Números Inteiros (Notas de Aula)

Julio Cesar Moraes Pezzott

Departamento de Matemática, UEM,

E-mail: jcmpezzott2@uem.br

O texto que se encaminha é baseado nos livros citados abaixo e para uma melhor compreensão do assunto, recomendamos o estudo destes:

• H. H. Domingues. *Fundamentos de aritmética*. Florianópolis: Editora da UFSC, 2009.

• C. P. Milies e S. P. Coelho. *Números. Uma introdução à matemática*. 3^a ed. São Paulo: Edusp, 2003.

1 Fundamentação axiomática

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

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

Em $\mathbb{Z}$, estão definidas duas operações: a *adição* "+" e a *multiplicação* "$\cdot$". O primeiro grupo de axiomas colocados aqui destaca propriedades de tais operações:

(Ax.1) (Associatividade da adição): Para quaisquer números inteiros a, b, c, temos que $a + (b + c) = (a + b) + c$.

(Ax.2) (Elemento neutro da adição): Existe um único elemento em $\mathbb{Z}$, o qual é denotado por 0 e chamado de *zero* ou *elemento neutro da adição*, tal que $a + 0 = a$, para todo $a \in \mathbb{Z}$.

(Ax.3) (Existência do Oposto): Para cada $a \in \mathbb{Z}$, existe um único elemento em $\mathbb{Z}$, o qual é denotado por $-a$ e chamado de *oposto* de a, tal que $a + (-a) = 0$.

(Ax.4) (Comutatividade da adição): Para quaisquer números inteiros a e b, temos que $a + b = b + a$.

(Ax.5) (Associatividade da multiplicação): Para quaisquer números inteiros a, b, c, temos que $a(bc) = (ab)c$.

(Ax.6) (Elemento neutro da multiplicação): Existe um único elemento em $\mathbb{Z}$, o qual é diferente de 0 e denotado por 1, tal que $1 \cdot a = a$, para todo $a \in \mathbb{Z}$. Tal elemento é chamado de *elemento neutro da multiplicação*.

(Ax.7) (Lei do cancelamento para a multiplicação): Para quaisquer números inteiros a, b e c tais que $a \neq 0$, temos que: se $ab = ac$, então $b = c$.

(Ax.8) (Comutatividade da multiplicação): Para quaisquer números inteiros a e b, temos que $ab = ba$.

(Ax.9) (Distributividade) Para quaisquer números inteiros a, b e c, temos que $a(b + c) = ab + ac$.

Utilizando tais axiomas, podemos provar alguns fatos.

Proposição 1.1. (Lei do cancelamento para a adição): *Para quaisquer números inteiros a, b e c temos que: se $a + b = a + c$, então $b = c$*

Demonstração. Por hipótese, $a + b = a + c$. Somamos o oposto de a em ambos os lados dessa igualdade; desse modo, $(-a) + (a + b) = (-a) + (a + c)$. Usando o Axioma (Ax.1), obtemos $[(-a)+a]+b = [(-a)+a]+c$, ou seja, $0+b = 0+c$, o que nos permite concluir que $b = c$. □

Proposição 1.2. *Para todo $a \in \mathbb{Z}$, temos que $a \cdot 0 = 0$.*

Demonstração. Pelo Axioma (Ax.9), temos

$$a \cdot 0 + a \cdot 0 = a(0 + 0) = a \cdot 0 = a \cdot 0 + 0,$$

ou seja, $a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$. Segue da Proposição 1.1 que $a \cdot 0 = 0$. □

Proposição 1.3. *Se $a, b \in \mathbb{Z}$ são tais que $ab = 0$, então $a = 0$ ou $b = 0$.*

Demonstração. Como $ab = 0$, podemos escrever, por conta da Proposição 1.2, $ab = a0$. Se $a = 0$, temos o resultado. Se $a \neq 0$, então, como $ab = a0$, segue do Axioma (Ax.7) que $b = 0$. □

Proposição 1.4. (Regra dos Sinais): *Dados inteiros a e b, são verdadeiras as seguintes afirmações:*

(i) $-(-a) = a$

(ii) $(-a)b = -(ab) = a(-b)$

(iii) $(-a)(-b) = ab$

Em $\mathbb{Z}$, também supomos que seja conhecida a relação "*menor que ou igual*", denotada por "$\leq$". Os axiomas apresentados na sequência abordam tal relação.

(Ax.10) (Propriedade Reflexiva): Para qualquer número inteiro a, temos que $a \leq a$.

(Ax.11) (Propriedade Antissimétrica): Para quaisquer números inteiros a e b, temos que se $a \leq b$ e $b \leq a$, então $a = b$.

(Ax.12) (Propriedade Transitiva) Para quaisquer números inteiros a, b e c, temos que se $a \leq b$ e $b \leq c$, então $a \leq c$.

Quando $a \leq b$ e $a \neq b$, escreveremos $a < b$ e diremos que a *é menor que* b. Além disso, quando conveniente, escreveremos $b \geq a$ no lugar que $a \leq b$ e diremos que b *é maior que ou igual a* a. De modo análogo, podemos escrever $b > a$ no lugar de $a < b$ e dizer que b *é maior que* a.

(Ax.13) (Tricotomia) Para quaisquer números inteiros a e b, temos que ou $a < b$ ou $a = b$ ou $b < a$

Diante dos axiomas (Ax.10), (Ax.11), (Ax.12) e (Ax.13), vemos que a relação $\leq$ é uma *relação de ordem total*.

Aqui, vamos fixar as seguintes notações:

- $\mathbb{Z}_+ = \{x \in \mathbb{Z} : x > 0\}$ é o conjunto dos *números inteiros positivos*.
- $\mathbb{Z}_- = \{x \in \mathbb{Z} : x < 0\}$ é o conjunto dos *números inteiros negativos*.

Os próximos dois axiomas vinculam a relação de ordem $\leq$ com as operações de adição e multiplicação em $\mathbb{Z}$.

