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* "·". 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 $1 > 0$. $\square$

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 $q = a/b = \dfrac{a}{b}$.
- 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.

$\square$

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,

$$\begin{array}{r|l} 138 & 7 \\ \cline{2-2} \underline{-7} & 19 \\ 68 & \\ \underline{-63} & \\ 5 & \end{array}$$

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:

$$\begin{aligned}
a &= bq_0 + r_0, \ \ 0 \leq r_0 < b \\
q_0 &= bq_1 + r_1, \ \ 0 \leq r_1 < b \\
q_1 &= bq_2 + r_2, \ \ 0 \leq r_2 < b \\
&\ \vdots \\
q_{n-2} &= bq_{n-1} + r_{n-1}, \ \ 0 \leq r_{n-1} < b \\
q_{n-1} &= b \cdot 0 + r_n, \ \ 0 < r_{n-1} < b
\end{aligned}$$

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:

$$\begin{array}{r|l} 1329 & 5 \\ \cline{2-2} * & 265 \\ 4 & \end{array} \qquad \begin{array}{r|l} 265 & 5 \\ \cline{2-2} * & 53 \\ 0 & \end{array} \qquad \begin{array}{r|l} 53 & 5 \\ \cline{2-2} * & 10 \\ 3 & \end{array} \qquad \begin{array}{r|l} 10 & 5 \\ \cline{2-2} * & 2 \\ 0 & \end{array} \qquad \begin{array}{r|l} 2 & 5 \\ \cline{2-2} * & 0 \\ 2 & \end{array}$$

Portanto, $1329 = (20304)_5$.

Exercício 3.3. Escreva 127 na base 4.

Solução:

$$\begin{array}{r|l} 127 & 4 \\ \cline{2-2} * & 31 \\ 3 & \end{array} \qquad \begin{array}{r|l} 31 & 4 \\ \cline{2-2} * & 7 \\ 3 & \end{array} \qquad \begin{array}{r|l} 7 & 4 \\ \cline{2-2} * & 1 \\ 3 & \end{array} \qquad \begin{array}{r|l} 1 & 4 \\ \cline{2-2} * & 0 \\ 1 & \end{array}$$

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 $\beta = 11$

$$\begin{array}{r|l} 855 & 12 \\ \cline{2-2} * & 71 \\ 3 & \end{array} \qquad \begin{array}{r|l} 71 & 12 \\ \cline{2-2} * & 5 \\ 11 & \end{array} \qquad \begin{array}{r|l} 5 & 12 \\ \cline{2-2} * & 0 \\ 5 & \end{array}$$

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:

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

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

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

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: