1 Aritmética dos Inteiros

1.1 Lema da Divisão e o Algoritmo de Euclides

Recorde-se que $|a|$, o módulo ou valor absoluto de a, designa

$$|a| = \begin{cases} a & \text{se } a \in \mathbb{N} \\ -a & \text{se } a \notin \mathbb{N} \end{cases}$$

Dados $a, b, c \in \mathbb{Z}$ denotamos por

$$a \mid b :$$

a divide b ou a é um **divisor** de b, a relação definida por

$$a \mid b \iff \exists q \in \mathbb{Z} : b = aq$$

Da definição decorrem imediatamente as seguintes propriedades:

1. $a \mid b$ e $b \mid c \implies a \mid c$
2. $a \mid b$ e $a \mid c \implies a \mid (b + c)$
3. $a \mid b \implies a \mid bs, \forall s \in \mathbb{Z}$
4. $a = bq + r$, $d \mid a$, $d \mid b \implies d \mid r$
5. $a \mid b \Leftrightarrow |a| \mid |b|$

Lema 1.1 *da Divisão (inteira):*

*Dados $b \in \mathbb{N} \setminus 0$ e $a \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$ **únicos**, tais que*

$$a = bq + r \quad e \quad 0 \leq r < b.$$

Demonstração 1.2 *De facto, o resto r pode ser* definido *como o menor elemento do conjunto, obviamente não vazio,*

$$X = \{a - bx | x \in \mathbb{Z}\} \cap \mathbb{N},$$

e definir q como o inteiro que satisfaz $a - bq = r$.
Notamos em primeiro lugar que $0 \leq r$, *pela definição do conjunto* X; *e se* $r \geq b$, *ou seja, se existisse* $s \geq 0$ *tal que* $r = b + s$, *então teríamos*

$$a = bq + r = b(q + 1) + s$$

e portanto teríamos $s \in X$ *mas* $s < r$, *em contradição com o facto de* r *ser o menor elemento deste conjunto.*
Além disso, r *é o único elemento de* X *menor que* b: *se* r' *é outro elemento de* X, $r' = a - bq'$ *temos* $r' = bq + r - bq'$ *e portanto* $r' - r = b(q - q')$; *como* $r' > r$ *temos* $q - q' > 0$, *logo* $r' = r + b(q - q') \geq b(q - q') \geq b$.

Notação 1.3 *(Knuth):* q *é o maior inteiro menor ou igual a* $\frac{a}{b}$, *representado na notação introduzida por D. Knuth como* $q = \left\lfloor \frac{a}{b} \right\rfloor$.

Teorema 1.4 *(Representação dos inteiros em bases):*

Seja b *um inteiro* ≥ 2. *Então qualquer inteiro positivo* a *pode ser* representado na base b, *isto é,* a *pode ser escrito de forma única como*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_2 b^2 + r_1 b + r_0$$

com $0 \leq r_i < b; i = 1, 2, \ldots, n$.

Notação 1.5 *Escreve-se então* $a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$.

Demonstração 1.6 *A demonstração é uma simples aplicação do Lema da Divisão e do Princípio de Indução Finita (Forte): em primeiro lugar,* 1 *tem a representação, obviamente única, dada por* $r_0 = 1$.
Suponhamos como hipótese de indução que para todo o $1 \leq m < n$ *existe uma representação única na base* b*; pelo Lema da Divisão* $n = qb + r_0$ *com* $0 \leq b$*; como* $q < n$ *temos*

$$q = s_{k-1}b^{k-1} + \cdots + s_0$$

para algum $0 < k$ *e* $0 \leq s_i < b$*, unicamente determinados, pelo que*

$$n = r_k b^k + \cdots + r_1 b + r_0$$

definindo $r_i = s_{i-1}$ *para todo o* $0 < i \leq k$*. Esta representação é única: se* $n = t_j b^j + \cdots + t_1 b + t_0$*, com* $0 \leq t_i < b$*, temos em primeiro lugar que, pelo Lema da Divisão,* $t_0 = r_0$*; mas então*

$$t_j b^j + \cdots + t_1 b = r_k b^k + \cdots + r_1 b$$

e portanto

$$t_j b^{j-1} + \cdots + t_1 = r_k b^{k-1} + \cdots + r_1 = q$$

e como por hipóse de indução a representação é única para todo o $1 \leq m < n$*, temos* $j = k$ *e* $t_i = r_i$ *para todo o* i.

