Números inteiros: alguns critérios de divisibilidade

André Fonseca e Teresa Almada
Universidade Lusófona
andre.fonseca@ulusofona.pt, talmada@ulusofona.pt

Os programas do Ensino Básico incluem vários critérios de divisibilidade de números naturais. Neste artigo apresentamos um critério de divisibilidade para números inteiros que, apesar do seu nível de generalidade, tem uma demonstração muito simples. Apresentamos também um critério de divisibilidade por 7 que generalizamos a qualquer número primo com 10. Grande parte do artigo está escrita numa linguagem simples e informal, de modo a que possa ser lido mesmo por quem está a iniciar-se no estudo da matemática.

PRELIMINARES

Muitas questões relacionadas com o conceito de divisibilidade estão diretamente ligadas à possibilidade da divisão inteira no conjunto $\mathbb{Z}$ dos números inteiros. Começamos por ver que realmente é possível efetuar a divisão inteira em $\mathbb{Z}$. Antes, porém, recordamos como é que aprendemos, no 1.º ciclo, o algoritmo da divisão. Por exemplo, para dividirmos 9 por 4, perguntamos: "Em 9 quantas vezes há 4?" A resposta é 2. Em 9 há duas vezes 4 e sobra 1. Para dividirmos 25 por 7, perguntamos: "Em 25 quantas vezes há 7?" E a resposta é 3 e sobram 4. Na verdade, perguntar "quantas vezes há d $(d > 0)$ num número a", equivale a perguntar "qual é o número máximo de d's que há em a?", ou ainda, a perguntar "quando é que a diferença $a - dq$ é mínima e não negativa?". Dizer que há "q vezes d em a" equivale a dizer que $a - dq \geq 0$ e que q é máximo, isto é, a diferença $a - dq$ é mínima, ou seja, $0 \leq a - dq < d$.

Proposição 1. *Se a e d são números inteiros e d é não nulo, então existem números inteiros q e r, únicos, de tal modo que*

$$a = dq + r \text{ e } 0 \leq r < |d|.$$

Demonstração. Comecemos por demonstrar o resultado para $d>0$. Procuramos um número q de tal modo que a diferença $a - dq$ seja mínima e não negativa, isto é, pretendemos encontrar o elemento mínimo do conjunto

$X = \{a - dx : x \text{ é um número inteiro e } a - dx \geq 0\}$.

Como os elementos do conjunto X pertencem a $\mathbb{N}_0$, se este conjunto for não vazio, existe o elemento mínimo de X. Como $d \geq 1$, então $d|a| \geq |a| \geq -a$, ou seja, $a + d|a| \geq 0$. Logo, $a + d|a|$ é um elemento do conjunto X e, portanto, o conjunto X é não vazio. Seja r o elemento mínimo do conjunto X e seja q um número inteiro tal que

$$r = a - dq, \text{ ou seja, } a = dq + r$$

Demonstremos que $r < d$. Se $r < d$, então

$$a - dq - d = a - d(q + 1) \geq 0.$$

Como $a - d(q + 1)$ pertence a X e $a - d(q + 1) \leq a - dq$, chegamos a uma contradição.

Provemos a unicidade dos números q e r nas condições referidas demonstrando que se q , q', r e r' designam números inteiros verificando as condições

$a = dq + r$ com $0 \leq r < d$ e $a = dq' + r'$ com $0 \leq r' < d$,

então

$$q = q' \text{ e } r = r'$$

Suponhamos que $dq + r = a = dq' + r'$. Como $d(q - q') = r' - r$, tem-se $|d(q - q')| = |r' - r|$.

Como

$$0 \leq r' < d \text{ e } 0 \leq r < d,$$

concluímos que

$$-d < r' - r < d, \text{ ou seja, } |r' - r| < d.$$

Assim,

$$d|q - q'| = |r' - r| < d \text{ isto é, } d|q - q'| < d.$$

Como d pertence a $\mathbb{N}$, terá de ser $|q - q'| = 0$, ou seja, $q = q'$. Então $dq + r = dq + r'$ e, portanto, $r = r'$.

Se $d < 0$, então $-d > 0$ e, portanto, existem q e r, únicos, tais que $a = -dq + r$, com $0 \leq r < -d$. Logo, $a = d(-q) + r$ com $0 \leq r < |d|$.

Vejamos alguns exemplos da divisão inteira em $\mathbb{Z}$.

Dividendo	Divisor	Quociente	Resto
-15	3	-5	0
15	-3	5	0
-21	6	-4	3
-21	-6	4	3

Dados a e d números inteiros e supondo que d é diferente de zero, dizemos que *d é um divisor de a*, ou que *d divide a*, ou ainda que *a é divisível por d*, ou até mesmo que *a é um múltiplo de d*, se o resto da divisão inteira de a por d é zero, isto é, se existir um número inteiro q de tal modo que $a = dq$.

Verificamos facilmente que se um número inteiro a é divisível por um produto d_1d_2 de números inteiros não nulos, então é divisível por cada um dos fatores d_1 e d_2. Com efeito, se

$$a = (d_1d_2)q, \text{ então } a = d_1(d_2q) \text{ e } a = d_2(d_1q).$$

No entanto, um número inteiro a ser divisível por d_1 e por d_2 não garante que a seja divisível pelo produto d_1d_2. Por exemplo, 36 é divisível por 3 e por 9 e, no entanto, não é divisível por 27. Há, no entanto, uma condição que garante que um número ao ser divisível por dois números é também divisível pelo seu produto. A demonstração deste resultado, que será apresentada mais à frente, envolve os conceitos de máximo divisor comum, de números primos entre si e de número primo. Antes de os recordarmos, apresentamos alguns resultados preliminares.

