UNIVERSIDADE DO MINHO
DEPARTAMENTO DE MATEMÁTICA

Matemática Discreta

Capítulo - Teoria de Números — Assis Azevedo

1. DIVISIBILIDADE

Definição 1.1. *Se $a, b \in \mathbb{Z}$, dizemos que a* **divide** *b e escrevemos $a \big| b$ se existir $x \in \mathbb{Z}$ tal que $b = ax$. Nestas condições dizemos também que a é um* **divisor** *de b ou que b é um* **múltiplo** *de a.*

Escreveremos $a \nmid b$ se a não dividir b.

Vejamos algumas consequências imediatas desta definição.

Teorema 1.2. *Sejam $a, b, c \in \mathbb{Z}$.*

a) $a \big| 0$, $1 \big| a$, $a \big| a$ *e* $-a \big| a$.

b) *Se* $a \big| b$ *então* $a \big| bc$.

c) *Se* $a \big| b$ *e* $b \big| c$ *então* $a \big| c$.

d) *Se* $a \big| b$ *e* $a \big| c$ *então* $a \big| \alpha b + \beta c$, *quaisquer que sejam os inteiros* α *e* β.

e) a *e* $-a$ *têm os mesmos divisores.*

f) *Se* $a \big| b$ *e* $b \big| a$ *então* $a = b$ *ou* $a = -b$.

g) *Se* $a \big| b$ *então* $ac \big| bc$.

h) *Se* $ac \big| bc$ *e* $c \neq 0$ *então* $a \big| b$.

Demonstração. (sucinta)

a) Note-se que $0 = 0\,a$, $a = 1\,a$ e $-a = (-1)\,a$.

b) Se $x \in \mathbb{Z}$ é tal que $b = ax$ então $bc = a(xc)$.

c) Se $x, y \in \mathbb{Z}$ são tais que $b = ax$ e $c = by$ então $c = a(xy)$.

d) Se $x, y \in \mathbb{Z}$ são tais que $b = ax$ e $c = ay$ então $\alpha b + \beta c = a\,(\alpha x + \beta y)$.

e) Basta usar a) e c).

f) Se $x, y \in \mathbb{Z}$ são tais que $b = ax$ e $a = by$ então $a = a(xy)$. Daqui resulta que $a = 0$ ou $xy = 1$. Se $a = 0$ então $b = ax = 0$. Se $xy = 1$ então $x = y = 1$ ou $x = y = -1$ e portanto $a = b$ ou $a = -b$.

g) Se $x \in \mathbb{Z}$ é tal que $b = ax$ então $bc = acx$.

h) Se $x \in \mathbb{Z}$ é tal que $bc = acx$ então, aplicando a lei do corte, $b = ax$.

$\square$

A alínea d) pode ser generalizada do seguinte modo: se a divide $b_1, b_2, \ldots, b_k$ então a divide $\sum_{i=1}^{k} \alpha_i b_i$ quaisquer que sejam os inteiros $\alpha_1, \alpha_2, \ldots, \alpha_k$.

Estamos agora em condições de enunciar e demonstrar o algoritmo da divisão que está na base do chamado algoritmo de Euclides que será introduzido na secção seguinte.

Teorema 1.3 (Algoritmo da divisão)**.** *Dados inteiros a, b, com $a \neq 0$ existem inteiros únicos q e r tais que*

$$b = aq + r, \quad 0 \leq r < |a|.$$

Demonstração. Vamos começar por mostrar a existência de q e r nas condições referidas.

Para simplificar a escrita vamos analisar várias situações possíveis:

- $\boxed{b = 0}$. Neste caso $b = 0\,a + 0$.
- $\boxed{a > 0 \text{ e } b > 0}$ (**caso relevante**). Consideremos $S = \{x \in \mathbb{Z} : a\,x > b\}$. Note-se que S é um subconjunto de $\mathbb{N}$ que não vazio pois é igual a $\mathbb{N} \cap \left]\frac{b}{a}, +\infty\right[$. Pelo princípio da boa ordenação seja x_0 o primeiro elemento de S. Nestas condições $a(x_0 - 1) \leq b < ax_0$ e portanto