O raciocínio feito na demonstração indica um algoritmo para determinar a representação na base b de a:

Exemplo 1.7 *Sejam, por exemplo,* $b = 6$ *e* $a = 347$*; temos sucessivamente*

$$\begin{aligned} 347 &= 57 \times 6 + 5 = \\ &= (9 \times 6 + 3) \times 6 + 5 = 9 \times 6^2 + 3 \times 6 + 5 = \\ &= (1 \times 6 + 3) \times 6^2 + 3 \times 6 + 5 = 6^3 + 3 \times 6^2 + 3 \times 6 + 5 \end{aligned}$$

e portanto, usando a notação introduzida acima $347 = (1\,3\,3\,5)_6$.

1.2 Máximo Divisor Comum

Definição 1.8 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, diz-se que d é o* ***máximo divisor comum*** *de a e b, $d = mdc(a, b)$, se*

(i) $d > 0$; (ii) $d \mid a$ e $d \mid b$; (iii) $c \mid a$ e $c \mid b \implies c \mid d$.

Nota 1.9 *Temos obviamente*

- $\forall a \in \mathbb{N} : mdc(a, 0) = a$;
- $\forall a \in \mathbb{N} : mdc(a, 1) = 1$.

Teorema 1.10 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, existe sempre o* ***máximo divisor comum*** *de a e b.*

Este facto pode ser estabelecido teoricamente e resolvido na prática pelo

Algoritmo de Euclides para calcular $mdc(a, b)\,; a, b \in \mathbb{N},\ a \geq b$:

1 Enquanto $b > 0$,, calcular $a = qb + r$ com $0 \leq r < b$, substituir a por b e b por r;

2 Quando $b = 0$, $a = mdc(a, b)$.

Uma descrição mais detalhada, incluindo a justificação de que este procedimento pára num número finito de passos, é: Seja $r_{-1} = a$ e $r_0 = b$; definimos por recorrência

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

com $0 \leq r_{k+1} < r_k$ para $k \geq 1$.
r_k é uma sucessão estritamente decrescente de inteiros não negativos e portanto existe m tal que $r_{m+1} = 0$; isso implica que $r_m \mid r_{m-1}$ e, por um

raciocínio anaálogo ao do princípio de Indução Finita, deduzimos que $r_m \mid r_n$ para todo o $n \geq -1$: se $r_m \mid r_k$ para todo o $k \geq n$, então como

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

tem que se ter $r_m \mid r_{n-1}$.
Portanto r_m é um divisor comum de a e b; mas, por outro lado, se $c \mid a$ e $c \mid b$, deduzimos da mesma forma que $c \mid r_n$ para todo o n e portanto $c \mid r_m$. Concluímos que $r_m = mdc(a, b)$.

Exemplo 1.11 *seja* $a = r_{-1} = 5324$ *e* $b = r_0 = 1023$*; obtemos sucessivamente*

$$\begin{aligned}
r_{-1} = 5324 = \quad & 5 \times 1023 + 209 = \quad q_1 r_0 + r_1 \\
r_0 = 1023 = \quad & 4 \times 209 + 187 = \quad q_2 r_1 + r_2 \\
r_1 = 209 = \quad & 1 \times 187 + 22 = \quad q_3 r_2 + r_3 \\
r_2 = 187 = \quad & 8 \times 22 + 11 = \quad q_4 r_3 + r_4 \\
r_3 = 22 = \quad & 2 \times 11 + 0 = \quad q_5 r_4 + r_5
\end{aligned}$$

Nota 1.12 *O algoritmo de Euclides pode ser visto como um caso especial do* ***desenvolvimento em fracção contínua*** *de um número :*

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{r_1}{q_2 r_1 + r_2} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = \cdots = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_m + \cfrac{1}{q_{m+1}}}}}}$$

Corolário 1.13 *Se* $d = mdc\,(a,b)$, *existem* $x, y \in \mathbb{Z}$:

$$xa + yb = d.$$

Demonstração 1.14 *Os coeficientes* x, y *podem ser obtidos por um procedimento análogo ao da demonstração anterior; se* $d = r_m$*, isso significa que*

$$d = r_{m-2} - q_m r_{m-1};$$

mas como $r_{m-3} = q_{m-1} r_{m-2} + r_{m-1}$

$$d = r_{m-2} - q_m \left(r_{m-3} - q_{m-1} r_{m-2}\right) = -q_m r_{m-3} + \left(1 + q_m q_{m-1}\right) r_{m-2}$$

e assim por diante: se já temos

$$d = s r_n + t r_{n+1}$$

e

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

então

$$d = s r_n + t \left(r_{n-1} - q_{n+1} r_n\right) = t r_{n-1} + \left(s - t q_{n+1}\right) r_n$$

e continuando deste modo acabamos com uma equação

$$d = xa + yb.$$

Nota 1.15 *Como se verifica facilmente, o* $mdc\,(a,b)$ *é o menor inteiro positivo que se pode escrever como combinação inteira de* a *e* b*.*

O cálculo dos coeficientes x e y do corolário anterior pode ser feito, com vantagem, procedendo de outro modo: como, para todo o $n > 0$, se tem $r_n = r_{n-2} - q_n r_{n-1}$, se já tivermos

$$r_{n-2} = x_{n-2} a + y_{n-2} b, \text{ e do mesmo modo } r_{n-1} = x_{n-1} a + y_{n-1} b$$

então obtemos igualmente uma combinação

$$r_n = x_n a + y_n b = (x_{n-2} - q_n x_{n-1}) a + (y_{n-2} - q_n y_{n-1}) b.$$

Podemos portanto ir calculando os coeficientes x_k e y_k ao mesmo tempo que calculamos os sucessivos r_k e q_k e chegar ao fim da aplicação do algoritmo, obtendo como resultado final o $mdc(a,b)$ e os coeficientes x e y da equação.

A tabela seguinte descreve a aplicação do algoritmo de Euclides a $a = 2163$ e $b = 910$, com o cálculo simultâneo dos x_i e y_i que satisfazem

$$r_i = ax_i + by_i :$$

				r_i	q_i	x_i	y_i
				2163		1	0
				910		0	1
$2163 =$	2×910	$+$	343	343	2	1	-2
$910 =$	2×343	$+$	224	224	2	-2	5
$343 =$	1×224	$+$	119	119	1	3	-7
$224 =$	1×119	$+$	105	105	1	-5	12
$119 =$	1×105	$+$	14	14	1	8	-19
$105 =$	7×14	$+$	7	7	7	-61	145
$14 =$	2×7	$+$	0				

Nota 1.16 *Estes cálculos podem também ser representados através do produto de matrizes: a equação acima pode escrever-se como*

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} x_{n-2} & y_{n-2} \\ x_{n-1} & y_{n-1} \end{pmatrix} = \begin{pmatrix} x_{n-1} & y_{n-1} \\ x_n & y_n \end{pmatrix};$$

com a condição inicial

$$r_{-1} = 1 \times a + 0 \times b = x_{-1}a + y_{-1}b$$

e

$$r_0 = 0 \times a + 1 \times b = x_0 a + y_0 b$$

temos que os coeficientes x e y pretendidos são os elementos da segunda linha da matriz

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{m-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

