Material Teórico - Módulo Números Naturais: Contagem, Divisibilidade e o Teorema da Divisão Euclidiana

Divisibilidade e Teorema da Divisão Euclidiana Parte 1

Oitavo Ano

Autor: Prof. Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

1 Divisibilidade de números inteiros

Dados números inteiros a e b, com $a \neq 0$, dizemos que a **divide** b, e neste caso denotamos $a \mid b$, quando existe um inteiro q tal que $b = a \cdot q$. Alternativamente, se a divide b, dizemos também que b é um **múltiplo** de a, ou que b é **divisível** por a, ou ainda que a é um **divisor** de b. Quando não existe um inteiro q satisfazendo $b = a \cdot q$, dizemos que a não divide b e denotamos $a \nmid b$.

Assim, temos por exemplo que $2 \mid 8$ (uma vez que $8 = 2 \cdot 4$) e $-3 \mid 9$ (pois $9 = (-3) \cdot (-3)$), mas $5 \nmid 12$ (haja vista que a igualdade $12 = 5 \cdot q$, com $q \in \mathbb{Z}$, é impossível).

Por outro lado, dado um inteiro qualquer a, temos $a = 1 \cdot a$, de sorte que $1 \mid a$. Também, se $a \neq 0$, então $a = a \cdot 1$ garante que $a \mid a$, enquanto $0 = a \cdot 0$ garante que $a \mid 0$. Doravante, utilizaremos os fatos colecionados neste parágrafo sem maiores comentários. Também doravante, e sempre que não houver perigo de confusão, ao escrevermos $a \mid b$ suporemos implicitamente que a e b são inteiros, com $a \neq 0$.

Os três exemplos a seguir mostram como utilizar fatorações e produtos notáveis para estabelecer divisibilidades.

Exemplo 1. *Mostre que* $21 \mid (5^8 - 2^8)$.

Solução. Iniciamos observando que $5^8 = \left(5^4\right)^2$ e $2^8 = \left(2^4\right)^2$. Além disso, utilizando o produto notável

$$b^2 - a^2 = (b - a)(b + a),$$

obtemos:

$$5^8 - 2^8 = \left(5^4\right)^2 - \left(2^4\right)^2 = (5^4 - 2^4)(5^4 + 2^4).$$

Utilizando o produto notável citado acima outra vez, temos que

$$5^4 - 2^4 = \left(5^2\right)^2 - \left(2^2\right)^2 = (5^2 - 2^2)(5^2 + 2^2).$$

Por sua vez, substituindo tal fatoração de $5^4 - 2^4$ naquela de $5^8 - 2^8$, chegamos a

$$\begin{aligned} 5^8 - 2^8 &= (5^2 - 2^2)(5^2 + 2^2)(5^4 + 2^4) \\ &= (25 - 4)(5^2 + 2^2)(5^4 + 2^4) \\ &= 21 \cdot (5^2 + 2^2)(5^4 + 2^4). \end{aligned}$$

Por fim, como $(5^2 + 2^2)(5^4 + 2^4)$ é um inteiro, segue da definição que $21 \mid (5^8 - 2^8)$. $\square$

Observe que, no exemplo anterior, poderíamos ter calculado

$$5^8 - 2^8 = 390625 - 256 = 390369$$

e, em seguida, realizado a divisão desse número por 21 para obter $390369 = 21 \cdot 18589$. Contudo, o próximo exemplo mostra que, por vezes, esse procedimento direto é impraticável (para certificar-se dessa afirmação, tente calcular 2^{48} *exatamente* mesmo com o auxílio de uma calculadora).

Exemplo 2. *Mostre que* $2^{48} - 1$ *é divisível por* $63 \cdot 65$.