(Ax.14) Para quaisquer números inteiros a, b e c, temos que se $a \leq b$, então $a + c \leq b + c$.

(Ax.15) Para quaisquer números inteiros a, b e c, temos que se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.

Proposição 1.5. *Dado $a \in \mathbb{Z}$, vale que:*

(i) *se $a \leq 0$, então $-a \geq 0$;*

(ii) *se $a \geq 0$, então $-a \leq 0$;*

(iii) $a^2 \geq 0$;

(iv) $1 > 0$.

Demonstração. (i) Se $a \leq 0$, então segue do Axioma (Ax.14) que $a+(-a) \leq 0+(-a)$. Como $a+(-a) = 0$ e $0+(-a) = -a$, obtemos $0 \leq -a$.

(ii) Exercício!

(iii) Aqui, vamos dividir em dois casos:

Caso 1: $a \geq 0$. Se $a \geq 0$, segue do Axioma (Ax.15) que $a^2 = a \cdot a \geq a \cdot 0 = 0$.

Caso 2: $a \leq 0$. Se $a \leq 0$, então $-a \geq 0$ (pelo item (i) acima) e, assim, $(-a)(-a) = (-a)^2 \geq 0$ (pelo Caso 1). Usando a Regra dos Sinais (item (iii) da Proposição 1.4), obtemos $(-a)^2 = a^2$. Logo $a^2 \geq 0$.

(iv) Como $1 = 1 \cdot 1$ e $1 \cdot 1 > 0$ (pelo item (iii)), temos $1 > 0$. □

Como consequência, temos:

- $\mathbb{Z}_+ = \{x \in \mathbb{Z} : x > 0\} = \{1, 2, 3, 4, \ldots\}$
- $\mathbb{Z}_- = \{x \in \mathbb{Z} : x < 0\} = \{\ldots, -4, -3, -2, 1\}$

(Ax.16) (Princípio da Boa Ordem): Todo conjunto não-vazio de inteiros não-negativos possui um elemento mínimo. Ou seja, se A é um subconjunto de $\{0, 1, 2, 3, \ldots\}$, então existe $k \in A$ tal que $k \leq a$, para todo $a \in A$.

Demonstrações para os próximos resultados desta seção podem ser encontradas em [2].

Proposição 1.6. *Se $a, b \in \mathbb{Z}$ são tais que $a \leq b \leq a + 1$, então $a = b$ ou $b = a + 1$. Consequentemente, se $0 \leq a \leq 1$, então $a = 0$ ou $a = 1$.*

Proposição 1.7. (Propriedade Arquimediana): *Dados inteiros positivos a e b, existe um inteiro positivo n tal que $na > b$.*

Proposição 1.8. *Todo subconjunto não-vazio de $\mathbb{Z}$ limitado inferiormente possui elemento mínimo. Analogamente, Todo subconjunto não-vazio de $\mathbb{Z}$ limitado superiormente possui elemento máximo.*

Exercício 1.9. Sejam $a, b \in \mathbb{Z}$. Mostre que:

(a) $(-1)a = -a$.

(b) Se $a^2 = 0$, então $a = 0$.

(c) Se $a^2 = a$, então $a = 0$ ou $a = 1$.

(d) $a + x = b$ tem solução única em $\mathbb{Z}$.

(e) Se $a < b$, então $-a > -b$.

Antes de passarmos para a próxima seção, destacamos mais duas definições.

- Muitas vezes, escreveremos $a - b$ para indicar a soma $a + (-b)$. Essa é a conhecida operação de *subtração*.
- O *módulo* de um número inteiro a, denotado por $|a|$, é definido por $|a| = \begin{cases} a, & \text{se } a \geq 0; \\ -a, & \text{se } a < 0. \end{cases}$

Proposição 1.10. *Sejam a e b números inteiros. Temos que:*

(i) $|a| \geq 0$. *Além disso, $|a| = 0$ se, e somente se, $a = 0$.*

(ii) $|ab| = |a||b|$.

(iii) $|a + b| \leq |a| + |b|$.

2 Divisibilidade e o Algoritmo da Divisão

Definição 2.1. Sejam a e b números inteiros. Dizemos que b *divide* a (ou que a é *divisível* por b) se existe um número inteiro q tal que $a = bq$.

- Quando b divide a, escrevemos $b \mid a$. Se b não divide a, escrevemos $b \nmid a$.
- Se $b \mid a$, diremos também que a é *múltiplo* de b e que b é um *divisor* de a.
- Se $b \mid a$ e $b \neq 0$, então existe um único $q \in \mathbb{Z}$ tal que $a = bq$. De fato, se existisse outro $q' \in \mathbb{Z}$ tal que $a = bq'$, teríamos $bq = bq'$ e, usando a Lei do Cancelamento (Ax.7), obteríamos $q = q'$. Por conta dessa unicidade, o número q, neste caso, recebe o nome de *quociente* de a por b; algumas vezes, escreveremos $q = a/b = \frac{a}{b}$.
- Notemos que $0 \mid a$ se, e somente se, $a = 0$. Neste caso, o quociente não é único, uma vez que $0 = 0 \cdot q$, para todo $q \in \mathbb{Z}$. Por conta disso, assumiremos, a partir daqui, que todos os divisores considerados neste texto são diferentes de zero.

Proposição 2.2. *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração. Se $b \mid a$, então existe $q \in \mathbb{Z}$ tal que $a = bq$. Daí, $|a| = |bq| = |b||q|$. Como $a \neq 0$, temos $|a| > 0$ e, assim, $|q| > 0$, ou seja, $1 \leq |q|$. Multiplicando ambos os lados dessa última desigualdade por $|b|$, obtemos $|b| \leq |b||q| = |a|$. □

Corolário 2.3. *São verdadeiras as afirmações:*

(i) *Os únicos divisores de 1 são 1 e -1.*

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

Demonstração. (i) Se $b \mid 1$, então $b \neq 0$ e segue da Proposição 2.2 que $|b| \leq 1$. Logo, $0 < |b| \leq 1$ e, assim, pela Proposição 1.6, temos $|b| = 1$. Portanto, $b = \pm 1$.