  $$b = aq + r, \quad \text{se } q = x_0 - 1 \text{ e } r = b - a(x_0 - 1)$$

  Para concluir basta notar que $0 \leq b - a(x_0 - 1) < ax_0 - a(x_0 - 1) = a$. No fundo q é o maior inteiro tal que aq é menor ou igual a b.
- $\boxed{a < 0 \text{ e } b > 0}$. Pelo caso anterior existem $q_1, r_1 \in \mathbb{Z}$ tais que $b = (-a)q_1 + r_1$ e $0 \leq r_1 < -a$. Deste modo $b = a(-q_1) + r_1$ e $0 \leq r_1 < |a|$.
- $\boxed{b < 0}$. Pelos casos anteriores sabemos que existem $q^*, r^* \in \mathbb{Z}$ tais que $-b = aq^* + r^*$ e $0 \leq r^* < |a|$. Deste modo

  $$b = a(-q^*) - r^* \quad = \quad \begin{cases} a(-q^* - 1) + (a - r^*) & \text{se } a > 0. \\ a(-q^* + 1) + (-a - r^*) & \text{se } a < 0 \end{cases}$$

  Note-se que $0 \leq (a - r^*) < |a|$, se $a > 0$ e $0 < (-a - r^*) < |a|$ se $a < 0$.

Vejamos agora a unicidade dos inteiros q e r. Suponhamos que $b = aq + r$ e $b = aq^* + r^*$ com $0 \leq r \leq |a|$ e $0 \leq r^* < |a|$. Nestas condições

$$a(q - q^*) \quad = \quad (r^* - r).$$

Note-se que $r^* - r$ pertence ao intervalo aberto $\big] - |a|,\ |a|\big[$. Como o único múltiplo de a que pertence a este intervalo é o 0 concluímos que $a(q - q^*) = r^* - r = 0$ e portanto $q = q^*$ (pois $a \neq 0$) e $r = r^*$. $\square$

A demonstração deste teorema pode ter sido feita usando um argumento de indução uma vez que, se $b = aq + r$ com $0 \leq r < |a|$ então

$$b+1 = \begin{cases} aq + (r+1) & \text{se } r+1 < a \\ a(q+1) + 0 & \text{se } r+1 = a \\ a(q-1) + 0 & \text{se } r+1 = -a \end{cases} \qquad b-1 = \begin{cases} aq + (r-1) & \text{se } r+1 < a \\ a(q-1) + 0 & \text{se } r+1 = a \\ a(q+1) + 0 & \text{se } r+1 = -a \end{cases}$$

Deste modo escrevemos $b+1$ e $b-1$ nas condições pretendidas se soubermos escrever b nas mesmas condições!!

Nas condições do teorema chamaremos **quociente** e **resto da divisão** de b por a aos inteiros q e r respectivamente. É claro que, a divide b se e só se o resto da divisão de b por a é igual a 0.

Vejamos um exemplo. Sabendo que $3333333 = 5555 \times 600 + 333$, qual o resto da divisão de 3333333 por -5555 ou de -3333333 por 5555 ou -5555? Utilizando o argumento usado acima

$$\begin{aligned} 3333333 &= \underbrace{(-5555)}_{\text{divisor}} \times (-600) + \underbrace{333}_{\text{resto}} \\ -3333333 &= 5555 \times (-600) - 333 = 5555 \times (-601) + (5555 - 333) = \underbrace{5555}_{\text{divisor}} \times (-601) + \underbrace{5222}_{\text{resto}} \\ -3333333 &= = \underbrace{(-5555)}_{\text{divisor}} \times (601) + \underbrace{5222}_{\text{resto}}. \end{aligned}$$

2. Máximo divisor comum

Note-se que, se $a \in \mathbb{Z} \setminus \{0\}$ então os divisores de a pertencem ao intervalo cujos extremos são a e $-a$. Em particular existe um número finito de divisores de a, sendo um deles o número 1. Tem então sentido a seguinte definição.

Definição 2.1. *Sejam a, b inteiros não ambos nulos. Ao maior inteiro que divide a e b chama-se* **máximo divisor comum** *de a e b e denota-se por (a, b) ou por mdc(a, b).*

Se $(a, b) = 1$ diz-se que a e b são primos entre si.

Escreverei mdc para simplificar máximo divisor comum.