Solução. Utilizando a mesma estratégia do exemplo anterior, temos:

$$\begin{aligned} 2^{48} - 1 = 2^{48} - 1^{48} &= \left(2^{24}\right)^2 - \left(1^{24}\right)^2 \\ &= (2^{24} - 1^{24})(2^{24} + 1^{24}) \\ &= (2^{12} - 1^{12})(2^{12} + 1^{12})(2^{24} + 1^{24}) \\ &= (2^6 - 1^6)(2^6 + 1^6)(2^{12} + 1^{12})(2^{24} + 1^{24}) \\ &= 63 \cdot 65 \cdot (2^{12} + 1)(2^{24} + 1). \end{aligned}$$

Como $(2^{12} + 1)(2^{24} + 1)$ é inteiro, concluímos a partir dos cálculos acima que $63 \cdot 65$ realmente divide $2^{48} - 1$. $\square$

Exemplo 3. *Em um número natural N de 9 algarismos, tem-se que os algarismos das unidades simples, unidades de milhar e unidade de milhão são iguais a X; os algarismos das dezenas simples, dezenas de milhar e dezenas de milhão são iguais a Y; e os algarismos das centenas simples, centenas de milhar e centenas de milhão são iguais a Z. Pode-se afirmar que N sempre será divisível por:*

(a) 333664.

(b) 333665.

(c) 333666.

(d) 333667.

(e) 333668.

Solução. Pelas hipóteses que foram listadas no enunciado do problema, o número N deve ter representação decimal

$$N = ZYXZYXZYX.$$

Daí, temos:

$$\begin{aligned} N &= ZYXZYXZYX \\ &= Z \cdot 10^8 + Y \cdot 10^7 + X \cdot 10^6 + Z \cdot 10^5 + Y \cdot 10^4 \\ &\quad + X \cdot 10^3 + Z \cdot 10^2 + Y \cdot 10^1 + X \cdot 10^0 \\ &= Z \cdot 10^2 \cdot (10^6 + 10^3 + 1) + Y \cdot 10 \cdot (10^6 + 10^3 + 1) \\ &\quad + X \cdot (10^6 + 10^3 + 1) \\ &= (Z \cdot 10^2 + Y \cdot 10 + X)(10^6 + 10^3 + 1) \\ &= M \cdot 1001001, \end{aligned}$$

onde M tem representação decimal $M = ZYX$.

Observando que $1001001 = 3 \cdot 333667$, concluímos que

$$N = M \cdot 3 \cdot 333667,$$

de sorte que N será divisível por 333667. Portanto, a resposta correta é o item (d). $\square$

A noção de divisibilidade de inteiros possui várias propriedades importantes, algumas das quais aparecem colecionadas na proposição a seguir. Ao leitor interessado em perceber como tais propriedades podem ser utilizadas na solução de problemas envolvendo o conceito de divisibilidade, sugerimos adiar a leitura da demonstração da proposição, partindo imediatamente para os exemplos que a seguem e o material da próxima seção.

Proposição 4. *As seguintes propriedades da relação de divisibilidade são válidas:*

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

(b) *Se $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, quaisquer que sejam os inteiros m e n.*

(c) *Se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$.*

(d) *Se $a \mid b$ e $b \mid a$, então $|a| = |b|$.*

(e) *Se $b \mid c$ e $a \neq 0$, então $ab \mid ac$.*

(f) *Se $ab \mid ac$, então $b \mid c$.*

(g) *Se $a \mid b$ e $b \neq 0$, então $\frac{b}{a} \in \mathbb{Z}$ e $\frac{b}{a} \mid b$.*

Prova. Para o item (a), sejam q_1 e q_2 inteiros tais que $b = aq_1$ e $c = bq_2$. Então, temos:

$$c = bq_2 = (aq_1)q_2 = a(q_1q_2),$$

com $q_1a_2 \in \mathbb{Z}$; logo, $a \mid c$.

Se $a \mid b$ e $a \mid c$, então existem q_1 e q_2 inteiros tais que $b = aq_1$ e $c = aq_2$. Daí, se m e n são números inteiros quaisquer, temos:

$$\begin{aligned} mb + nc &= m(aq_1) + n(aq_2) \\ &= a(mq_1) + a(nq_2) \\ &= a(mq_1 + nq_2), \end{aligned}$$

com $mq_1 + nq_2 \in \mathbb{Z}$; assim, $a \mid (mb + nc)$ e o item (b) fica demonstrado.