Se n é um número inteiro, representamos por $n\mathbb{Z}$ o conjunto de todos os múltiplos de n.

O conjunto $n\mathbb{Z}$ dos múltiplos de n tem as seguintes propriedades:

1. O conjunto $n\mathbb{Z}$ é não vazio, pois $0 = n \times 0$;
2. Se a pertence a $n\mathbb{Z}$ e b pertence a $n\mathbb{Z}$, então $a - b$ pertence a $n\mathbb{Z}$.
3. Se a pertence a $n\mathbb{Z}$ e m pertence a $\mathbb{Z}$, então ma pertence a $n\mathbb{Z}$.

Porque o conjunto $n\mathbb{Z}$ tem as propriedades (1) a (3), dizemos que $n\mathbb{Z}$ é um *ideal* de $\mathbb{Z}$.

A qualquer subconjunto de $\mathbb{Z}$ com estas propriedades chamamos um *ideal* de $\mathbb{Z}$, isto é, um ideal de $\mathbb{Z}$ é um subconjunto I de $\mathbb{Z}$ com as propriedades:

1. O conjunto I é não vazio;
2. Se a e b são elementos de I, então $a - b$ é um elemento de I;
3. Se a é um elemento de I e α é um número inteiro qualquer, então $a\alpha$ é um elemento de I.

Observamos que o conjunto $T = \{0\}$ e o conjunto $\mathbb{Z}$ são ideais de $\mathbb{Z}$, já que $T = 0\mathbb{Z}$ e $\mathbb{Z} = 1\mathbb{Z}$.

Um número inteiro d não nulo é divisor de um inteiro a se, e só se, a é um elemento de $d\mathbb{Z}$. Este facto evidencia o papel dos ideais na teoria da divisibilidade.

Observamos que se I é um ideal de $\mathbb{Z}$, então zero é um elemento de I. De facto, por I ser não vazio, existe um elemento a em I. Da propriedade 2 resulta que $a - a = 0$ é um elemento de I. Além disso, se a é um elemento de I, o mesmo acontece com $-a$, pois se a é um elemento de I, então, pela propriedade 2, $0 - a = -a$ é um elemento de I.

Proposição 2. *Um subconjunto I de $\mathbb{Z}$ é um ideal de $\mathbb{Z}$ se, e só se, existe um número inteiro não negativo n de tal modo que $I = n\mathbb{Z}$.*

Demonstração. Do que observámos antes decorre que os conjuntos da forma $n\mathbb{Z}$ são ideais de $\mathbb{Z}$. Falta mostrar que se I é um ideal de $\mathbb{Z}$, então existe um número inteiro não negativo n de tal modo que $I = n\mathbb{Z}$.

Seja I um ideal de $\mathbb{Z}$. Se $I = \{0\}$, então $I = 0\mathbb{Z}$. Suponhamos que $I \neq \{0\}$ e seja a um elemento não nulo de I. Ou $a > 0$ ou $-a > 0$, pelo que o conjunto P definido por $P = \{x \in I : x > 0\}$ é não vazio e os seus elementos são números naturais. Seja n o elemento mínimo de P e vejamos que $I = n\mathbb{Z}$. De acordo com a propriedade 3 da definição de ideal, qualquer múltiplo de n é um elemento de I, já que sendo n um elemento de P, n é também um elemento de I. Reciprocamente, seja a um elemento de I e vejamos que a é um múltiplo de n. Como n é diferente de zero, pela proposição 1 podemos garantir a existência de números inteiros q e r de tal modo que

$$a = nq + r \text{ e } 0 \leq r < n.$$

Pretendemos provar que $r = 0$. Se $r \neq 0$, então seria $a - nq = r > 0$. Como a e n são elementos de I, o mesmo acontece com $a - nq$ (propriedades 2 e 3 da definição de ideal). Assim, $a - nq$ é um elemento positivo de I e, portanto, um elemento de P. Dado que n é o elemento mínimo de P, tem-se que $n \leq a - nq = r$, contrariando o facto de se ter $r < n$.

Logo, $r = 0$ e, portanto, $a = nq$ é um elemento de $n\mathbb{Z}$.

Esta proposição permite mostrar que dados dois números inteiros, não ambos nulos, existe em $\mathbb{Z}$ o máximo divisor comum desses números. Antes, porém, recordamos a definição de máximo divisor comum de dois números inteiros.

Dados números inteiros a e b, não ambos nulos, um número inteiro positivo d diz-se *máximo divisor comum* de a e b se

1. d é divisor de a e de b, ou seja, d é divisor comum de a e b;
2. Se c é divisor de a e de b, então c é um divisor de d.

Proposição 3. *Se a e b são números inteiros não ambos nulos, então existe e é único o máximo divisor comum de a e b.*

Demonstração. Consideremos o conjunto I definido por

$$I = \{ax + by : x \text{ e } y \text{ são números inteiros arbitrários}\}.$$

Provemos que I é um ideal de $\mathbb{Z}$. I é não vazio pois, por exemplo, $a = a \times 1 + b \times 0$ e $b = a \times 0 + b \times 1$ são elementos de I.

Se $ax + by$ e $ax' + by'$ são elementos de I, então,

$$(ax + by) - (ax' + by') = a(x - x') + b(y - y)$$

o que prova que $ax + by - (ax' + by')$ é um elemento de I, e se $ax + by$ é um elemento de I e z é um número inteiro, então $z(ax + by) = a(zx) + b(zy)$ é um elemento de I. Assim, I é um ideal de $\mathbb{Z}$.