(ii) Se $b \mid a$ e $a \mid b$, então existem $q, s \in \mathbb{Z}$ tais que $a = bq$ e $b = as$. Daí, $a = bq = (as)q = a(sq)$. Como $a \neq 0$, obtemos $1 = sq$, ou seja, q divide 1. Pelo item (i), temos $q = \pm 1$, o que nos fornece $a = \pm b$. □

Proposição 2.4. *Sejam a, b, c e d números inteiros. São verdadeiras as seguintes afirmações:*

(i) *$a \mid a$.*

(ii) *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

(iii) *Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.*

(iv) *Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$.*

(v) *Se $a \mid b$ então $a \mid bm$, para todo $m \in \mathbb{Z}$.*

(vi) *Se $a \mid b$ e $a \mid c$, então $a \mid (bm + cn)$, para quaisquer $m, n \in \mathbb{Z}$.*

Demonstração. (i) Basta observar que $a = 1 \cdot a$.

(ii) Se $a \mid b$ e $b \mid c$, então existem inteiros q e s tais que $b = aq$ e $c = bs$. Daí $c = bs = (aq)s = a(qs)$ e isso nos diz que $a \mid c$.

(iii) Se $a \mid b$ e $c \mid d$, então existem inteiros q e s tais que $b = aq$ e $d = cs$. Assim, $bd = (aq)(cs) = ac(qs)$; logo $ac \mid bd$.

(iv) Se $a \mid b$ e $a \mid c$, então existem $q, s \in \mathbb{Z}$ tais que $b = aq$ e $c = as$. Disso resulta que $b + c = aq + as = a(q + s)$ e isso prova que $a \mid (b + c)$.

(v) Se $a \mid b$, então $b = aq$, para algum $q \in \mathbb{Z}$. Assim, para qualquer $m \in Z$, obtemos $bm = aqm = a(qm)$, isto é, $a \mid bm$.

(vi) Exercício! □

Exercício 2.5. Suponha que o inteiro b divide os inteiros $a_1, a_2, \ldots, a_n$. Mostre que, para quaisquer inteiros $m_1, m_2, \ldots, m_n$, b divide a soma $a_1m_1 + a_2m_2 + \ldots + a_nm_n$.

Nosso objetivo agora é provar o Algoritmo da Divisão. Para isso, precisaremos do seguinte lema.

Lema 2.6. *Sejam a e b números inteiros tais que $a \geq 0$ e $b > 0$. Então existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$, com $0 \leq r < b$.*

Demonstração. Consideremos o seguinte conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Se $x = 0$, então $a - bx = a \geq 0$. Assim, $a \in S$, ou seja, $S \neq \emptyset$. Como S é formado apenas por inteiros não-negativos, segue do Princípio da Boa Ordem (Ax.16) que existe $r = \min S$. Já que $r \in S$, temos que r é da forma $r = a - bq \geq 0$, para algum $q \in \mathbb{Z}$.

Afirmamos que $r < b$. De fato, se ocorresse $r \geq b$, teríamos $a - b(q + 1) = a - bq - b = r - b \geq 0$ e daí $a - b(q + 1) \in S$. Neste caso, temos a contradição $a - b(q + 1) = r - b < r = \min S$. Portanto, $r < b$. □

Teorema 2.7. (Algoritmo da Divisão) *Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$. Então existem inteiros q e r tais que $a = bq + r$ $0 \leq r < |b|$. Mais: q e r são únicos com tais propriedades.*

Demonstração. Primeiramente, vamos provar que q e r podem ser determinados no caso em que $b > 0$ e a é um inteiro qualquer. O caso $a \geq 0$ foi resolvido no lema anterior. Por isso, podemos supor $a < 0$. Daí $|a| > 0$ e, pelo lema acima,

existem $q', r' \in \mathbb{Z}$ tais que $|a| = bq'+r'$, com $0 \leq r' < |b| = b$. Se $r' = 0$, então $-|a| = a = -(bq') = b(-q')+0 = b(-q')+r'$ e, assim, fazendo $q = -q'$ e $r = r'$, temos o desejado. Se $r' > 0$, temos que

$$a = -|a| = -(bq'+r') = b(-q')-r' = b(-q')-b+b-r' = \\ = b(-q'-1)+(b-r').$$

De $0 < r' < b$ vem que $0 < b - r' < b$. Aqui, $q = -q' - 1$ e $r = b - r'$ verificam as condições exigidas no enunciado do teorema.

Analisemos agora o caso $b < 0$. Para todo $a \in \mathbb{Z}$, segue do que vimos acima que existem inteiros q' e r' tais que $a = |b|q' + r'$, com $0 \leq r' < |b|$. Como $b < 0$, temos $|b| = -b$ e daí $a = |b|q' + r' = (-b)q' + r' = b(-q') + r'$. Fazendo $q = -q'$ e $r = r'$, obtemos o desejado.

Unicidade: Suponha que existam $q, q', r, r' \in \mathbb{Z}$ tais que $a = bq + r$ e $a = bq' + r'$, com $0 \leq r < |b|$ e $0 \leq r' < |b|$. Daí $bq + r = bq' + r'$. Sem perda de generalidade, vamos supor $r' \geq r$. Daí, $(q - q')b = r' - r \geq 0$. Como $|b| > r'$, temos $r' - r < |b|$ e disso resulta que $(q - q')b = r' - r < |b|$; logo, $0 \leq |q - q'||b| < |b|$. Sendo $|b| > 0$, obtemos $0 \leq |q - q'| < 1$, o que nos fornece $|q - q'| = 0$, ou seja, $q = q'$. Da igualdade $bq+r = bq'+r'$ vem que $r = r'$ e provamos assim a unicidade.

