$.

Assim, podemos construir as classes de equivalência $\overline{z}$ para cada $z \in \mathbb{Z}$. Note que $\overline{z}$ consiste de todos os núumeros inteiros relacionados com z, isto é, todos os números inteiros que deixam o mesmo resto que z na divisão Euclidiana por m. Temos então,

$$\begin{aligned}
\overline{0} &= \{0, \pm m, \pm 2m, \pm 3m, \pm 4m, \dots\} \\
\overline{1} &= \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, ...\} \\
\overline{2} &= \{2, 2 \pm m, 2 \pm 2m, 2 \pm 3m, ...\} \\
\overline{3} &= \{3, 3 \pm m, 3 \pm 2m, 3 \pm 3m, ...\} \\
&\vdots \\
\overline{m-1} &= \{m-1, (m-1) \pm m, (m-1) \pm 2m, (m-1) \pm 3m, \dots\} \\
&= \{-1, -1 \pm m, -1 \pm 2m, -1 \pm 3m, \dots\} = \overline{-1} \\
\overline{m} &= \{m, m \pm m, m \pm 2m, m \pm 3m, \dots\} = \{0, \pm m, \pm 2m, \pm 3m, \dots\} = \overline{0}
\end{aligned}$$

e a partir daí as classes se repetem, e portanto, temos m classes de equivalência distintas, chamadas classes de equivalência módulo m. O conjunto destas classes de equivalência, denotado por $\mathbb{Z}_m$ é

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{\approx} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}.$$

Note que o conjunto $\mathbb{Z}_m$ tem exatamente m elementos. Vamos definir neste conjunto duas operações e verificar que estas operações possuem propriedades importantes. Para cada $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos a soma $\overline{a} + \overline{b}$ por

$$\overline{a} + \overline{b} = \overline{a+b},$$

e o produto $\overline{a}\overline{b} = \overline{a} \cdot \overline{b}$ por

$$\overline{a}\overline{b} = \overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{ab}.$$

Observe nas definições de soma e produto acima, que no primeiro membro temos a soma e o produto de duas classes, enquanto no segundo membro a soma e o produto incidem sobre os representantes a e b. Uma pergunta natural surge agora. Já que a não é o único elemento que está na classe $\overline{a}$, perguntamos se a soma e o produto ainda são os mesmos (no sentido da relação de equivalência), tomando outro elemento da classe $\overline{a}$ (ou da classe $\overline{b}$). O que faremos então é mostrar que estas operações estão bem definidas, isto é, dados $a \approx x$ e $b \approx y$ mostraremos que $\overline{a} + \overline{b} = \overline{x} + \overline{y}$ e que $\overline{a} \cdot \overline{b} = \overline{x} \cdot \overline{y}$.

Se $a \approx x$ e $b \approx y$ então $m|(a-x)$ e $m|(b-y)$, e assim $m|(a-x+b-y)$ ou $m|((a+b)-(x+y))$ e da definição da relação segue que $(a+b) \approx (x+y)$ ou ainda,

$\overline{a+b} = \overline{x+y}$. Então

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{x+y} = \overline{x} + \overline{y},$$

e a operação de adição está bem definida. Para a multiplicação, como $m|(a-x)$ e $m|(b-y)$, temos $m|((a-x)b)$ e $m|((b-y)x)$, donde $m|[(a-x)b+(b-y)x]$. Isto é, $m|(ab-xb+bx-yx)$ ou ainda $m|(ab-xy)$ e da definição da relação segue que $(ab) \approx (xy)$ ou ainda, $\overline{ab} = \overline{xy}$. Então

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{xy} = \overline{x} \cdot \overline{y},$$

e a operação multiplicação está bem definida.