Como a e b são elementos de I e a e b não são ambos nulos, então, pela proposição 2, existe um número inteiro positivo d de tal modo que $I = d\mathbb{Z}$. Provemos que d é o máximo divisor comum de a e b.

Como a e b são elementos de $d\mathbb{Z}$, concluímos que d é um divisor comum a a e a b. Suponhamos que c é um divisor de a e de b. Então, a e b são elementos de $c\mathbb{Z}$ e, como este conjunto é um ideal, todos os elementos de $I = d\mathbb{Z}$ são elementos de $c\mathbb{Z}$, em particular o número $d = d \times 1$ é um elemento de $c\mathbb{Z}$, o que prova que c é um divisor de d.

Quanto à unicidade, observe-se que se d e d' são ambos máximos divisores comuns de a e de b, então, pela definição de máximo divisor comum, podemos afirmar que d divide d' e que d' divide d. Em $\mathbb{Z}$, tem-se $d = d'$ ou $d = -d'$, mas como um máximo divisor comum é, por definição, um inteiro positivo, concluímos que $d = d'$.

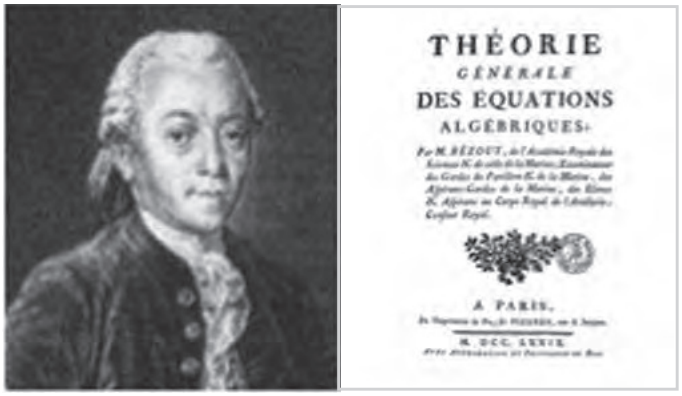
Se a e b são números inteiros não ambos nulos, escrevemos $d = \text{mdc}\,(a, b)$ para significar que d é o máximo divisor comum de a e b.

Corolário. Identidade de Bézout. *Se a e b são números inteiros não ambos nulos e $d = mdc(a,b)$, então existem números inteiros x e y tais que $d = ax + by$.*

Demonstração. Da demonstração da proposição anterior decorre que d é um elemento do conjunto

$$I = \{ax + by : x \text{ e y são números inteiros arbitrários}\}.$$

Assim, podemos garantir a existência de números inteiros x e y tais que $d = ax + by$.



Étienne Bézout (1730–1783)

Observamos que os números inteiros x e y referidos na identidade de Bézout não são determinados de modo único. Por exemplo, mdc (4, 6) = 2 e $4 \times (-1) + 6 \times 1 = 2 = 4 \times 2 + 6 \times (-1)$.

Esta identidade foi provada pelo matemático francês Étienne Bézout, autor de várias obras, das quais destacamos *Théorie générale des équations algebriques*. Esta obra existe na Biblioteca Nacional de França e pode ser consultada em *http://www.bnf.fr/fr/acc/x.accueil.html*

Recordamos que p se diz *primo* se p admitir exatamente dois divisores positivos distintos, a saber: o número 1 e o número $|p|$.

De acordo com a definição, os números -1, 0 e 1 não são números primos, pois -1 e 1 têm apenas um divisor positivo, enquanto qualquer número inteiro positivo é divisor de 0.

Decorre das definições de número primo e de máximo divisor comum que se p é um número primo e a é um número inteiro não divisível por p, então $\text{mdc}(p, a) = 1$.

Dois números inteiros a e b dizem-se *primos entre si* se $\text{mdc}(a, b) = 1$.

Proposição 4. *Sejam a, b e p números inteiros e suponhamos que p é distinto de -1, de 0 e de 1.*

O número p é um número primo se, e só se, p dividir a ou dividir b, sempre que p divida o produto ab.

Demonstração. Suponhamos que p é um número primo e admitamos que p divide o produto ab e não divide a. Queremos mostrar que p divide b. Como p é primo e não divide a, então $\text{mdc}(p, a) = 1$. Pela identidade de Bézout existem números inteiros x e y tais que $px + ay = 1$. Então,

$$b = pbx + aby.$$

Como p divide o produto ab, existe um número inteiro q de tal modo que $ab = pq$. Substituindo ab na igualdade $b = pbx + aby$, obtemos que $b = pbx + pqy = p(bx + qy)$, ficando assim provado que p divide b.

Reciprocamente, suponhamos que se p divide um produto, então p divide um dos fatores e provemos que p é um número primo. Demonstremos que se d é um divisor positivo de p, então $d = 1$ ou $d = |p|$.

Seja d um divisor positivo de p. Então existe um número inteiro k de tal modo que $p = dk$. Todo o número inteiro não nulo é divisor de si próprio. Assim, p divide dk pelo que, usando a hipótese, se tem

$$p \text{ divide } d \text{ ou } p \text{ divide } k.$$

Se p divide d, então existe um número inteiro q_1 de tal modo que $d = pq_1$. Substituindo d na igualdade $p = dk$, obtemos $p = kq_1$. Logo, $kq_1 = 1$, ou seja, $k = 1$ ou $k = -1$. Se $k = -1$, então $d = -p = |p|$. Se $k = 1$, então $d = p = |p|$.