□

Definição 2.8. Os inteiros q e r determinados no teorema acima são chamados, respectivamente, de *quociente* e *resto* da divisão de a por b.

Exercício 2.9. Determinar o quociente q e o resto r da divisão de a por b nos seguintes casos:

(i) $a = 138$, $b = 7$

(ii) $a = -138$ e $b = 7$

(iii) $a = 138$ e $b = -7$

Solução: (i) Aqui,

$$\begin{array}{r|l} 1\,3\,8 & 7 \\ \cline{2-2} \underline{-7} & 1\,9 \\ 6\,8 & \\ \underline{-6\,3} & \\ 5 & \end{array}$$

Logo, $138 = 7 \cdot 19 + 5$; daí $q = 19$ e $r = 5$.

(ii) Pelo item (i), $138 = 7 \cdot 19 + 5$ e, assim,

$$-138 = -(7 \cdot 19 + 5) = -(7 \cdot 19) - 5 = 7(-19) - 5 = \\ = 7 \cdot (-19) - 7 + 7 - 5 = 7(-19) + 7(-1) + 2 = \\ = 7(-20) + 2.$$

Daí $q = -20$ e $r = 2$.

(iii) $138 = 7 \cdot 19 + 5 = (-7)(-19) + 5$; logo $q = -19$ e $r = 5$.

Definição 2.10. Um número inteiro divisível por 2 é dito *par*. Quando um número inteiro não for divisível por 2, este será chamado *ímpar*.

Observação 2.11. Dado um número inteiro a, segue do Algoritmo da Divisão que existem inteiros q e r tais que $a = 2q + r$, com $0 \leq r < 2$. Logo $r \in \{0, 1\}$. Se $r = 0$, então a é par. Se $r = 1$, então a é um número ímpar. Ou seja, todo número ímpar é da forma $2q + 1$, para algum inteiro q.

Exercício 2.12. Mostre que todo inteiro ímpar é da forma $4k + 1$ ou $4k + 3$.

Solução: Dado um número inteiro a, segue do Algoritmo da Divisão que existem inteiros q e r tais que $a = 4q + r$, com $0 \leq r < 4$. Analisemos os possíveis valores de r:

- se $r = 0$, então $a = 4q = 2(2q)$ é par;

- se $r = 1$, então $a = 4q + 1 = 2(2q) + 1$ é ímpar;

- se $r = 2$, então $a = 4q + 2 = 2(2q + 1)$ é par;

- se $r = 3$, temos $a = 4q + 3 = 2(2q + 1) + 1$ é ímpar.

Portanto, a é ímpar se, e somente se, $r \in \{1, 3\}$. Em tais casos, vemos que a é da forma $a = 4k + 1$ ou $4k + 3$.

Exercício 2.13. Mostre que o quadrado de um número inteiro é da forma $3k$ ou $3k + 1$.

Exercício 2.14. Sabe-se que o resto da divisão do inteiro a por 8 é 3. Determine o resto da divisão de $a^2 + 1$ por 4.

Solução: Temos que $a = 8q+3$, para algum $q \in \mathbb{Z}$. Assim,

$$a^2 + 1 = (8q + 3)^2 + 1 = (16q^2 + 48q + 9) + 1 = \\ = 4(4q^2) + 4(12q) + 4 \cdot 2 + 2 = 4(4q^2 + 12q + 2) + 2.$$

O resto é 2.

Exercício 2.15. Sabe-se que o resto da divisão do inteiro a por 6 é 4. Determine o resto da divisão de $a^2 + 1$ por 6.

Exercício 2.16. Prove que:

(i) Dado $a \in \mathbb{Z}$, um dos inteiros a, $a+2$ ou $a+4$ é múltiplo de 3.

(ii) Se a é ímpar, então $24 \mid a(a^2 - 1)$.

(iii) Se 2 não divide a, então 8 divide $a^2 - 1$.

Exercício 2.17. Determine números inteiros a e b tais que $a - b = 184$, e o quociente e o resto da divisão de a por b sejam, respectivamente, $q = 16$ e $r = 4$.

3 Representação dos números em outras bases

Teorema 3.1. *Seja b um inteiro, $b \geq 2$. Todo inteiro positivo a pode ser escrito de modo único na forma*

$$a = r_n b^n + r_{n-1} b^{n-1} + \ldots + r_1 b + r_0,$$

em que $n \geq 0$, $r_n \neq 0$ e, para todo índice $i \in \{0, 1, \ldots, n\}$, tem-se $0 \leq r_i < b$

Demonstração. Existência: Dividindo a por b, obtemos $q_0, r_0 \in \mathbb{Z}$ tais que $a = bq_0 + r_0$, com $0 \leq r_0 < b$. Na sequência, dividimos q_0 por b e obtemos inteiros q_1 e r_1 tais que $q_0 = bq_1 + r_1$, com $0 \leq r_1 < b$. Repetimos o processo até obtermos um quociente nulo. Isso deve ocorrer em algum passo, pois cada quociente obtido é maior ou igual a zero e menor que o quociente obtido anteriormente.

Suponha que o primeiro quociente nulo seja o n-ésimo termo. Assim, temos:

$a = bq_0 + r_0, \ \ 0 \leq r_0 < b$

$q_0 = bq_1 + r_1, \ \ 0 \leq r_1 < b$

$q_1 = bq_2 + r_2, \ \ 0 \leq r_2 < b$

$\vdots$

$q_{n-2} = bq_{n-1} + r_{n-1}, \ \ 0 \leq r_{n-1} < b$

$q_{n-1} = b \cdot 0 + r_n, \ \ 0 < r_{n-1} < b$

Logo

$$\begin{aligned} a &= bq_0 + r_0 = b(bq_1 + r_1) + r_0 = \\ &= b^2 q_1 + br_1 + r_0 = b^2(bq_2 + r_2) + br_1 + r_0 = \\ &= b^3 q_2 + b^2 r_2 + br_1 + r_0 = \ldots = \\ &= b^n r_n + b^{n-1} r_{n-1} + b^{n-2} r_{n-2} + \ldots + b^2 r_2 + br_1 + r_0. \end{aligned}$$

Unicidade: Será omitida. □

O número b dado no teorema acima é chamado de *base* e vamos escrever $(r_n r_{n-1} r_{n-2} \ldots r_0)_b$ para indicar como que o número a é representado na base b.