Definição 1.17 *Dizemos que a e b são **primos entre si** se $mdc(a,b) = 1$.*

Deduz-se portanto do resultado anterior que a e b são primos entre si se e só se existem inteiros x e y tais que

$$xa + yb = 1$$

Teorema 1.18 *Se* $a, b, c \in \mathbb{Z}$,

$$mdc\,(a, c) = 1 \ e\ c \mid ab \implies c \mid b.$$

Demonstração 1.19 *De facto, como existem inteiros* x, y *tais que* $ax+cy = 1$*, temos*

$$abx + cby = b$$

e como c *divide as duas parcelas da esquerda tem também que dividir* b*.*

Proposição 1.20 *Se* $mdc(a, b) = 1$

$$a|c \ e\ b|c \implies (ab)|c$$

Demonstração 1.21 *Sabemos que existem inteiros* u, v *tais que* $au+bv = 1$*; por outro lado,* $c = ax = by$*. Então,*

$$byu = cu = aux = (1 - bv)x$$

e portanto

$$x = b(yu + vx) \ e\ c = ab(yu + vx)$$

Mais geralmente,

Proposição 1.22 *Se $a_1, a_2, \cdots, a_k$ são primos dois a dois, ou seja*

$$mdc(a_i, a_j) = 1 \qquad \forall\, i \neq j$$

então

$$a_i | c \quad \forall\, 1 \leq i \leq k \implies (\prod_{i=1}^{k} a_i) | c$$

Demonstração 1.23 *Usamos indução: o caso $k = 2$ é o da proposição anterior; suponhamos então que a implicação é verdadeira para $k - 1$; então dados inteiros $a_1, a_2, \cdots, a_k$ nas condições do enunciado, temos que os $k - 1$ inteiros $a_1, a_2, \cdots, a_{k-1}$ também satisfazem essas condições e portanto, pela hipótese de indução, $(a_1 a_2 \cdots a_{k-1}) | c$; mas os dois inteiros $a_1 a_2 \cdots a_{k-1}$ e a_k são primos entre si e ambos dividem c; estamos portanto nas condições do caso $k = 2$ e podemos concluir, pela proposição anterior, que*

$$(a_1 \cdots a_k) | c$$

Corolário 1.24 *Se $d = mdc\,(a, b)$, a equação*

$$ax + by = c$$

tem soluções $x, y \in \mathbb{Z}$ se e só se $d \mid c$. Mais, se (x_0, y_0) é uma solução desta equação, o conjunto de todas as soluções é constituído pelos pares de inteiros (x, y) da forma

$$x = x_0 + k\frac{b}{d} \quad ; \quad y = y_0 - k\frac{a}{d} \quad ; \quad k \in \mathbb{Z}.$$

Demonstração 1.25 *A primeira parte do resultado é óbvia: se $d = as + bt$ e $c = dm$, então $c = a(ms) + b(mt)$; por outro lado, se $c = ax + by$, então $d \mid c$.*

Dada uma solução $c = ax_0 + by_0$, é evidente que, para qualquer $k \in \mathbb{Z}$, se tem também

$$c = a(x_0 + k\frac{b}{d}) + b(y_0 - k\frac{a}{d})$$

Suponhamos que $c = az + bw$; então

$$ax_0 + by_0 = az + bw \Leftrightarrow a(x_0 - z) = b(w - y_0) \Leftrightarrow \frac{a}{d}(x_0 - z) = \frac{b}{d}(w - y_0)$$

Mas, como se verifica imediatamente a partir da definição de máximo divisor comum, se $mdc(a, b) = d$ então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$; logo, se $\frac{a}{d}$ divide o produto $\frac{b}{d}(w - y_0)$, pelo Teorema anterior tem que dividir $w - y_0$, ou seja, existe um inteiro k tal que

$$w = y_0 + k\frac{a}{d}.$$

Substituindo na equação anterior,

$$\frac{a}{d}(x_0 - z) = \frac{b}{d}(w - y_0) = \frac{b}{d}k\frac{a}{d}$$

e portanto

$$z = x_0 - k\frac{b}{d}$$

como queríamos provar.

Corolário 1.26 *Se $a, b_1, b_2, \cdots, b_n$ são inteiros tais que*

$$mdc(a, b_i) = 1 \ \forall i$$

então $mdc(a, b) = 1$, onde $b = \prod_{i=1}^{n} b_i$.