Recorde-se que qualquer inteiro é um divisor de 0. Esta é a razão porque na definição de mdc, foi colocada a restrição de a e b não serem ambos nulos.

A seguinte proposição agrupa algumas consequências simples da definição de mdc.

Proposição 2.2. *Se a e b são inteiros não ambos nulos, então:*

a) $(a,b) = (b,a) = (-a,b) = (a,-b) = (-a,-b)$*;*

b) $(a,b) \geq 1$*;*

c) se a divide b então $(a,b) = |a|$*;*

d) $(a,a) = (a,0) = |a|$ *se* $a \neq 0$*;*

e) $(a,1) = 1$*;*

f) se $b = aq + r$ *então* $(a,b) = (a,r)$*.*

Demonstração. (sucinta)

a) Basta notar que os divisores de um inteiro e do seu simétrico são os mesmos.

b) 1 é divisor de a e de b.

c) $|a|$ é o maior divisor de a e divide b.

d) e e) são casos particulares de c).

f) Vamos ver que se d é um inteiro então d divide a e b se e só se d dividir r e a. De facto, se d divide a e b então divide r porque $r = a - bq$. Inversamente, se d divide r e a então também divide b, porque $b = aq + r$. Em ambos os argumentos usamos a alínea d) do Teorema 1.2. □

Nota 2.3. *Na última alínea da proposição anterior (que será usada constantemente) não se está a supor que r seja o resto da divisão de a por b.*

Como aplicação destes resultados podemos calcular o máximo divisor comum de dois quaisquer inteiros. Para isso basta aplicar algumas vezes o algoritmo da divisão e a proposição anterior (especialmente a última alínea). Costuma-se chamar **algoritmo de Euclides** a este método.

Por exemplo, para calcular $(218, 486)$ obtemos,

$$\begin{array}{rcll}
(218,486) & = & (218,50) & \text{porque } 486 = 2 \times 218 + 50 \\
& = & (50,18) & \text{porque } 218 = 4 \times 50 + 18 \\
& = & (18,14) & \text{porque } 50 = 2 \times 18 + 14 \\
& = & (14,4) & \text{porque } 18 = 1 \times 14 + 4 \\
& = & (4,2) & \text{porque } 14 = 3 \times 4 + 2 \\
& = & (2,0) & \text{porque } 4 = 2 \times 2 + 0 \\
& = & 2 & \text{pela Proposição 2.2, alínea e)}
\end{array}$$

Note-se que, se calcularmos o máximo divisor de a e b aplicando este método, a sucessão dos restos que surge é estritamente decrescente até tomar o valor 0. Nesse momento podemos concluir que $(a,b) = (r,0) = r$ em que r é o último resto diferente de 0 que apareceu nas nossas contas.

É claro que na prática não necessitamos de fazer estas contas até ao fim. Por exemplo, no caso anterior é obvio que $(14,4) = 2$, pois os divisores positivos de 4 são 1, 2 e 4 e o 4 não divide 14. Ou então é claro que $(4,2) = 2$ porque 2 divide 4.

Vejamos outro exemplo,

$$\begin{array}{rcll}
(71\,877, 24\,947) & = & (24\,947, 21\,983) & \text{porque } 71\,877 = 2 \times 24\,947 + 21\,983 \\
& = & (21\,983, 2\,964) & \text{porque } 24\,947 = 21\,983 + 2\,964 \\
& = & (2\,964, 1\,235) & \text{porque } 21\,983 = 7 \times 2\,964 + 1\,235 \\
& = & (1\,235, 494) & \text{porque } 2\,964 = 2 \times 1\,235 + 494 \\
& = & (494, 247) & \text{porque } 1\,235 = 2 \times 494 + 247 \\
& = & (247, 0) & \text{porque } 494 = 2 \times 247 \\
& = & 247. &
\end{array}$$

Note-se também que cada um dos restos que aparecem se pode escrever como combinação linear (com coeficientes inteiros) dos restos anteriores e de a e b. Em particular o máximo divisor comum de a e b escreve-se como combinação linear (com coeficientes inteiros) de a e b. Os cálculos são os seguintes (usando as igualdades acima por ordem inversa). Dentro das "caixas" estão os restos e os números "originais" estão sublinhados!