Para o item (c), se $a \mid b$, então existe um inteiro q tal que $b = aq$. Sendo $b \neq 0$, temos $q \neq 0$, de sorte que $|q| \geq 1$. Portanto,

$$|b| = |aq| = |a||q| \geq |a| \cdot 1 = |a|,$$

conforme queríamos demonstrar.

Para a prova do item (d), comecemos observando que, se $a \mid b$ e $b \mid a$, então $a \neq 0$, $b \neq 0$. Portanto, segue do item (c) que

$$|a| \leq |b| \quad \text{e} \quad |b| \leq |a|,$$

o que por sua vez acarreta $|a| = |b|$.

Suponha agora que $b \mid c$ e escreva $c = bq$, para um certo inteiro q. Multiplicando ambos os membros dessa igualdade por um inteiro não nulo a, obtemos

$$ac = a(bq) = (ab)q,$$

o que garante que $(ab) \mid (ac)$ e prova o item (e).

Para o item (f), se $(ab) \mid (ac)$, então temos

$$ac = (ab)q = a(bq),$$

para algum inteiro q. Agora, como $ac \neq 0$, temos $a \neq 0$. Podemos, então cancelar a em ambos os membros da igualdade $ac = a(bq)$ para obter $c = bq$ ou, o que é o mesmo, $b \mid c$.

Finalmente, quanto ao item (g), se $a \mid b$, então existe $q \in \mathbb{Z}$ tal que $b = aq$. Sendo $b \neq 0$, temos $q \neq 0$. Por outro lado, uma vez que a última igualdade também pode ser escrita como $b = qa$, concluímos que $q \mid b$. Basta, agora, observar que $q = \frac{b}{a}$. □

Dois casos particulares do item (b) da proposição anterior, os quais resultam importantes em aplicações, são obtidos fazendo-se respectivamente $m = n = 1$ e $m = 1$, $n = -1$. Assim procedendo, concluímos que:

$$a \mid b \text{ e } a \mid c \Rightarrow \begin{cases} a \mid (b + c) \\ a \mid (b - c) \end{cases}. \tag{1}$$

Em palavras, podemos nos referir às divisibilidades acima da seguinte forma: *a soma e a diferença de dois múltiplos de um inteiro a continuam múltiplos de a.*

O exemplo a seguir explora esse círculo de ideias.

Exemplo 5. *Sejam a e b números naturais tais que $2a + b$ é divisível por 13. Qual das alternativas a seguir contém outro múltiplo de 13?*

(a) $91a + b$.

(b) $92a + b$.

(c) $93a + b$.

(d) $94a + b$.

(e) $95a + b$.

Solução. Note que $91a = 13 \cdot 7a$ é um múltiplo de 13. Como $2a + b$ é um múltiplo de 13 por hipótese, a discussão que antecede o enunciado do exemplo garante que

$$91a + (2a + b) = 93a + b$$

é também um múltiplo de 13. Portanto, a alternativa correta é o item (c). □

O próximo exemplo utiliza o mesmo tipo de ideia que os dois exemplos iniciais em uma situação genérica, para a qual também nos valeremos do resultado do item (a) da proposição anterior.

Exemplo 6. *Se a, m e n são inteiros positivos, com $m > n$, mostre que $\left(a^{2^n} + 1\right) \mid \left(a^{2^m} - 1\right)$.*

Solução. Observe inicialmente que

$$\left(a^{2^n}+1\right)\left(a^{2^n}-1\right)=\left(a^{2^n}\right)^2-1^2=a^{2^{n+1}}-1.$$

Logo,

$$\left(a^{2^n}+1\right) \mid \left(a^{2^{n+1}}-1\right).$$

Por outro lado, um cálculo análogo ao acima garante que, para um inteiro positivo k, temos:

$$\left(a^{2^k}+1\right)\left(a^{2^k}-1\right)=\left(a^{2^k}\right)^2-1^2=a^{2^{k+1}}-1.$$

Logo,

$$\left(a^{2^k}-1\right) \mid \left(a^{2^{k+1}}-1\right).$$

Agora, como $m>n$, temos $m=n+p$, em que p é um inteiro positivo. Portanto, combinando as divisibilidades estabelecidas acima com sucessivas aplicações do item (a) da proposição anterior (com k sucessivamente igual a $n+1$, $n+2$, ..., $n+p-1=m-1$), obtemos:

$$\left.\begin{array}{r}(a^{2^n}+1) \mid (a^{2^{n+1}}-1)\\ (a^{2^{n+1}}-1) \mid (a^{2^{n+2}}-1)\end{array}\right\} \Rightarrow (a^{2^n}+1) \mid (a^{2^{n+2}}-1);$$

$$\left.\begin{array}{r}(a^{2^n}+1) \mid (a^{2^{n+2}}-1)\\ (a^{2^{n+2}}-1) \mid (a^{2^{n+3}}-1)\end{array}\right\} \Rightarrow (a^{2^n}+1) \mid (a^{2^{n+3}}-1);$$

etc

$$\left.\begin{array}{r}(a^{2^n}+1) \mid (a^{2^{n+p-1}}-1)\\ (a^{2^{n+p-1}}-1) \mid (a^{2^{n+p}}-1)\end{array}\right\} \Rightarrow (a^{2^n}+1) \mid (a^{2^{n+p}}-1).$$

Por fim, essa última divisibilidade é o mesmo que

$$(a^{2^n}+1) \mid (a^{2^m}-1).$$

□

Exemplo 7. *Dados a, b e c inteiros positivos tais que $a+b+c$ é divisível por 6, prove que $a^3+b^3+c^3$ também é divisível por 6.*

Solução. Se $a+b+c$ é divisível por 6, então existe um inteiro q tal que $a+b+c=6q$. Daí, obtemos:

$$\begin{aligned} a+b+c=6q &\Rightarrow a+b=6q-c\\ &\Rightarrow (a+b)^3=(6q-c)^3\\ &\Rightarrow a^3+b^3+3ab(a+b)=\\ &\quad =216q^3-108q^2c+6qc^2-c^3.\end{aligned}$$

Observe que

$$216q^3-108q^2c+6qc^2=6(36q^3-18q^2c+qc^2).$$

Então, fazendo $p=36q^3-18q^2c+qc^2$, podemos escrever

$$a^3+b^3+3ab(a+b)=6p-c^3$$

ou, o que é o mesmo,

$$a^3+b^3+c^3=6p-3ab(a+b).$$

Afirmamos agora que $3ab(a+b)$ é sempre um múltiplo de 6. Realmente, se ao menos um dos inteiros a ou b for par, então $3ab(a+b)$ terá um fator 2 e, assim, será múltiplo de 6; por outro lado, se a e b forem ambos ímpares, então $a+b$ será par, de sorte que $3ab(a+b)$ novamente terá um fator 2 e, então, será múltiplo de 6.

Por fim, uma vez que tanto $6p$ quanto $3ab(a+b)$ são múltiplos de 6, segue de (1) (com 6 no lugar de a, $6p$ no lugar de b e $3ab(a+b)$ no lugar de c – nas notações de lá) que

$$6p-3ab(a+b)=a^3+b^3+c^3$$

também é múltiplo de 6. □

2 O algoritmo da divisão

Antes de enunciarmos o teorema conhecido como **Algoritmo da Divisão**, apresentamos abaixo, como ferramenta essencial para a sua demonstração, o **Teorema de Eudoxo**.

Teorema 8. *Se a e b são inteiros dados, com $b \neq 0$, então ou a é um múltiplo de b ou a se encontra entre dois múltiplos consecutivos de b.*

Prova. Suponha que $a>0$ e $b>0$ (os demais casos podem ser tratados de modo análogo a esse).