Se p divide k, existe um número inteiro q_2 de tal modo que $k = pq_2$. Substituindo k na igualdade $p = dk$, obtemos $p = pdq_2$, donde $dq_2 = 1$ e, consequentemente, $d = 1$.

ALGUNS CRITÉRIOS DE DIVISIBILIDADE

Proposição 5. *Sejam a, d_1 e d_2 números inteiros e suponhamos que d_1 e d_2 são números primos entre si. Tem-se que o produto d_1d_2 é um divisor de a se, e só se, os números d_1 e d_2 são divisores de a.*

Demonstração. Conforme foi observado anteriormente, se a é divisível por d_1d_2, então a é divisível por d_1 e por d_2. Suponhamos que um número inteiro a é divisível por d_1 e por d_2 com d_1 e d_2 primos entre si e demonstremos que a é divisível por d_1d_2. Sejam q_1 e q_2 números inteiros tais que

$$a = d_1q_1 \text{ e } a = d_2q_2.$$

Como $\text{mdc}(d_1, d_2) = 1$, pela identidade de Bézout, existem números inteiros x e y tais que $d_1x + d_2y = 1$. Tem-se

$$a = d_1ax + d_2ay = d_1d_2q_2x + d_2d_1q_1y = d_1d_2(q_2x + q_1y),$$

o que prova que o produto d_1d_2 divide a.

Esta proposição permite deduzir vários critérios de divisibilidade. Enunciamos, a título de exemplo, apenas alguns desses critérios.

Critério de divisibilidade por 6. Um número inteiro é divisível por 6 se, e só se, é divisível por 2 e por 3.

Critério de divisibilidade por 12. Um número inteiro é divisível por 12 se, e só se, é divisível por 3 e por 4.

Critério de divisibilidade por 14. Um número inteiro é divisível por 14 se, e só se, é divisível por 2 e por 7.

Critério de divisibilidade por 15. Um número inteiro é divisível por 15 se, e só se, é divisível por 3 e por 5.

Critério de divisibilidade por 18. Um número inteiro é divisível por 18 se, e só se, é divisível por 2 e por 9.

Critério de divisibilidade por 21. Um número inteiro é divisível por 21 se, e só se, é divisível por 3 e por 7.

CONGRUÊNCIAS

Se a, b e n são números inteiros e $n > 0$, dizemos que *a é congruente com b módulo n* se a e b têm o mesmo resto na divisão inteira por n. Neste caso escrevemos

$$a \equiv b (\text{mod} n).$$

Verificamos facilmente que se a, b e c são números inteiros, então

1. *Reflexividade:* $a \equiv a (\text{mod} n)$;
2. *Simetria*: se $a \equiv b (\text{mod} n)$, então $b \equiv a (\text{mod} n)$;
3. *Transitividade:* se $a \equiv b (\text{mod} n)$ e $b \equiv c (\text{mod} n)$, então $a \equiv c (\text{mod} n)$.

Porque a relação binária $\equiv (\text{mod} n)$ tem as propriedades (1) a (3), dizemos que a relação é uma *relação de equivalência*. Uma *relação de congruência* é uma relação de equivalência compatível com a operação de adição e com a operação de multiplicação.

Proposição 6. *Se a, b e n são números inteiros e n é positivo, então $a \equiv b (\text{mod} n)$ se, e só se, n é um divisor de $a - b$.*

Demonstração. Suponhamos que $a \equiv b (\text{mod} n)$. Então, a e b têm o mesmo resto na divisão inteira por n e, portanto, existem números inteiros q_1, q_2 e r tais que

$$a = nq_1 + r \text{ e } b = nq_2 + r, \text{ com } 0 \leq r < n.$$

Como $a - b = n(q_1 - q_2)$ concluímos que n divide $a - b$.

Reciprocamente, suponhamos que n é um divisor de $a - b$ e seja q um número inteiro tal que

$$a - b = nq.$$

Sejam q_1, q_2, r_1 e r_2 números inteiros tais que $a = nq_1 + r_1$ e $b = nq_2 + r_2$, com $0 \leq r_1, r_2 < n$.

Suponhamos que $r_2 \leq r_1$. Então

$$nq = a - b = n(q_1 + q_2) + (r_1 - r_2).$$

Como $0 \leq r_1 - r_2 < n$, então, pela unicidade do resto, obtemos que $r_1 = r_2$, ou seja $a \equiv b(\mathrm{mod} n)$.

Proposição 7. *Sejam a, b, c, d e n números inteiros com n positivo. Se $a \equiv b(\mathrm{mod} n)$ e $c \equiv d(\mathrm{mod} n)$, então $a + c \equiv b + d(\mathrm{mod}\ n)$ e $ac \equiv bd(\mathrm{mod} n)$.*

Demonstração. Suponhamos que $a \equiv b(\mathrm{mod} n)$ e $c \equiv d(\mathrm{mod} n)$. Então, $a - b$ e $c - d$ são múltiplos de n. Assim,

$$(a + c) - (b + d) = (a - b) + (c - d)$$

é um múltiplo de n e, portanto, $a + c \equiv b + d(\mathrm{mod}\ n)$.

Por outro lado, $ac - bd = (a - b)c + (c - d)b$ é múltiplo de n, e, portanto, $ac \equiv bd(\mathrm{mod} n)$.