$$\begin{array}{rcl}
247 & = & \boxed{1\,235} - 2 \times \boxed{494} \\
& = & \left(\boxed{21\,983} - 7 \times \boxed{2\,964}\right) - 2 \times \left(\boxed{2\,964} - 2 \times \boxed{1\,235}\right) \\
& = & \boxed{21\,983} - 9 \times \boxed{2\,964} + 4 \times \boxed{1\,235} \\
& = & (\underline{71\,877} - 2 \times \underline{24\,947}) - 9 \times \left(\underline{24\,947} - \boxed{21\,983}\right) + 4 \times \left(\boxed{21\,983} - 7 \times \boxed{2\,964}\right) \\
& = & \underline{71\,877} - 11 \times \underline{24\,947} + 13 \times \boxed{21\,983} - 28 \times \boxed{2\,964} \\
& = & \underline{71\,877} - 11 \times \underline{24\,947} + 13 \times (\underline{71\,877} - 2 \times \underline{24\,947}) - 28 \times \left(\underline{24\,947} - \boxed{21\,983}\right) \\
& = & 14 \times \underline{71\,877} - 65 \times \underline{24\,947} + 28 \times \boxed{21\,983} \\
& = & 14 \times \underline{71\,877} - 65 \times \underline{24\,947} + 28 \times (\underline{71\,877} - 2 \times \underline{24\,947}) \\
& = & 42 \times \underline{71\,877} - 121 \times \underline{24\,947}
\end{array}$$

Formalmente temos o seguinte teorema.

Teorema 2.4. *Se a e b são inteiros, não ambos nulos e $d = (a,b)$ então existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.*

Demonstração. Vamos fazer a demonstração por indução sobre $k = \min\{|b|, |a|\}$ que pertence a $\mathbb{N}_0$. Se $k = 0$ então a ou b é igual a 0. Se $a = 0$ (o outro caso é análogo) então, pela Proposição 2.2, $(a,b) = |b|$ e, portanto, $(a,b) = 0\,a + 1\,b$, se $b > 0$ e $(a,b) = 0\,a + (-1)\,b$, se $b < 0$.

Vejamos a demonstração do passo de indução. Podemos supor que $|b| \geq |a| > 0$. Sejam q e r tais que $b = aq + r$ com $0 \leq r < |a|$. Em particular $\min\{|b|, |a|\} > k = \min\{r, |a|\}$.

Usando a hipótese de indução e a igualdade $(a,b)=(a,r)$ sabemos que que existem $x,y\in\mathbb{Z}$ tais que $ax+ry=d$. Daqui resulta que $a(x-qy)+by=d$. □

Na prática o que se faz é usar o algoritmo de Euclides, mas agora, de baixo para cima.

Vejamos algumas consequências deste último teorema.

Proposição 2.5. *Se $a,b,c\in\mathbb{Z}$ são tais que $a\big|bc$ e $(a,b)=1$ então $a\big|c$.*

Demonstração. Sejam, usando o teorema anterior $x,y\in\mathbb{Z}$ tais que $ax+by=1$. Multiplicando por c obtemos $acx+bcy=c$. Como a divide acx e bcy (pois $a|\,bc$ por hipótese), concluímos que a divide a soma destes dois números que é igual a c. □

Chama-se a atenção que a condição $(a,b)=1$ é necessária como se pode ver se escolhermos $a=4$ e $b=c=2$.

Teorema 2.6. *Se a,b são inteiros não ambos nulos e $m\in\mathbb{N}$ então*

a) $(ma,mb)=m(a,b)$;

b) $\left(\frac{a}{d},\frac{b}{d}\right)=\frac{1}{d}(a,b)$, *se d divide a e b;*

c) $\left(\frac{a}{d},\frac{b}{d}\right)=1$, *se $d=(a,b)$.*

Demonstração. a) Sejam $d=(a,b)$, $d^*=(ma,mb)$. Como d divide a e b então dm divide am e bm. Pela definição de máximo divisor comum concluímos que $dm\le d^*$. Por outro lado, usando o Teorema 2.4, consideremos $x,y\in\mathbb{Z}$ tais que $ax+by=d$. Daqui obtemos $amx+bmy=dm$. Como d^* divide amx e bmy podemos concluir que d^* divide $amx+bmy$ que é igual a dm. Em particular, uma vez que se tratam de números positivos, $d^*\le dm$.