Estamos acostumados a expressar números na base 10. Por exemplo, o símbolo 5672 representa o número inteiro $5 \cdot 10^3 + 6 \cdot 10^2 + 7 \cdot 10 + 2$. Quando não explicitarmos a base b na expressão de a, assumimos que a base considerada é a base 10.

Exercício 3.2. Escreva 1329 na base 5.

Solução:

1329 | 5	265 | 5	53 | 5	10 | 5	2 | 5
$*$ 265	$*$ 53	$*$ 10	$*$ 2	$*$ 0
4	0	3	0	2

Portanto, $1329 = (20304)_5$.

Exercício 3.3. Escreva 127 na base 4.

Solução:

127 | 4	31 | 4	7 | 4	1 | 4
$*$ 31	$*$ 7	$*$ 1	$*$ 0
3	3	3	1

Logo, $127 = (1333)_4$.

Exercício 3.4. Escreva 855 na base 12.

Solução: Aqui, precisamos de mais dois algarismos para representarmos os inteiros 10 e 11. Façamos $\alpha = 10$ e $\beta = 11$

855 | 12	71 | 12	5 | 12
$*$ 71	$*$ 5	$*$ 0
3	11	5

Logo, $855 = (5\beta 3)_{12} = (5(11)3)_{12}$.

Observação 3.5. Note que

$$(5113)_{12} = 5 \cdot 12^3 + 1 \cdot 12^2 + 1 \cdot 12 + 3 = 1887 \neq 855,$$

ou seja, $855 \neq (5113)_{12}$. Agora,

$$(5(11)3)_{12} = 5 \cdot 12^2 + 11 \cdot 12 + 3 = 855.$$

Exercício 3.6. Escreva $(1245)_6$ na base 10.

Solução: $(1245)_6 = 1 \cdot 6^3 + 2 \cdot 6^2 + 4 \cdot 6 + 5 = 317$.

Exercício 3.7. Escreva o número a na base b:

(i) $a = 1472, \ b = 5$.

(ii) $a = 114, \ b = 2$.

(iii) $a = 15422, \ b = 12$.

(iv) $a = (2356)_7, \ b = 10$.

(v) $a = (532)_6, \ \ b = 8$.

(vi) $a = (21)_3, \ b = 12$.

4 Máximo divisor comum

Sejam a e b inteiros não ambos iguais a zero. Dizemos que um inteiro c é um *divisor comum* de a e b se $c \mid a$ e $c \mid b$.

Fixemos as seguintes notações:

$D(a) = \{d \in \mathbb{Z} \, : \, d \mid a\}$

$D(b) = \{d \in \mathbb{Z} \, : \, d \mid b\}$

$D(a, b) = \{d \in \mathbb{Z} \, : \, d \mid a \text{ e } d \mid b\}$

Vemos que $D(a, b) = D(a) \cap D(b)$. Além disso, $D(a, b)$ é limitado superiormente, pois se $a \neq 0$, então $c \leq |a|$, para todo $c \in D(a, b)$. Logo, o conjunto $D(a, b)$ possui elemento máximo. Disso segue a seguinte definição:

Definição 4.1. Sejam a e b inteiros não ambos iguais a zero. O *máximo divisor comum* (MDC) de a e b é o número denotado por $\text{mdc}(a, b)$ e definido como sendo o máximo do conjunto $D(a, b)$ dos divisores comuns de a e b.

Exemplo 4.2. Vemos que:

$D(6) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$

$D(9) = \{-9, -3, -1, 1, 3, 9\}$

$D(10) = \{-10, -5, -2, -1, 1, 2, 5, 10\}$.

Assim,

$D(6, 9) = D(6) \cap D(9) = \{-3, -1, 1, 3\}$

$D(6, 10) = D(6) \cap D(10) = \{-2, -1, 1, 2\}$

$D(9, 10) = D(9) \cap D(10) = \{-1, 1\}$

Portanto, $\text{mdc}(6, 9) = 3$, $\text{mdc}(6, 10) = 2$ e $\text{mdc}(9, 10) = 1$.

Teorema 4.3. (Teorema de Bézout) *Sejam $a, b \in \mathbb{Z}$ ambos diferentes de zero e seja $d = \text{mdc}(a, b)$. Então existem inteiros x e y tais que $d = ax + by$.*

Demonstração. Temos que $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$ (prove isso!). Assim, sem perda de generalidade, podemos supor $a > 0$ e $b > 0$. Consideremos o seguinte conjunto:

$$S = \{au + bv : u, v \in \mathbb{Z} \text{ e } au + bv > 0\}$$

Se $u = v = 1$, temos $au + bv = a + b > 0$, ou seja, $a + b \in S$ e disso vem que $S \neq \emptyset$. Como S é formado por inteiros positivos, segue do Princípio da Boa Ordem que S possui elemento mínimo, digamos $d = \min S$. Como $d \in S$, existem inteiros x e y tais que $d = ax + by$.