Se $a<b$, então a se encontra entre dois múltiplos consecutivos de b, que são $0=b\cdot 0$ e $b=b\cdot 1$. Suponha, pois, que $a>b$ e que a não é um múltiplo de b. Imagine duas pessoas, P_1 e P_2, situadas sobre a reta numerada, a uma distância de a unidades uma da outra, estando P_2 à frente de P_1 (no sentido positivo da reta). Em um certo momento, P_1 começa a caminhar em direção à P_2 com passos de comprimento b, até ultrapassá-la. Se P_1 deu q passos antes de chegar a P_2, mas ultrapassou P_2 após dar $q+1$ passos, então

$$bq<a \quad \text{mas} \quad b(q+1)>a.$$

Portanto, a está situado entre os múltiplos consecutivos bq e $b(q+1)$ de b. □

Podemos finalmente enunciar e provar o Algoritmo da Divisão.

Teorema 9. *Se a e b são números inteiros, com $b \neq 0$, então existem, e são únicos, inteiros q e r tais que*

$$a=bq+r, \text{ com } 0\le r<|b|.$$

*Os números q e r são chamados, respectivamente, **quociente** e **resto** da divisão de a por b.*

Prova. Como $|b| > 0$, o Teorema de Eudoxo (aplicado a a e a $|b|$) garante a existência de um número inteiro q tal que

$$|b|q' \leq a < |b|(q'+1).$$

(Observe que, nas desigualdades acima, contemplamos simultaneamente as possibilidades de a ser um múltiplo de $|b|$ – quando teremos $a = |b|q'$ – e de a não o ser.)

Daí, obtemos:

$$0 \leq a - |b|q' < |b|.$$

Fazendo $r = a - |b|q'$, segue então que:

$$a = |b|q' + r, \text{ com } 0 \leq r < |b|.$$

Mas, como $|b| = \pm b$, podemos escrever $|b|q' = bq$, com $q = \pm q'$. Fazendo assim, obtemos

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

Para o que falta, suponhamos que existisse outro par q_1 e r_1 de inteiros tais que

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

Então, teríamos:

$$\begin{aligned} bq + r = bq_1 + r_1 &\Rightarrow b(q - q_1) = r_1 - r \\ &\Rightarrow |(q-q_1)b| = |r_1 - r| \\ &\Rightarrow |q - q_1||b| = |r_1 - r|. \end{aligned}$$

A última igualdade nos diz que $|b|$ divide $|r_1 - r|$. Por outro lado, as desigualdades $0 \leq r < |b|$ e $0 \leq r_1 < |b|$ implicam que a distância entre r e r_1 não chega a $|b|$, isto é, que $|r_1 - r| < |b|$. Assim, pelo item (c) da Proposição 4, não podemos ter $|r_1 - r| \neq 0$ (pois aquele item, junto com a divisibilidade de $|r_1 - r|$ por $|b|$, acarretaria $|b| \leq |r_1 - r|$, o que não é o caso). Logo, temos $|r_1 - r| = 0$, ou seja $r_1 = r$. Daí, segue imediatamente que $q_1 = q$, de sorte que q e r são, de fato, os dois únicos inteiros que satisfazem as condições do enunciado. □

Uma elaboração útil do Algoritmo da Divisão é a que segue: imagine que dividimos um certo inteiro a por 4; o algoritmo da divisão afirma que obteremos um quociente q e um resto r, de modo que

$$a = 4q + r, \text{ com } 0 \leq r < 4.$$

Então, $r = 0, 1, 2$ ou 3, e isso significa que a (que é um inteiro arbitrário) pode ser escrito em uma das formas a seguir:

$$4q, \ 4q+1, \ 4q+2 \text{ ou } 4q+3.$$

Evidentemente, não há nada de especial no uso do inteiro 4 no argumento acima. De outra forma, um argumento análogo permite concluir que, dado um inteiro $b \neq 0$, temos que todo inteiro a pode ser escrito de uma das formas

$$bq, \ bq+1, \ \ldots, bq + (q-1),$$

para algum inteiro q, de acordo com o resto da divisão de a por b. Em particular, veja que a é divisível por b exatamente quando o resto da divisão de a por b for igual a 0.

Vejamos alguns exemplos.