Agora, dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, temos

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}),$$

e também

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a},$$

donde seguem a associatividade e a comutatividade de $+$ em $\mathbb{Z}_m$. Procuramos agora um elemento neutro para $+$ em $\mathbb{Z}_m$, isto é desejamos encontrar $e \in \mathbb{Z}_m$ tal que $\overline{a} + e = e + \overline{a} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$. Mas como elemento de $\mathbb{Z}_m$, temos que $e = \overline{x}$ para algum $x \in \mathbb{Z}$. Desejamos então encontrar $x \in \mathbb{Z}$, tal que $\overline{a} + \overline{x} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$. Da igualdade $\overline{a} + \overline{x} = \overline{a}$ vem que $\overline{a+x} = \overline{a}$ e da definição da relação vem que $m|(a+x-a)$, ou ainda, $m|x$. Em outras palavras x é múltiplo de m, isto é, $x = km$ para qualquer $k \in \mathbb{Z}$. Mas os elementos da forma km são pertencentes à classe $\overline{0}$, e portanto $e = \overline{x} = \overline{0}$. Vamos agora mostrar que todo $\overline{a} \in \mathbb{Z}_m$ é simetrizável pela operação $+$. Dado $\overline{a} \in \mathbb{Z}_m$ procuramos um elemento $-(\overline{a}) = \overline{x} \in \mathbb{Z}_m$, chamado simétrico de $\overline{a}$, que satisfaz $\overline{a} + \overline{x} = \overline{0}$. Desta igualdade, segue que $\overline{a+x} = \overline{0}$ e da definição de relação $m|(a+x-0)$. Em outras palavras, $a+x$ é múltiplo de m, isto é $a+x = km$ para $k \in \mathbb{Z}$, donde segue que $x = -a+km$. Os números da forma $-a+km$ são pertencentes à classe $\overline{-a}$ ou ainda à classe $\overline{m-a}$, donde todo elemento $\overline{a} \in \mathbb{Z}_m$ e simetrizável sendo $-\overline{a} = \overline{-a} = \overline{m-a}$ o seu simétrico.

Isto posto, a adição torna o conjunto $\mathbb{Z}_m$ um grupo abeliano. Provaremos na sequência que a operação multiplicação é associativa, comutativa, distributiva em relação à adição e admite um elemento neutro.

Dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, temos que

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c}),$$

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a},$$

e também

$$\begin{aligned} \overline{a} \cdot (\overline{b} + \overline{c}) &= \overline{a} \cdot \overline{b+c} = \overline{a(b+c)} \\ &= \overline{ab+ac} = \overline{ab} + \overline{ac} = (\overline{a} \cdot \overline{b}) + (\overline{a} \cdot \overline{c}). \end{aligned}$$

Desejamos agora obter um elemento neutro $e = \overline{x}$ para $\cdot$, isto é, um elemento $\overline{x} \in \mathbb{Z}_m$ que satisfaça $\overline{a} \cdot \overline{x} = \overline{x} \cdot \overline{a} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$. Desta igualdade, temos que $\overline{ax} = \overline{a}$ e da definição da relação $m|(ax-a)$ ou $m|a(x-1)$. Mas como $\overline{a}$ é arbitrário em $\mathbb{Z}_m$, em geral

m não divide a, e então resta que $m|(x-1)$, ou ainda $x \approx 1$, o que é equivalente a $\overline{x} = \overline{1}$. Segue então que $\overline{1}$, é o elemento neutro para $\cdot$.

Do que provamos até agora, o conjunto $\mathbb{Z}_m$ é um anel comutativo com unidade. Nosso próximo passo é no sentido de melhorar a estrutura deste conjunto. Infelizmente isto nem sempre é possível. Desejaríamos agora mostrar que o conjunto $\mathbb{Z}_m$ é um anel de integridade ou mesmo um corpo. Isto dependerá do número m.

Pode-se verificar como exemplo que no conjunto $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ os elementos não nulos $\overline{2}$, $\overline{3}$ e $\overline{4}$ não possuem inverso multiplicativo.

Contudo, é possível mostrar que em $\mathbb{Z}_m$ todo elemento não nulo $\overline{a}$ é simetrizável pela operação produto, se e somente se, m e a forem primos entre si, isto é, $mdc(a, m) = 1$.

De fato, se m e a (podemos supor $1 \leq a \leq m-1$) são inteiros primos entre si, então existem números inteiros q e u tais que $au + qm = 1$. Segue que $au - 1 = (-q)m$ e então $m|(au-1)$. Segue que $au \approx 1$ ou equivalentemente $\overline{au} = \overline{1}$ ou ainda $\overline{a} \cdot \overline{u} = \overline{1}$, e portanto $\overline{a}$ e simetrizável para a operação multiplicação, sendo $\overline{u}$ este simétrico (inverso multiplicativo).

Reciprocamente se $\overline{a} \in \mathbb{Z}_m^*$ é simetrizável para a operação de multiplicação então existe $\overline{u} \in \mathbb{Z}_m^*$ tal que $\overline{a} \cdot \overline{u} = \overline{1}$. Isto significa que $\overline{au} = \overline{1}$ e também que $au \approx 1$. Da definição da relação segue que $au - 1 = qm$ ou ainda $au + (-q)m = 1$ para algum $q \in \mathbb{Z}$. Segue da proposição 2.4 que a e m são primos entre si.

Em particular, se m é um número primo, então todos os elementos não nulos de $\mathbb{Z}_m$ são simetrizáveis para a operação de multiplicação, o que torna o conjunto $\mathbb{Z}_m$ um corpo.