Vamos mostrar que $d = \text{mdc}(a, b)$. De fato, notemos que $a \in S$, porque $a = 1 \cdot a + 0 \cdot b$. Logo, $d \leq a$. Pelo Algoritmo da Divisão, existem inteiros q e r tais que $a = dq + r$, com $0 \leq r < d$. Mostremos que $r = 0$. Com efeito, se ocorresse $r > 0$, teríamos

$$r = a - dq = a - q(ax + by) = a - qax - bqy =$$
$$= a(1 - qx) + b(-qy) > 0,$$

o que implicaria $r \in S$, com $r < d$, contradizendo o fato que d é o mínimo de S. Logo $r = 0$ e disso vem que $a = dq$, ou seja, $d \mid a$. Analogamente, prova-se que $d \mid b$ e, assim, temos que $d \in D(a, b)$. Por fim, se $d' \mid a$ e $d' \mid b$, então $d' \mid (ax + by)$ e, assim, $|d'| \leq |d| = d$. Isso prova que d é o elemento máximo de $D(a, b)$, ou seja, $d = \text{mdc}(a, b)$.

□

Teorema 4.4. *Sejam $a, b \in \mathbb{Z}$ e $d \in \mathbb{Z}_+$. Temos que $\text{mdc}(a, b) = d$ se, e somente se, as duas seguintes condições são satisfeitas:*

(i) *$d \mid a$ e $d \mid b$;*

(ii) *se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.*

Demonstração. Seja $d = \text{mdc}(a, b)$. Então é claro que a condição (i) se verifica e, na prova do Teorema de Bézout, vimos que a condição (ii) é satisfeita. Reciprocamente, se d satisfaz a condição (i), então $d \in D(a, b)$. Pela condição (ii), se $d' \in D(a, b)$, então $d' \mid d$ e disso segue que $d' \leq d$, o que prova $d = \max D(a, b)$, isto é, $d = \text{mdc}(a, b)$. □

Proposição 4.5. *Seja d um divisor positivo comum de a e b. Temos que $d = mdc(a, b)$ se, e somente se, $mdc(a/d, b/d) = 1$.*

Demonstração. Suponha $d = \text{mdc}(a, b)$. Existem inteiros a_1 e b_1 tais que $a = da_1$ e $b = db_1$. Afirmamos que $\text{mdc}(a_1, b_1) = 1$. De fato, se $d_1 = \text{mdc}(a_1, b_1)$, segue do Teorema de Bézout que existem inteiros x e y tais que $d_1 = a_1x + b_1y$ e, daí, $dd_1 = ax + by$. Como $d_1 \mid a_1$, temos que $dd_1 \mid da_1$, isto é, $dd_1 \mid a$. Do mesmo modo, concluímos que $dd_1 \mid b$. Agora, se $d' \in \mathbb{Z}$ é tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$ (pelo Teorema 4.4) e, consequentemente, $d' \mid dd_1$. Segue do Teorema 4.4 que $\text{mdc}(a, b) = dd_1$, o que nos fornece $d_1 = 1$.

Suponhamos agora que $\text{mdc}(a/d, b/d) = 1$. Escrevendo $a_1 = a/d$ e $b_1 = b/d$, segue do Teorema de Bézout que existem inteiros x e y tais que $1 = a_1x + b_1y$, o que implica $d = ax + by$. Se $d' \mid a$ e $d' \mid b$, então $d' \mid (ax + by)$, ou seja, $d' \mid d$. Pelo Teorema 4.4, $d = \text{mdc}(a, b)$. □

Teorema 4.6. (Teorema de Euclides) *Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid bc$. Se $\text{mdc}(a, b) = 1$, então $a \mid c$.*

Demonstração. Se $\text{mdc}(a, b) = 1$, então segue do Teorema de Bézout que existem inteiros x e y tais que $1 = ax + by$. Logo, $c = c(ax + by) = a(cx) + (bc)y$. Como $a \mid a$ e $a \mid bc$, temos que $a \mid a(cx)$ e $a \mid b(cy)$ e disso segue que a divide a soma $acx + bcy$, isto é, $a \mid c$. □

Definição 4.7. Dizemos que os inteiros a e b são *primos entre si* (ou *relativamente primos*) se $\text{mdc}(a, b) = 1$.

Proposição 4.8. *Sejam a e b inteiros primos entre si. Se $c \in \mathbb{Z}$ é tal que $a \mid c$ e $b \mid c$, então $ab \mid c$.*

Demonstração. Se $a \mid c$, então $c = aq$, para algum $q \in \mathbb{Z}$. Logo, $b \mid aq$ (visto que $b \mid c$). Como $\text{mdc}(a, b) = 1$, segue do Teorema de Euclides que $b \mid q$, isto é, $q = bs$, para algum $s \in \mathbb{Z}$. Desse modo, $c = aq = abs$, o que prova que $ab \mid c$.

□

Exercício 4.9. Sejam $a, b, c \in \mathbb{Z}$. Prove que:

(i) Se $a|b$ e $\text{mdc}(b, c) = 1$, então $\text{mdc}(a, c) = 1$.

(ii) $\text{mdc}(a, c) = \text{mdc}(b, c) = 1$ se, e somente se, $\text{mdc}(ab, c) = 1$.

Exercício 4.10. Sejam $a, b, d \in \mathbb{Z}$, com $d > 0$. Verifique se as afirmações abaixo são verdadeiras ou falsas, justificando sua resposta.

(i) Se existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$, então $d = \text{mdc}(a, b)$.

(ii) Se existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$, então $\text{mdc}(a, b) = 1$.

Exercício 4.11. Sejam $a, b, c, d \in \mathbb{Z}$, com $d = \text{mdc}(a, b)$. Mostre que:

(i) Os inteiros x e y tais que $d = ax + by$ não são univocamente determinados.

(ii) Existem inteiros x e y tais que $c = ax + by$ se, e somente se, $d|c$.

Nosso intuito agora é apresentar um método que nos diz como calcular o mdc entre dois números inteiros. Para isso, precisamos dos seguintes resultados.

Lema 4.12. *Se $b \mid a$, então* $\text{mdc}(a, b) = |b|$.