Exemplo 10. *Um numero inteiro positivo k deixa resto 4 quando dividido por 7. Calcule o resto da divisão de $k^2 + k + 1$ por 7.*

Solução. Observe que, se k deixa resto 4 quando dividido por 7, então podemos escrever $k = 7q + 4$, para algum inteiro positivo q. Daí, obtemos:

$$\begin{aligned} k^2 + k + 7 &= (7q+4)^2 + (7q+4) + 1 \\ &= (49q^2 + 14q + 16) + 7q + 5 \\ &= 49q^2 + 21q + 21 \\ &= 7 \cdot (7q^2 + 3q + 3). \end{aligned}$$

Então, $k^2 + k + 1$ é divisível por 7, isto é deixa resto 0 quando dividido por 7. □

Exemplo 11. *Mostre que, na divisão de um quadrado perfeito por 4, os únicos restos possíveis são 0 e 1.*

Solução. Por definição, se n é um quadrado perfeito, então $n = m^2$ para algum inteiro não negativo m. Agora, conforme discutimos anteriormente, temos $m = 4q$, $m = 4q+1$, $m = 4q+2$ ou $m = 4q+3$, para algum inteiro não negativo q. Analisemos separadamente o que cada uma dessas quatro possibilidades diz sobre n:

(i) $m = 4q$: temos

$$n = m^2 = (4q)^2 = 16q^2 = 4 \cdot (4q^2),$$

de sorte que n deixa resto 0 quando dividido por 4.

(ii) $m = 4q + 1$: aqui,

$$\begin{aligned} n = m^2 &= (4q+1)^2 \\ &= 16q^2 + 8q + 1 \\ &= 4 \cdot (4q^2 + 2q) + 1. \end{aligned}$$

Então, n deixa resto 1 na divisão por 4.

(iii) $m = 4q + 2$: temos

$$\begin{aligned} n = m^2 &= (4q+2)^2 \\ &= 16q^2 + 16q + 4 \\ &= 4 \cdot (4q^2 + 4q + 1); \end{aligned}$$

novamente, n deixa resto 0 quando dividido por 4.

(iv) $m = 4q + 3$: segue que

$$\begin{aligned} n = m^2 &= (4q+3)^2 \\ &= 16q^2 + 24q + 9 \\ &= 4 \cdot (4q^2 + 6q + 2) + 1. \end{aligned}$$

Como no caso (ii), n deixa resto 1 na divisão por 4.

Em qualquer caso, verificamos que o resto da divisão do quadrado perfeito n por 4 é sempre igual a 0 ou 1. □

Exemplo 12. *Mostre que se a, b e c são inteiros tais que $a^2 + b^2 = c^2$, então a e b não são ambos ímpares.*

Solução. Por *contraposição*, suponha que a e b fossem ambos ímpares. Então, seus quadrados também o seriam. Mas, pelo exemplo anterior, quando dividimos um quadrado perfeito por 4, as únicas possibilidades para os restos dessa divisão são 0 ou 1. Sendo a^2 e b^2 ímpares, concluímos que devem existir inteiros q_1 e q_2 tais que $a^2 = 4q_1 + 1$ e $b^2 = 4q_2 + 1$. Isso implica

$$c^2 = a^2 + b^2 = 4(q_1 + q_2) + 2,$$

o que é um absurdo, pois, novamente utilizando o exemplo anterior, um quadrado perfeito não pode deixar resto 2 quando dividido por 4. □

Exemplo 13. (BANCO OBMEP 2016) *Júlia está treinando para olimpíadas de matemática. Um dia ela decide dividir* 2014 *por cada um dos divisores inteiros positivos de* 2015*. Para cada divisão, ela escreve o quociente no seu caderno e o resto em uma lousa. Vamos ajudar Júlia.*

(a) Escreva os oito divisores inteiros positivos de 2015.

(b) Para cada um desses divisores, faça a divisão de 2014 *por ele e escreva uma lista com os quocientes e outra com os restos obtidos.*

(c) Ao terminar, Júlia percebeu uma grande "coincidência": os números escritos no caderno eram os mesmos que estavam no quadro, apenas escritos em uma ordem diferente. Seria uma coincidência? Mostre que, para qualquer número n que Júlia escolher, se ela calcular o quociente e o resto da divisão de $n - 1$ por cada um dos divisores positivos de n, os números no caderno e na lousa serão exatamente os mesmos, estando apenas, possivelmente, escritos em uma ordem diferente.