Se a e n são números inteiros e n é positivo, representamos por $[a]_{\equiv(\mathrm{mod} n)}$ o conjunto de todos os números inteiros congruentes com a módulo n. A este conjunto chamamos *classe de congruência módulo n* do número inteiro a, isto é, o conjunto de todos os números inteiros que têm o mesmo resto que a na divisão inteira por n.

Tem-se

$$[a]_{\equiv(\mathrm{mod} n)} = [b]_{\equiv(\mathrm{mod} n)} \text{ se, e só se, } a \equiv b(\mathrm{mod} n).$$

É de notar que se a é um número inteiro, então

$$[a]_{\equiv(\mathrm{mod} n)} = [r]_{\equiv(\mathrm{mod} n)}$$

onde r é o resto da divisão inteira de a por n. Como os restos possíveis na divisão inteira por n são os números inteiros de 0 a $n - 1$, concluímos que existem exatamente n classes de congruência módulo n distintas.

Por exemplo, as classes de congruência módulo 5 são $[0]_{\equiv(\mathrm{mod} n)}$, $[1]_{\equiv(\mathrm{mod} n)}$, $[2]_{\equiv(\mathrm{mod} n)}$, $[3]_{\equiv(\mathrm{mod} n)}$ e $[4]_{\equiv(\mathrm{mod} n)}$.

A compatibilidade da relação $\equiv (\mathrm{mod} n)$ com as operações de adição e de multiplicação, permite definir no conjunto das classes de congruência módulo n uma operação de adição e uma operação de multiplicação do seguinte modo:

$$[a]_{\equiv(\mathrm{mod} n)} + [b]_{\equiv(\mathrm{mod} n)} = [a + b]_{\equiv(\mathrm{mod} n)}$$

e

$$[a]_{\equiv(\mathrm{mod} n)} \times [b]_{\equiv(\mathrm{mod} n)} = [ab]_{\equiv(\mathrm{mod} n)}.$$

Por exemplo,

$$[3]_{\equiv(\mathrm{mod}5)} + [4]_{\equiv(\mathrm{mod}5)} = [7]_{\equiv(\mathrm{mod}5)} = [2]_{\equiv(\mathrm{mod}5)}$$

e

$$[2]_{\equiv(\mathrm{mod}5)} \times [4]_{\equiv(\mathrm{mod}5)} = [8]_{\equiv(\mathrm{mod}5)} = [3]_{\equiv(\mathrm{mod}5)}.$$

CRITÉRIO GERAL DE DIVISIBILIDADE

Observamos que, dados números inteiros a e d, com d não nulo, provar que a é divisível por d é mostrar que a divisão inteira de a por d é exata, ou seja, que o resto da divisão é zero, isto é,

$$[a]_{\equiv(\mathrm{mod} d)} = [0]_{\equiv(\mathrm{mod} d)}.$$

Consideremos o número 27564. Como é sabido, este número pode ser representado na forma

$$27564 = 2\mathrm{x}10^4 + 7\mathrm{x}10^3 + 5\mathrm{x}10^2 + 6\mathrm{x}10^1 + 4\mathrm{x}10^0.$$

Na verdade, qualquer número inteiro pode ser escrito naquela forma. Se $a = a_k a_{k-1} \ldots a_1 a_0$ é a representação no sistema decimal de um número inteiro a, então

$$a = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0 = \sum_{i\ 0}^{k} a_1 10^i.$$

Dados números inteiros não negativos i e d, com d diferente de zero, representamos por R_{id} o *resto da divisão inteira de* 10^i *por* d. Do que dissemos antes, resulta que

$$[10^i]_{\equiv(\mathrm{mod} d)} = [R_{id}]_{\equiv(\mathrm{mod} d)}.$$

Proposição 8. ***Critério geral de divisibilidade.***
Sejam $a = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$ e d números inteiros e suponhamos que d é não nulo.

Tem-se que o número a é divisível por d se, e só se, o número inteiro $\sum_{i=0}^{k} a_i R_{id}$ é divisível por d.

Demonstração. O número a é divisível por d se, e só se,

$$[a]_{\equiv(\mathrm{mod} d)} = [0]_{\equiv(\mathrm{mod} d)}.$$

Mas

$$\begin{aligned}
[a]_{\equiv(\mathrm{mod} d)} &= [\sum_{i=0}^{k} a_i 10^i]_{\equiv(\mathrm{mod} d)} = \\
&= \sum_{i=0}^{k} [a_i]_{\equiv(\mathrm{mod}\ d)} \times [10^i]_{\equiv(\mathrm{mod}\ d)} \\
&= \sum_{i=0}^{k} [a_i]_{\equiv(\mathrm{mod} d)} \times [R_{id}]_{\equiv(\mathrm{mod} d)} = \\
&= [\sum_{i=0}^{k} a_i R_{id}]_{\equiv(\mathrm{mod} d)}.
\end{aligned}$$

Assim,

$[a]_{\equiv(\mathrm{mod} d)} = [0]_{\equiv(\mathrm{mod} d)}$ se, e só se,

$$[\sum_{i=0}^{k} a_i R_{id}]_{\equiv(\mathrm{mod} d)} = [0]_{\equiv(\mathrm{mod} d)}$$

e, portanto,

a é divisível por d se, e só se, o número inteiro $\sum_{i=0}^{k} a_i R_{id}$ é divisível por d.