b) Basta notar que

$$(a,b) \quad = \quad \left(d\,\frac{a}{d},d\,\frac{b}{d}\right) \quad = \quad d\left(\frac{a}{d},\frac{b}{d}\right) \qquad \text{pela alínea a)}$$

c) É apenas um caso particular de b). □

Teorema 2.7. *Se a,b,m são inteiros não nulos então (ab,m) divide o produto de (a,m) por (b,m). Em particular, se a e b são primos com m então ab também é primo com m.*

Demonstração. Sejam $d=(a,m)$, $d'=(b,m)$ e $D=(ab,m)$. Consideremos $x,y,x',y'\in\mathbb{Z}$ tais que $ax+my=d$ e $bx'+my'=d'$. Multiplicando obtemos

$$ab(xx')+m(axy'+ybx'+ymy')=dd'.$$

Como D divide ab e m então divide $ab(xx')+m(axy'+ybx'+ymy')$ que é igual a dd'.

Se a e b forem primos com m então $d=d'=1$ e portanto $D=1$ pois divide dd'. □

Note-se que, em geral $(ab, m) \neq (a, m) \times (b, m)$, como se pode ver considerando, por exemplo, $a = b = m > 1$.

O seguinte resultado diz-nos que o máximo divisor comum de dois números é não só o **maior** dos divisores comuns mas é ele mesmo um **múltiplo** de todos os divisores comuns desses números. Por exemplo, os divisores comuns de 12 e 30 são $1, 2, 3, 6$ e os seus simétricos e o maior deles todos (6) é múltiplo de todos os outros.

Teorema 2.8. *Um inteiro é um divisor de dois inteiros não ambos nulos se e só se for um divisor do máximo divisor comum desses números. Dito de outro modo, se $a, b, k \in \mathbb{Z}$, com a e b não ambos nulos, então*

$$\begin{cases} k \big| a \\ k \big| b \end{cases} \iff k \big| \, (a, b).$$

Demonstração. Se k divide (a, b) então k divide a e b porque (a, b) divide a e b. Inversamente, se k divide a e b e $x, y \in \mathbb{Z}$ são tais que $(a, b) = ax + by$ então k divide (a, b) pois (a, b) é a soma de dois múltiplos de k. □

Este resultado será usado **sistematicamente**. Para além disso diz-nos como definir máximo divisor comum em contextos mais gerais.

Definição 2.9. *Sejam $a, b \in \mathbb{Z}$. Chama-se* **mínimo múltiplo comum** *de a e b (denotado por $[a, b]$ ou por $mmc(a, b)$) ao menor múltiplo positivo de a e de b.*

Note-se que, se $a, b \in \mathbb{Z}$ então $|ab|$ é um múltiplo positivo de a e de b e portanto a definição dada acima tem sentido. Muitos dos resultados que mostrámos para o mdc têm um análogo para o mmc. Em particular, aqueles da Proposição 2.2 e do Teorema 2.6: se $a, b \in \mathbb{Z}$,

- $[a, 0] = 0$;
- $[a, b] = [b, a] = [-a, b] = [a, -b] = [-a, -b]$;
- se a divide b então $[a, b] = |b|$;
- $[a, a] = [a, 1] = |a|$;
- $[ma, mb] = m[a, b]$, se $m \in \mathbb{N}$;
- $\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{1}{d}\,[a, b]$, se d divide a e b.

Uma relação entre o mdc e o mmc é dada pelo seguinte resultado.