Solução.

(a) Observe que a fatoração de 2015 como um produto de números primos é $5 \cdot 13 \cdot 31$. Portanto, de fato, 2015 tem 8 divisores positivos, que são:

$$1, 5, 13, 31, 65, 155, 403 \text{ e } 2015.$$

(b) Efetuando as divisões de 2014 por cada um dos divisores de 2015 encontrados no item anterior, obtemos:

$$\begin{aligned} 2014 &= 1 \cdot 2014 + 0 \\ 2014 &= 5 \cdot 402 + 4 \\ 2014 &= 13 \cdot 154 + 12 \\ 2014 &= 31 \cdot 64 + 30 \\ 2014 &= 65 \cdot 30 + 64 \\ 2014 &= 155 \cdot 12 + 154 \\ 2014 &= 403 \cdot 4 + 402 \\ 2014 &= 2015 \cdot 0 + 2014. \end{aligned}$$

Portanto, as listas dos quocientes e dos restos realmente coincidem:

$$0, 4, 12, 30, 64, 154, 402 \text{ e } 2014.$$

Note que, além dos números nas duas listas serem os mesmos, eles são exatamente os antecessores dos divisores positivos de 2015.

(c) Agora, se x é um divisor positivo de n, então existe $y \in \mathbb{Z}$ (que também é um divisor positivo de n) tal que $n = xy$. Observe que

$$\begin{aligned} n = xy &\Longrightarrow n - 1 = xy - 1 \\ &\Longrightarrow n - 1 = xy - x + x - 1 \\ &\Longrightarrow n - 1 = x(y-1) + (x-1) \end{aligned}$$

e

$$\begin{aligned} n = xy &\Longrightarrow n - 1 = xy - 1 \\ &\Longrightarrow n - 1 = xy - y + y - 1 \\ &\Longrightarrow n - 1 = y(x-1) + (y-1). \end{aligned}$$

Como $0 \le x - 1 < x$ e $0 \le y - 1 < y$, então, por unicidade, os restos nas divisões de $n - 1$ por x e por y são respectivamente iguais a $x - 1$ e $y - 1$, e os quocientes nas mesmas divisões são respectivamente iguais a $y - 1$ e $x - 1$. Vale ressaltar que, se $x = y$ (caso em que n é um quadrado perfeito), então

$$\begin{aligned} n = x^2 &\Longrightarrow n - 1 = x^2 - 1 \\ &\Longrightarrow n - 1 = x^2 - x + x - 1 \\ &\Longrightarrow n - 1 = x(x-1) + (x-1), \end{aligned}$$

ou seja, temos apenas uma divisão, com quociente e resto iguais. Portanto, a lista formada com os quocientes é a mesma que a lista formada com os restos.

□

Dicas para o Professor

Recomendamos que sejam utilizadas uma sessão de 50min para discutir cada uma das seções que compõem esse material. Na seção 1, explique com muito cuidado as propriedades da divisão de números inteiros, enfatizando a aplicação das propriedades nos exemplos resolvidos. Isso facilitará o entendimento por parte dos alunos. Nos exemplos que fazem parte da seção 2, chame a atenção dos alunos para os pontos nos quais o Algoritmo da Divisão esteja sendo utilizado, pois muitas vezes esse teorema é utilizado sem que eles percebam.

As referências colecionadas a seguir contém muitos problemas e exemplos relacionados ao conteúdo do presente material.

Sugestões de Leitura Complementar

1. A. Caminha. *Tópicos de Matemática Elementar Volume 5: Teoria do Números*, 2ª Edição. Rio de Janeiro, SBM, 2013.

2. D. Fomin, S. Genkin e I. Itenberg. *Mathematical World, Volume 8: Mathematical Circles (Russian Experience)*. AMS, 1996.

3. J. P. O. Santos. *Introdução à Teoria dos Números.* Rio de Janeiro, SBM, 2000.