Corolário 1. *Critério de divisibilidade por 2. Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 2 se, e só se, o algarismo das unidades, a_0, é um número par.*

Demonstração. Como $R_{i2} = 0$ sempre que $i > 0$ e $R_{02} = 1$, então $\sum_{i=0}^{k} a_i R_{i2} = a_0$ e, portanto, de acordo com a proposição anterior, a é divisível por 2 se, e só se, a_0 é divisível por 2 ou, equivalentemente, a_0 é um número par.

Corolário 2. *Critério de divisibilidade por 3. Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 3 se, e só se, o número $\sum_{i=0}^{k} a_i$ é divisível por 3.*

Demonstração. Como $R_{i3} = 1$, qualquer que seja o i, então a é divisível por 3 se, e só se, $\sum_{i=0}^{k} a_i R_{i3} = \sum_{i=0}^{k} a_i$, é divisível por 3. Assim, um número inteiro é divisível por 3 se, e só se, a soma dos seus algarismos é divisível por 3.

Corolário 3. Critério de divisibilidade por 4. *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 4 se, e só se, o número $a_1\, a_0$ é divisível por 4.*

Demonstração. Como $R_{14} = 2$, $R_{04} = 1$ e $R_{i4} = 0$, sempre que i seja maior do que 1, então a é divisível por 4 se, e só se, $\sum_{i=0}^{k} a_i R_{i4} = 2a_i + a_0$ é divisível por 4. Assim, de acordo com a proposição 8, $2a_1 + a_0$ é divisível por 4 se, e só se, $10a_1 + a_0$ é divisível por 4, ou seja, um número inteiro é divisível por 4 se, e só se, o número constituído pelos seus dois últimos algarismos for divisível por 4.

Corolário 4. *Critério de divisibilidade por 5. Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 5 se, e só se, o algarismo das unidades, a_0, é zero ou cinco.*

Demonstração. Como $R_{i5} = 0$, sempre que $i > 0$ e $R_{05} = 1$, então $\sum_{i=0}^{k} a_i R_{i5} = a_0$.

Logo, a é divisível por 5 se, e só se, $a_0 = 0$ ou $a_0 = 5$. Logo, um número inteiro é divisível por 5 se, e só se, o algarismo das unidades é 0 ou 5.

Corolário 5. Critério de divisibilidade por 6. *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 6 se, e só se, o algarismo das unidades é um número par e a soma $\sum_{i=0}^{k} a_i$ é divisível por 3.*

Demonstração. De acordo com a proposição 5, o número a é divisível por 6 se, e só se, é divisível por 2 e por 3. O resultado decorre dos corolários 1 e 2.

Corolário 6. *Critério de divisibilidade por 8. Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 8 se, e só se, o número $a_2\ a_1\ a_0$ é divisível por 8.*

Demonstração. Como $R_{28} = 4$, $R_{18} = 2$, $R_{08} = 1$ e $R_{i8} = 0$ sempre que $i \geq 3$, então

$$\sum_{i=0}^{k} a_i R_{i8} = 4a_2 + 2a_1 + a_0.$$

Logo, de acordo com a proposição 8, o número $4a_2 + 2a_1 + a_0$ é divisível por 8 se, e só se, o mesmo acontece com $a_2 a_1 a_0 = 10^2 a_2 + 10a_1 + a_0$, ou seja, um número inteiro é divisível por 8 se, e só se, o número constituído pelos seus três últimos algarismos é divisível por 8.

Corolário 7. *Critério de divisibilidade por 9.* Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 9 se, e só se, a soma $\sum_{i=0}^{k} a_i$ é divisível por 9.

Demonstração. O resultado decorre imediatamente da proposição 8 e do facto de $R_{i9} = 1$ qualquer que seja o $i > 0$.

Corolário 8. *Critério de divisibilidade por 10.* Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 10 se, e só se, $a_0 = 0$.

Demonstração. O resultado decorre do critério geral e do facto de se ter $R_{0,10} = 1$ e $R_{i10} = 0$ sempre que $i \geq 1$.

CRITÉRIO DE DIVISIBILIDADE POR UM NÚMERO PRIMO SUPERIOR A 5

Seja a um inteiro e suponhamos que

$$a = a_k...a_1 a_0 = \sum_{i=0}^{k} a_i 10^i.$$

Notemos que o número inteiro

$$b = a_k \ldots a_1 \text{ se escreve na forma } \sum_{i=1}^{k} a_i 10^{i-l}.$$

Proposição 9. *Critério de divisibilidade por 7. Um número inteiro $a = a_k...a_1 a_0$ é divisível por 7 se, e só se, o número inteiro $a_k...a_1 - 2a_0$ é divisível por 7.*

Demonstração. Suponhamos que $a = \sum_{i=0}^{k} a_i 10^i = 7q$. Então,

$$\sum_{i=1}^{k} a_i 10^i + a_0 = 7q \text{ donde } -2a_0 = 2\sum_{i=1}^{k} a_1 10^i - 2 \times 7q.$$

Vejamos que $\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0$ é divisível por 7. Ora,

$$\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0 = \sum_{i=1}^{k} a_i 10^{i-1} + 2\sum_{i=1}^{k} a_i 10^i - 2\times 7q =$$

$$= \sum_{i=1}^{k} a_i 10^{i-1} + 2\times 10\sum_{i=1}^{k} a_i 10^{i-1} - 2\times 7q =$$

$$= (1+20)\sum_{i=1}^{k} a_i 10^{i-1} - 2\times 7q =$$

$$= 7(3\sum_{i=1}^{k} a_i 10^{i-1} - 2q),$$

o que prova que o número

$$\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0 \text{ é divisível por 7.}$$