Proposição 2.10. *Se $a, b \in \mathbb{Z} \setminus \{0\}$ então $(a, b)[a, b] = |ab|$. Em particular $[a, b]$ divide ab.*

Demonstração. Atendendo ao que foi dito acima podemos considerar que $a, b \in \mathbb{N}$. Sejam $d = (a, b)$ e $D = [a, b]$. Note-se que $\frac{ab}{d}$ é múltiplo de a e de b pois

$$\frac{ab}{d} = a \cdot \frac{b}{d} = \frac{a}{d} \cdot b, \quad \text{e} \quad \frac{b}{d}, \frac{a}{d} \in \mathbb{N}.$$

Por definição de mmc podemos concluir que $D \leq \frac{ab}{d}$ ou seja, que $dD \leq ab$. Usando o Teorema 2.4, sejam $x, y \in \mathbb{Z}$ tais que $ax + by = d$. Deste modo $aDx + bDy = dD$. Como ab divide aDx (porque b divide D) e bDy (porque a divide D) podemos concluir que ab também divide $aDx + bDy$ que é igual a dD. Obtemos assim $dD = ab$. □

Temos agora um resultado análogo ao do Teorema 2.8.

Teorema 2.11. *Um inteiro é um múltiplo de dois inteiros se e só se for um múltiplo do mínimo múltiplo comum desses números. Dito de outro modo, Se $a, b, k \in \mathbb{Z}$ então*

$$\begin{cases} a \big| k \\ b \big| k \end{cases} \Leftrightarrow \quad [a, b] \big| k.$$

Demonstração. Basta considerar o caso em que a e b não são nulos pois caso contrário k terá de ser zero e o resultado é trivial. Suponhamos que a e b dividem k. Como a e b também dividem $[a, b]$, podemos concluir, usando o Teorema 2.8, que a e b dividem $(k, [a, b])$. Mas então, por definição de mmc, $[a, b] \leq (k, [a, b])$. Mas é obvio que $(k, [a, b]) \leq [a, b]$ pois $(k, [a, b])$ é um divisor de $[a, b]$.

A implicação contrária é imediata! □

Nota 2.12. *Podemos definir o máximo divisor comum e mínimo múltiplo comum de vários inteiros desde, no primeiro caso, pelo menos um desses inteiros não seja nulo. Notando que, temos as igualdades*

$$(a_1, a_2, \ldots, a_n) = (a_1, (a_2, \ldots, a_n)), \quad [a_1, a_2, \ldots, a_n] = [a_1, [a_2, \ldots, a_n]]$$

sempre que os máximos divisores comuns envolvidos tenham sentido, podemos facilmente generalizar os resultados já demonstrados.

Em particular, se $a_1, a_2, \ldots, a_d$ são inteiros não todos nulos e $d = (a_1, a_2, \ldots, a_n)$ então

$$\exists\, x_1, x_2, \ldots, x_n \in \mathbb{Z} : \quad a_1x_1 + a_2x_2 + \cdots a_nx_n = d.$$

Isto acontece porque, usando a igualdade acima, $(a_1, (a_2, \ldots, a_n))$ escreve-se como combinação linear de a_1 e de $(a_2, \ldots, a_n)$. Para concluir basta usar um argumento de indução.

Como exemplo vamos encontrar $x, y, z \in \mathbb{Z}$ tal que $6x + 10y + 15z = (6, 10, 15)$.

Começamos por notar que $(6, 10, 15) = ((6, 10), 15)$.

- escrevemos $(6, 10)$ na forma $6\,x_1 + 10\,y_1$. Obtemos $(6, 10) = 2$, $x_1 = 2$ e $y_1 = -1$;
- escrevemos $((6, 10), 15)$ na forma $2x_2 + 15\,y_2$ (pois $(6, 10) = 2$). Feitas as contas obtemos $(2, 15) = 1$, $x_2 = -7$ e $y_2 = 1$.

Concluímos assim que

$$(6,10,15)=(2,15)=1=2x_2+15y_2=(6x_1+10y_1)x_2+15y_2=6x_1x_2+10y_1x_2+15y_2$$

e portanto $6x+10y+15z=(6,10,15)$ em que $x=x_1x_2=-14$, $y=y_1x_2=7$ e $z=1$.

Os teoremas 2.8 e 2.11 podem ser generalizado do seguinte modo:

Se $k, a_1, \ldots, a_n$ são inteiros não nulos então

- $k \big| (a_1, a_2, \ldots, a_n)$ se e só se $k \big| a_i$ para todo $i = 1, 2, \ldots, n$;
- $[a_1, a_2, \ldots, a_n] \big| k$ se e só se $a_i \big| k$ para todo $i = 1, 2, \ldots, n$.

Vejamos uma aplicação deste resultado.