Demonstração 1.27 *Existem inteiros x_i e y_i (com $1 \leq i \leq n$) tais que*

$$ax_i + b_i y_i = 1 \ \forall i$$

Multiplicando estas igualdades termo a termo obtemos

$$aX + bY = 1$$

onde $Y = y_1 y_2 \cdots y_n$.

O conceito de máximo divisor comum generaliza-se a mais de dois inteiros e prova-se (ver exercícios) que

$$mdc(a_1, a_2, \cdots, a_n) = mdc(mdc(a_1, a_2, \cdots, a_{n-1}), a_n)$$

e a partir desta igualdade conclui-se que se $d = mdc(a_1, a_2, \cdots, a_n)$, então existem inteiros x_i tais que

$$d = \sum_{i=1}^{n} x_i a_i$$

e que um inteiro c tem uma representação desta forma se e só se $d \mid c$.

1.3 Números primos e o Teorema Fundamental da Aritmética

Definição 1.28 *Um inteiro* $p > 1$ *diz-se* ***primo*** *se os seus únicos divisores positivos são* 1 *e o próprio* p.

Deduz-se facilmente que qualquer inteiro $n > 1$ é divisível por algum primo. Além disso, o último corolário da secção anterior tem como consequência a seguinte

Proposição 1.29 *Dados* $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ *e* p *primo,*

$$p \mid a_1 a_2 \ldots a_n \implies \exists i : p \mid a_i.$$

Teorema 1.30 *O conjunto dos números primos é infinito.*

Demonstração 1.31 *Seja de facto $p_1, p_2, \cdots, p_m$ um qualquer conjunto finito de primos (por exemplo, os primeiros m primos); o número*

$$N = p_1 p_2 \cdots p_m + 1$$

ou é primo ou tem que ter um factor primo p; se $p \in \{p_1, p_2, \cdots, p_m\}$ então p dividiria o produto $p_1 p_2 \cdots p_m$ e então teria que dividir 1, o que é impossível. Em qualquer caso verificamos que N tem um factor primo diferente de qualquer um dos p_i.

Teorema 1.32 *Teorema Fundamental da Aritmética*

Para cada inteiro $n > 1$, existem primos $p_1, p_2, \ldots, p_r$, tais que

$$n = p_1 p_2 \ldots p_r$$

e essa factorização é única a menos de permutação dos factores.

Demonstração 1.33 *A demonstração deste Teorema pode ser feita por uma aplicação do Princípio de Indução Finita (Forte) e das propriedades deduzidas anteriormente:*
$n = 1$ é o produto do conjunto vazio de primos (tal como a soma de um conjunto vazio de números é igual a zero...) e $n = 2$ é primo; dado $n > 2$, suponhamos, como hipótese de indução, que todo o natural menor que n tem uma factorização única em factores primos.
Se n é primo tem evidentemente uma factorização única; caso contrário, podemos factorizar $n = n_1 n_2$ com $1 < n_1, n_2 < n$; por hipótese de indução, n_1 e n_2 têm ambos factorização única

$$n_1 = p_1 p_2 \cdots p_m, \qquad n_2 = p'_1 p'_2 \cdots p'_l$$

e portanto n tem claramente uma factorização em factores primos

$$n = p_1 p_2 \cdots p_m p'_1 p'_2 \cdots p'_l$$

Para vermos que essa factorização é única notamos que se

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

são duas factorizações em factores primos, então p_1, por ser primo, divide forçosamente um dos factores q_i, que podemos supor, renumerando os factores, ser q_1; mas como este é primo, os seus únicos divisores (positivos) são 1 e q_1 e portanto $p_1 = q_1$.
Cancelando esse factor obtemos

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_t$$

e como $\dfrac{n}{p_1}$ é menor que n, tem factorização única em factores primos, ou seja $s = t$ e os q_i coincidem com os p_i, a menos de uma permutação dos factores. Mas então o mesmo acontece com as factorizações de n.