Reciprocamente, suponhamos que $\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0 = 7p$.. Então, multiplicando ambos os membros por 10, obtemos,

$$\sum_{i=1}^{k} a_i 10^i - 20a_0 = 7\times 10p, \text{ donde}$$

$$\sum_{i=1}^{k} a_i 10^i + a_0 - (20+1)a_0 = 7\times 10p.$$

Logo,

$$a = \sum_{i=1}^{k} a_i 10^i + a_0 = 21a_0 + 7\times 10p = 7(3a_0 + 10p),$$

o que prova que

$$a = \sum_{i=0}^{k} a_i 10^i \text{ é divisível por 7.}$$

Observamos que este critério pode ser aplicado sucessivamente até obter um número que seja fácil verificar se é múltiplo de 7. Vejamos um exemplo. Consideremos o número a = 129654 e apliquemos o critério sucessivamente para averiguarmos se este número é divisível por 7. Ora, o número 129654 é divisível por 7 se, e só se, 12965–8 = 12957 é divisível por 7. Mas, 12957 é divisível por 7 se, e só se, 1295–14 = 1281 é divisível por 7. Da mesma forma, 1281 é divisível por 7 se, e só se, o mesmo acontece com 128–2 = 126. Como $126 = 7\times 18$, então 129654 é divisível por 7.

Analisemos o critério de divisibilidade por 7: um número inteiro $\sum_{i=0}^{k} a_i 10^i$ é divisível por 7 se, e só se, o mesmo acontece com o número inteiro $\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0$. A primeira pergunta que nos ocorre é: porquê o número 2 e não outro? Qual é o papel do número 2 na demonstração deste critério? Analisando, verificamos que a razão para ser o número 2 é o facto de $10\times 2+1$ ser um múltiplo de 7. Isto sugere que o critério talvez possa ser generalizável a qualquer número primo p superior a 5 se pudermos garantir a existência de um número inteiro k_p de tal modo que

$$10k_p + 1 \text{ seja um múltiplo de } p.$$

Se p é um número primo superior a 5, então p não divide 10, e, portanto, p e 10 são primos entre si. Pela identidade de Bézout, existem números inteiros x e y de tal modo que $10x + py = 1$. Então $py = 1 - 10x$. Consideremos $k_p = p - x$ e vejamos que $10(p-x)+1$ é um múltiplo de p. Ora,

$10(p-x)+1 = 10p - 10x + 1 = 10p + py = (10+y)p$.

Parece estar encontrado um valor possível para k_p. Coloca-se, no entanto, uma questão. Os coeficientes da identidade de Bézout não são determinados de modo único. Como resolver esta questão? A primeira ideia que nos ocorre é tomar para valor de k_p o resto da divisão inteira de $p - x$ por p. O resto é determinado de forma única. No entanto, se $10x + py = 1$ e $10z + pw = 1$, será que $p - x$ e $p - z$ têm o mesmo resto na divisão inteira por p? Vejamos que sim. O que queremos provar é que $p - x \equiv p - z (mod p)$. De acordo com a proposição 6, tudo o que teremos de mostrar é que $(p-x) - (p+z) = z - x$ é um múltiplo de p.

Da igualdade $10x + py = 1$ decorre que $10x = 1 - py$ e da igualdade $10z + pw = 1$ resulta que $10z = 1 - pw$. Assim, podemos afirmar que

$10(z-x) = 10z - 10x = 1 - pw - 1 + py = p(y-w)$.

A igualdade $10(z-x) = p(y-w)$ garante que p divide o produto $10(z-x)$. Assim, como p não divide 10, pela proposição 4, p divide $z - x$, ficando assim provado que $p - x$ e $p - z$ têm o mesmo resto na divisão inteira por p. A questão está resolvida: **dado um número primo p superior a 5 e números inteiros x e y de tal modo que $10x+py$ =1, tomamos para valor de k_p o resto da divisão inteira de $p–x$ por p.**

Na tabela seguinte apresentamos alguns valores de k_p .

p (nº primo)	$10x+py=1$ (Id de Bézout)	$p-x$	$p–x=pq+r$ (divisão de $p-x$ por p)	$k_p=r$
11	$10\times(-1)+11\times 1=1$	12	$11\times 1+1$	1
13	$10\times(-9)+13\times 7=1$	22	$13\times 1+9$	9
17	$10\times(-5)+17\times 3=1$	22	$17\times 1+5$	5
19	$10\times(-17)+19\times 9=1$	36	$19\times 1+17$	17
23	$10\times(-16)+23\times 7=1$	39	$23\times 1+16$	16
29	$10\times(-26)+29\times 9=1$	55	$29\times 1+26$	26
31	$10\times(-3)+31\times 1=1$	33	$31\times 1+3$	3

Proposição 10. ***Critério de divisibilidade por um número primo superior a 5.*** *Seja p um número primo superior a 5 e sejam x e y inteiros tais que $10x+py=1$. Seja k_p o resto da divisão de p–x por p. Tem-se que um número inteiro $a = a_k...a_1a_0$ é divisível por p se, e só se, o número inteiro $a_k...a_1 - k_pa_0$ é divisível por p.*

Demonstração. Suponhamos que $\sum_{i=0}^{k} a_i 10^i = np$. Então,

$$\sum_{i=1}^{k} a_i 10^i + a_0 = np, \text{ donde } -k_p a_0 = k_p \sum_{i=1}^{k} a_i 10^i - k_p np.$$