Lema 4.13. *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, e considere inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$. Nestas condições, temos que $D(a, b) = D(b, r)$ e, consequentemente,* $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Demonstração. Por hipótese, $a = bq + r$, com $0 \leq r < |b|$. Se $x \in D(a, b)$, então $x \mid a$ e $x \mid b$. Como $r = a - bq$, temos que $x \mid r$ e, assim, $x \in D(r, b)$. Isso prova que $D(a, b) \subset D(b, r)$.

Por outro lado, se $x \in D(b, r)$, então $x \mid b$ e $x \mid r$ e disso resulta que $x \mid (bq + r)$, isto é $x \mid a$. Logo $x \in D(a, b)$ e isso prova a inclusão $D(b, r) \subset D(a, b)$. Logo $D(a, b) = D(b, r)$ e, portanto, $\text{mdc}(a, b) = \text{mdc}(b, r)$. □

• Método das Divisões Sucessivas (Algoritmo de Euclides)

Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q_1 e r_1 tais que

$$a = bq_1 + r_1, \text{ com } 0 \leq r_1 < |b|.$$

Se ocorrer $r_1 = 0$, então $b \mid a$ e daí $\text{mdc}(a, b) = b$ (pelo Lema 4.12). Se $r_1 \neq 0$, então existem $q_2, r_2 \in \mathbb{Z}$ tais que

$$b = r_1 q_2 + r_2, \text{ com } 0 \leq r_2 < r_1.$$

Se $r_2 = 0$, então $r_1 \mid b$ e daí $\text{mdc}(b, r_1) = r_1$. Pelo Lema 4.13, concluímos que $\text{mdc}(b, r_1) = \text{mdc}(a, b) = r_1$. Se $r_2 \neq 0$, então existem $q_3, r_3 \in \mathbb{Z}$ tais que

$$r_1 = r_2 q_2 + r_3, \text{ com } 0 \leq r_3 < r_2.$$

Se $r_3 = 0$, então $r_2 \mid r_1$ e disso resulta que $\text{mdc}(r_1, r_2) = r_2$ e, logo, $r_2 = \text{mdc}(r_2, r_1) = \text{mdc}(b, r_2) = \text{mdc}(a, b)$. Se $r_3 \neq 0$, repetimos o processo, ou seja, efetuamos a divisão de r_2 por r_3. Chegaremos em uma sequência $b \geq r_1 \geq r_2 \geq \ldots \geq 0$. Para algum índice n, teremos $r_{n+1} = 0$. De fato, se todos os elementos do conjunto $\{b, r_1, r_2, \ldots\}$ fossem diferentes de zero, tal conjunto seria um subconjunto não-vazio de inteiros positivos sem elemento mínimo, o que contradiz o Princípio da Boa Ordem. Logo, existe n tal que

$$r_{n-2} = r_{n-1} q_n + r_n, \text{ com } r_{n-1} = r_n q_{n+1}.$$

Usando os Lemas 4.12 e 4.13, concluímos que $r_n = \text{mdc}(r_{n-1}, r_{n-2}) = \text{mdc}(r_{n-2}, r_{n-3}) = \ldots = \text{mdc}(b, r_1) = \text{mdc}(a, b)$.

Para o caso em que $a < 0$ ou $b < 0$, basta observar que $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$.

Exemplo 4.14. Vamos determinar o mdc entre 1128 e 336. Efetuando divisões sucessivas, temos:

$$\begin{array}{r|l} 1128 & 336 \\ \hline -1008 & 3 \\ \hline 120 & \end{array} \qquad \begin{array}{r|l} 336 & 120 \\ \hline -240 & 2 \\ \hline 96 & \end{array} \qquad \begin{array}{r|l} 120 & 96 \\ \hline -96 & 1 \\ \hline 24 & \end{array} \qquad \begin{array}{r|l} 96 & 24 \\ \hline -96 & 4 \\ \hline 0 & \end{array}$$

Logo $\text{mdc}(1128, 336) = \text{mdc}(336, 120) = \text{mdc}(120, 96) = \text{mdc}(24, 96) = 24$.

Pelo Teorema de Bézout, existem inteiros x_0 e y_0 tais que $\text{mdc}(1128, 336) = 1128x_0 + 336y_0$. Queremos agora encontrar x_0 e y_0. Para isso, observamos que

$$1128 = 3 \cdot 336 + 120$$
$$336 = 2 \cdot 120 + 96$$
$$120 = 1 \cdot 96 + 24$$
$$96 = 4 \cdot 24$$

Logo,

$$24 = 120 - 1 \cdot 96 = 120 - (336 - 2 \cdot 120) = 3 \cdot 120 - 1 \cdot 336 =$$
$$= 3(1128 - 3 \cdot 336) - 1 \cdot 336 = 3 \cdot 1128 + (-10) \cdot 336.$$

Portanto, $x_0 = 3$ e $y_0 = -10$.

Exemplo 4.15. Queremos agora determinar o mdc entre 1540 e 396. Para isso, efetuamos as seguintes divisões sucessivas:

$$\begin{array}{r|l} 1540 & 396 \\ \hline -1188 & 3 \\ \hline 352 & \end{array} \qquad \begin{array}{r|l} 396 & 352 \\ \hline -352 & 1 \\ \hline 44 & \end{array} \qquad \begin{array}{r|l} 352 & 44 \\ \hline -352 & 8 \\ \hline 0 & \end{array}$$

Daí $\text{mdc}(1540, 396) = \text{mdc}(396, 352) = \text{mdc}(352, 44) = 44$.

Pelo Teorema de Bézout, existem inteiros x_0 e y_0 tais que $\text{mdc}(1540, 396) = 1540x_0 + 396y_0$. Para encontrarmos x_0 e y_0, destacamos que:

$$1540 = 3 \cdot 396 + 352 \quad \text{e} \quad 396 = 1 \cdot 352 + 44$$

Logo, $44 = 396 - 1 \cdot 352 = 396 - (1540 - 3 \cdot 396) =$
$= (-1) \cdot 1540 + 4 \cdot 396$. Portanto, $x_0 = -1$ e $y_0 = 4$.