Se designarmos por P_k a sucessão crescente de todos os números primos, $P_1 = 2, P_2 = 3, \cdots$, podemos escrever a factorização de n como

$$n = \prod_{k \geq 1} P_k^{i_k}$$

onde os expoentes i_k satisfazem a condição de serem 0 excepto para um número finito de casos, com a convenção de que o produto de um número infinito de 1 é 1 (à semelhança do que se passa com a soma de um número infinito de termos iguais a zero). Qualquer sucessão i_k que satisfaça as condições

$$i_k \geq 0 \forall k \geq 1, \qquad \exists m : i_k = 0 \forall k > m$$

corresponde a uma factorização de um natural positivo e temos portanto uma bijecção entre o conjunto dos naturais positivos e o conjunto das sucessões

que satisfazem aquelas condições, e o produto de dois naturais corresponde, por essa bijecção, à soma das sucessões respectivas: se

$$n = \prod_{k\geq 1} P_k^{i_k}, \qquad m = \prod_{k\geq 1} P_k^{j_k}$$

então

$$nm = \prod_{k\geq 1} P_k^{i_k+j_k}$$

A relação de divisibilidade $n \mid m$ traduz-se em $i_k \leq j_k$, $\forall k$ e, do mesmo modo,

$$mdc(n,m) = \prod_{k\geq 1} P_k^{\min\{i_k,j_k\}}, \qquad mmc(n,m) = \prod_{k\geq 1} P_k^{\max\{i_k,j_k\}}$$

onde $mmc(n,m)$ designa o menor múltiplo comum dos dois naturais n e m.

Nota 1.34 *O Teorema Fundamental da Aritmética pode parecer evidente, de tal modo as propriedades dos números inteiros estão enraizadas na nossa mente. O seu alcance, e a sua dependencia da validade do Lema da Divisão, são melhor compreendidos se estudarmos a aritmética de outros conjuntos. Para isso é conveniente reformular alguns dos conceitos apresentados de forma ligeiramente diferente.*
Designemos por ***unidades*** *de $\mathbb{Z}$ os inteiros invertíveis,ou seja aqueles inteiros x para os quais existe algum inteiro y tal que $xy = 1$. Obviamente, as únicas unidades de $\mathbb{Z}$ são 1 e -1. Podemos então definir* ***número indecomponível*** *da seguinte forma: x é indecomponível se $x = yz$ implica que ou y ou z seja unidade.*
É claro que em $\mathbb{Z}$ um número é indecomponível exactamente se for primo, e como deduzimos atrás, esses inteiros podem também ser caracterizados pela propriedade

$$p \text{ é primo } \Leftrightarrow (p \mid ab \implies p \mid a \vee p \mid b).$$

donde se seguem todos os resultados já deduzidos sobre os inteiros, incluindo o Teorema Fundamental da Aritmética.
Mas consideremos agora um outro exemplo de conjunto de números,

$$C = \{a + b\sqrt{10}\ a, b \in \mathbb{Z}\}.$$

As operações de soma e multiplicação estão bem definidas neste conjunto, isto é, a soma e produto de dois números de C pertence ainda a C, e têm as mesmas propriedades elementares já descritas para $\mathbb{Z}$. Em particular, podemos definir a relação de divisibilidade e definir unidade e número indecomponível da mesma forma que fizemos para $\mathbb{Z}$. Note-se que C tem

muito mais unidades do que $\mathbb{Z}$*, por exemplo* $3+\sqrt{10}$ *é unidade, com inverso* $-3+\sqrt{10}$*, e portanto também* $(3+\sqrt{10})^k$ *é unidade, para qualquer* $k \geq 1$*. Temos*

$$2 \times 3 = (2+\sqrt{10})(-2+\sqrt{10}),$$

como se verifica facilmente. Mas, como se pode verificar (embora menos facilmente) directamente a partir das definições, todos os números $2, 3, 2+\sqrt{10}, -2+\sqrt{10}$ *são indecomponíveis. Portanto em* C *não vale o Teorema Fundamental da Aritmética, e um número indecomponível pode dividir o produto de dois números sem dividir nenhum deles.*