Vejamos que $\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0$ é divisível por p. Ora,

$$\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 = \sum_{i=1}^{k} a_i 10^{i-1} + k_p \sum_{i=1}^{k} a_i 10^i - k_p np =$$

$$= \sum_{i=1}^{k} a_i 10^{i-1} + k_p \times 10 \sum_{i=1}^{k} a_i 10^{i-1} - k_p np =$$

$$= (1 + k_p \times 10) \sum_{i=1}^{k} a_i 10^{i-1} - k_p np.$$

Como $1 + 10k_p$ é um múltiplo de p, então $1 + 10k_p$ é de forma mp, para algum número inteiro m. Assim,

$$\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 =$$

$$= (1 + k_p \times 10) \sum_{i=1}^{k} a_i 10^{i-1} - k_p np =$$

$$= p(m \sum_{i=1}^{k} a_i 10^{i-1} - k_p n),$$

o que prova que

$$\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 \text{ é divisível por } p.$$

Reciprocamente, suponhamos que $\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 = np$. Então, multiplicando ambos os membros por 10, obtemos

$$\sum_{i=1}^{k} a_i 10^i - 10k_p a_0 = 10np, \text{ donde}$$

$\sum_{i=1}^{k} a_i 10^i + a_0 - (10k_p + 1)a_0 = 10np$. Logo

$$\sum_{i\ 1}^{k} a_i 10^i + a_0 = (10k_p + 1)a_0 + 10np.$$

Como $10k_p + 1$ é um múltiplo de p, então $10k_p + 1 = mp$, para algum número inteiro m.
Assim, $\sum_{i=1}^{k} a_i 10^i + a_0 = (10k_p + 1)a_0 + 10np = mpa_0 + 10np = p(ma_0 + 10n)$, logo

$$a = \sum_{i=0}^{k} a_i 10^i \text{ é divisível por } p.$$

Observamos que da análise à demonstração que acabamos de apresentar se conclui que o critério de divisibilidade pode ser estendido a qualquer número inteiro que seja primo com 10.

Vejamos alguns exemplos de aplicação da proposição 10.

O número 155023 é divisível por 11. De facto, o valor de k_{11} **é 1**. Considerando a seguinte sequência de números,

155023 ▷ 115502 – 3 × 1 = 15499 ▷ 1549 – 9 × 1 = 1540 ▷ 154 – 0=154 ▷ 15 – 4 × 1 =11

Concluímos, uma vez que 11 é divisível por 11, que 155023 é divisível por 11.

O número 96993 é divisível por 13. Neste caso, o valor de k_{13} **é 1**. Considerando a seguinte sequência de números,

96993 ▷ 9699 – 3×9 = 9672 ▷ 967 – 2×9 = 949 ▷ 94 – 9×9 = 13

Concluímos, uma vez que 13 é divisível por 13, que o mesmo acontece com 96993.

O número 1381675 é divisível por 17. Basta atender a que o valor de k_{17} **é 1** e consideremos a seguinte sequência de números:

1381675 ▷ 138167 – 5×5 =138142 ▷ 13814 – 2×5 = 13804 ▷ 1380 – 4×5 = 1360 ▷ 136 – 0×5

Verificamos, como 136 = 8x17, que então 1381675 é divisível por 17.

O número 136078 é divisível por 19. De facto, o valor de k_{19} **é 17** e, considerando a seguinte sequência de números,

136078 ▷ 13607 – 8×17 = 13471 ▷ 1347– 17 = 1330 ▷ 133 = 7×19

Concluímos que 136078 é divisível por 19.

O número 209921 é divisível por 23. Notemos que o valor de k_{23} **é 16**, pelo que, considerando a seguinte sequência de números:

209921 ▷ 20992 – 1×16= 20976 ▷ 2097 – 6×16 = 2001 ▷ 200 – 1×16 =184

Dado que 184 = 8×23, então concluímos que 209921 é divisível por 23.

O número 236205 é divisível por 29. Notemos que o valor de k_{29} **é 26**, pelo que considerando a seguinte sequência de números,

$$236205 \triangleright 23620 - 5\times26 = 23490 \triangleright 2349 - 0\times26 = 2349 \triangleright 234 - 9\times26 = 0$$

concluímos que 236205 é divisível por 29.

O número 218922 é divisível por 31. Neste caso, o valor de k_{31} **é 3**. Considerando a seguinte sequência de números,

$$218922 \triangleright 21892 - 2\times3 = 21886 \triangleright 2188 - 3\times6 = 2170 \triangleright 217 = 7\times31$$

podemos afirmar que 218922 é divisível por 31.

BIBLIOGRAFIA

Niven, I., Zuckerman, H., Montgomery, H., *An Introduction to the Theory of Numbers*, 5th Edition, Wiley & Sons, 1991.

Van der Waerden, B., *Algebra*, Springer-Verlag, 2003.

SOBRE OS AUTORES

André Fonseca obteve o grau de Doutor (PhD) em Matemática, no ano de 2004, na Universidade de Leicester, Reino Unido, e efetuou um pós-doutoramento na Universidade de Chicago durante o ano 2005. Atualmente é Professor no Departamento de Matemática da Universidade Lusófona de Lisboa. Desenvolve investigação na área da Teoria de Representações.

Teresa Almada tem o grau de Doutor em Matemática pela Universidade de Lisboa desde 1994. É diretora do Departamento de Matemática da Universidade Lusófona de Lisboa. Desenvolve investigação em Teoria dos Reticulados e em Álgebras da Lógica. Desde longa data que Teresa Almada se interessa por questões relacionadas com o ensino da Matemática, a que tem dedicado algum do seu tempo.