Exemplo 2.13. *Vamos mostrar que o produto de* 5 *números inteiros consecutivos é múltiplo de* 120. *Dito de outro modo, vamos mostrar que* $120 \big| n(n+1)(n+2)(n+3)(n+4)$, *se* $n \in \mathbb{Z}$.

Note-se que $120 = 8 \times 5 \times 3$ *e que* $[8,5,3] = 120$ *(verifique!). Deste modo*

$$120 \big| n(n+1)(n+2)(n+3)(n+4) \iff \begin{cases} 8 \big| n(n+1)(n+2)(n+3)(n+4) \\ 5 \big| n(n+1)(n+2)(n+3)(n+4) \\ 3 \big| n(n+1)(n+2)(n+3)(n+4). \end{cases}$$

Transformamos uma questão num sistema de 3 *questões semelhantes envolvendo números mais pequenos. Para concluir basta notar que, em* 5 *números consecutivos:*

- *um deles é múltiplo de* 5 *e portanto o seu produto também é;*
- *pelo menos um deles é múltiplo de* 3 *e portanto o seu produto também é;*
- *pelo menos dois deles são múltiplo de* 2, *sendo um deles múltiplo de* 4 *e portanto o seu produto é múltiplo de* 4×2.

Exercícios

Muitos exercícios podem ser facilmente "inventados" pelos alunos. Por exemplo

o aluno deve tentar, depois de escolher inteiros a e b, calcular (a,b) e $[a,b]$ e escrever (a,b) combinação linear de a e de b. O mesmo pode ser feito se considerarmos 3 ou mais inteiros.

Vejamos outros exercícios, **cuja resolução terá de ser feita tendo em conta *apenas* os resultados enunciados**.

1) Verifique que o produto de:

a) 2 inteiros consecutivos é múltiplo de 2;
b) 3 inteiros consecutivos é múltiplo de 6;
c) 4 inteiros consecutivos é múltiplo de 24.

2) Dê um exemplo de $m, n \in \mathbb{N}$ tais que n^n divide m^m e n não divide m.
3) Para $a \in \{4, 5, 6, 7, \ldots, 30\}$ calcule $(244812738142, a)$.
4) Calcule$(987654, 987654 \times 1111 + 66)$;
5) Mostre que todo o quadrado perfeito é da forma $4n + 1$ ou da forma $4n$.
6) Mostre que o produto de dois inteiros da forma $6k + 5$ é da forma $6k + 1$.
7) Mostre que o quadrado de todo o inteiro ímpar é da forma $8k + 1$.
8) Mostre que a quarta potência de todo o inteiro ímpar é da forma $16k + 1$.
9) Mostre que, se n é ímpar e 3 não divide n, então $n^2 - 1$ é múltiplo de 24.
10) Mostre que, se n é a soma de 3 cubos, então o resto da divisão de n por 9 não é 4.
11) Dê exemplos de 3 inteiros não nulos cujo máximo divisor comum é igual a 1 mas que, dois a dois, não sejam primos entre si.
12) Mostre que $n^2 - 1$ é divisível por 8, se n é ímpar.
13) Mostre que, se $n \in \mathbb{Z}$:

a) $n^2 - n$ é divisível por 2;
b) $n^3 - n$ é divisível por 6;
c) $n^5 - n$ é divisível por 30;
d) $n^7 - n$ é divisível por 42.

14) Mostre que o resto da divisão da soma de dois quadrados por 4 nunca é igual a 3.
15) Mostre que a soma de dois inteiros é par se e só se a sua diferença for par.
16) Se $n \in \mathbb{N}$, quais os possíveis valores para:

a) $(n, n + 2)$?
b) $(n, n + 3)$?
c) $(n, n + 4)$?
d) $(n, n + 6)$?
e) $(n^2 + n + 7, n + 5)$?
f) $(2n^2 + n + 7, 3n + 5)$?