Exercício 4.16. Use o Algoritmo de Euclides para obter inteiros x e y tais que:

(a) $\text{mdc}(56, 72) = 56x + 72y$.

(b) $\text{mdc}(24, 138) = 24x + 138y$.

(c) $\text{mdc}(119, 272) = 119x + 272y$.

(d) $\text{mdc}(18, 42) = 18x + 42y$.

5 Mínimo múltiplo comum

Sejam a e b inteiros diferentes de zero e denote por $M^+(a, b)$ o conjunto formado por todos os inteiros positivos que são múltiplos de a e b simultaneamente. Visto que $|a||b| \in M^+(a, b)$, temos $M^+(a, b) \neq \emptyset$ e, assim, pelo Princípio da Boa Ordem, tal conjunto possui elemento mínimo.

Definição 5.1. Sejam a e b inteiros diferentes de zero. O *mínimo múltiplo comum* (mmc) de a e b é o elemento mínimo do conjunto $M^+(a, b)$.

Proposição 5.2. *Sejam a e b inteiros diferentes de zero e seja $m \in \mathbb{Z}_+$. Temos que $m = \text{mmc}(a, b)$ se, e somente se, são satisfeitas as seguintes duas condições:*

(i) *$a \mid m$ e $b \mid m$;*

(ii) *se $a \mid m'$ e $b \mid m'$, então $m \mid m'$.*

Proposição 5.3. *Sejam a e b inteiros diferentes de zero. Se $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$, então $md = |ab|$.*

Demonstração. Aqui, faremos a prova apenas para o caso em que $a > 0$ e $b > 0$ (os demais casos são análogos).

Como $d \mid a$ e $d \mid b$, temos que $d \mid ab$ e iremos escrever $x = \frac{ab}{d}$. Vamos mostrar que $x = m$. Para isso, devemos provar que x satisfaz as duas condições dadas na Proposição 5.2. Escrevamos $a = da_1$ e $b = db_1$. Pela Proposição 4.5, temos que $\text{mdc}(a_1, b_1) = 1$. Agora, note que $x = a_1 b$ (uma vez que $x = \frac{ab}{d}$ e $a_1 = \frac{a}{d}$) e também $x = ab_1$. Isso prova que $a \mid x$ e $b \mid x$. A condição (i) da Proposição 5.2 está verificada.

Tomemos $m' \in \mathbb{Z}$ tal que m' é múltiplo de a e de b. Então, como $a \mid m'$, existe $q \in \mathbb{Z}$ tal que $m' = aq = da_1 q = a_1(dq)$. Ainda, note que $b \mid m'$, o que significa $db_1 \mid a_1(dq)$ e, assim, existe $s \in \mathbb{Z}$ tal que $a_1(dq) = b_1(ds)$, o que nos fornece $a_1 q = b_1 s$, isto é, $b_1 \mid a_1 q$. Uma vez que $\text{mdc}(a_1, b_1) = 1$, segue do Teorema de Euclides que $b_1 \mid q$ e, daí, $q = b_1 q_1$, para algum $q_1 \in \mathbb{Z}$. Como $xd = ab = da_1 db_1$, temos que $x = a_1 db_1$ e, assim, $m' = a_1(dq) = a_1 db_1 q_1 = xq_1$. Isso prova que $x \mid m'$, ou seja, x satisfaz a condição dada no item (ii) da Proposição 5.2. Portanto, $x = m$. □

Obtemos assim uma fórmula para o cálculo do mmc entre dois números inteiros não-nulos:

$$\text{mmc}(a, b) = \frac{|ab|}{\text{mdc}(a, b)}$$

Exemplo 5.4. Sabemos, pelo Exemplo 4.14, que $\text{mdc}(1128, 336) = 24$. Agora, $1128 \cdot 336 = 379008$ e $379008 = 24 \cdot 15792$. Portanto, $\text{mmc}(1128, 336) = 15792$.

Exemplo 5.5. Pelo Exemplo 4.15, $\text{mdc}(1540, 396) = 44$. Uma vez que $1540 \cdot 396 = 609840$ e $609840 = 44 \cdot 13860$, segue do teorema anterior que $\text{mmc}(1540, 396) = 13860$.

Exercício 5.6. Calcule:

(a) $\text{mmc}(56, 72)$ (b) $\text{mmc}(24, 138)$

(c) $\text{mmc}(119, 272)$ (d) $\text{mmc}(18, 42)$

Exercício 5.7. Determine inteiros positivos a e b tais que $ab = 9900$ e $\text{mdc}(a, b) = 330$.

Exercício 5.8. Sejam a e b inteiros não-nulos. Mostre que: $\text{mdc}(a, b) = \text{mmc}(a, b)$ se, e somente se, $|a| = |b|$.

6 Números primos e o Teorema Fundamental da Aritmética

Iniciamos com a definição de número primo.

Definição 6.1. Um número inteiro p é dito *primo* se p possui exatamente dois divisores positivos: 1 e $|p|$.

Observação 6.2. De acordo com a definição acima, -1, 0 e 1 não são números primos, uma vez que o único divisor positivo de -1 e 1 é o número 1 e, como sabemos, 0 possui uma infinidade de divisores positivos.

Exemplo 6.3. Eis alguns números primos positivos: 2, 3, 5, 7, 11, 13, 17, 19, 23.

Exemplo 6.4. O número 4 não é primo, pois 1, 2 e 4 dividem 4.

Exercício 6.5. Liste todos os números primos positivos menores que 100.

Definição 6.6. Um inteiro diferentes de -1, 0 e 1 que não é um número primo é chamado de *composto*.

Definição 6.7. Se b é um divisor de a tal que $1 < |b| < |a|$, diremos que b é um *divisor próprio* de a.