17) Mostre que, se $(a, b) = 1$ então $(a + b, a - b)$ é igual a 1 ou a 2.
18) Verifique que $(6k + 5, 7k + 6) = 1$, qualquer que seja $k \in \mathbb{Z}$.
19) Mostre que, se $n \in \mathbb{N}$ então $(n! + 1, (n + 1)! + 1) = 1$.
20) Mostre que, se $a, b \in \mathbb{N}$ e $[a, b] = (a, b)$ então $a = b$.
21) Mostre que, se $n \in \mathbb{N}$ então $(n, n + 1) = 1$ e $[n, n + 1] = n(n + 1)$.
22) Encontre todos os inteiros positivos a, b tais que $(a, b) = 10$ e $[a, b] = 100$.
23) Mostre que, se $a, b \in \mathbb{Z}$ e $d = (a, b)$ e $D = [a, b]$ então $\left[\frac{D}{a}, \frac{D}{b}\right] = \frac{D}{d}$
24) Mostre que, se $a, b, n \in \mathbb{N}$ e a^n divide b^n então a divide b.
25) É ou não verdade que, se $a, b, n \in \mathbb{N}$ com $n \geq 2$ e a^n divide $2b^n$ então a divide b?
26) Mostre que, se a, b, c são inteiros não nulos então $(c, [a, b]) = [(c, a), (c, b)]$.
27) Mostre que, se $n > 1$ então $n^4 + 4$ é o produto de dois inteiros maiores do que 1.

28) Mostre que, se $n \in \mathbb{Z}$ então $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7\,n}{15}$. é um número inteiro. Para que valores de n esse número é múltiplo de n?
29) Em quantos zeros termina o número 1132! (factorial de 1132)?
30) Mostre que o último algarismo não nulo de $n!$ é sempre par, se $n \geq 2$.
31) Em quantos zeros termina o número $\frac{500!}{200!}$?
32) Para que inteiros n o número $n!$ termina em 40 zeros?
33) Mostre que, se $n \in \mathbb{N}$ então $n!$ não pode terminar em 247 nem em 248 zeros.

3. Números Primos

Sabemos que todo o número inteiro é divisível por ele próprio, pelo seu simétrico, por 1 e por -1.

Definição 3.1. *Sejam $n, d \in \mathbb{Z}$. Diz-se d é um* **divisor próprio** *de n se $d \big| n$ e $d \notin \{1, -1, n, -n\}$.*

Definição 3.2. *Um inteiro diz-se:*

- ⋆ **irredutível** *se tiver exactamente dois divisores positivos.*
- ⋆ **redutível** *ou* **composto** *se tiver mais do que dois divisores positivos.*

Por exemplo: 6 e -6 são redutíveis pois admitem 4 divisores positivos (1, 2, 3 e 6); 5 e -5 são irredutíveis pois admitem apenas 2 divisores positivos (1 e 5); 1 e -1 são os únicos inteiros que não são irredutíveis nem redutíveis, pois têm apenas 1 divisor positivo (1); 0 é redutível pois todo o inteiro positivo é divisor de 0.

Note-se que os inteiros que não têm divisores próprios são o 1, o -1 e os números irredutíveis.

É também claro que se n for um inteiro positivo redutível então é um produto de dois inteiros a, b tais que $1 < a, b < n$. Para mostrar isto basta considerar a um divisor positivo de n que seja diferente de 1 e de n e $b = \frac{n}{a}$ que é um inteiro (porque a divide n), é diferente de 1 (pois caso contrário $n = a$) e diferente de n (pois caso contrário $a = 1$).

Definição 3.3. *Um inteiro positivo p diz-se* **primo** *se satisfaz a condição*

$$\forall a, b \in \mathbb{Z} \quad \Big[p \big| ab \Longrightarrow p \big| a \text{ ou } p \big| b \Big].$$

Note-se que esta condição de primalidade pode ser generalizada do seguinte modo

$$\forall a_1, a_2, \ldots, a_n \in \mathbb{Z} \quad \Big[p \big| a_1 a_2 \cdots a_n \Longrightarrow \exists\, i : \; p \big| a_i \Big].$$

Deste modo,

$$\boxed{\text{um número primo divide um produto se e só se dividir um dos factores.}}$$

Note-se que 6 não é um número primo porque 6 divide 2×3 e 6 não divide 2 nem 3.

Denotaremos por $\mathbb{P}$ o conjunto formado pelos números primos. Por abuso de notação diremos "primo" em vez de "número primo"

Teorema 3.4. *Um inteiro maior do que* 1 *é primo se e só se for irredutível.*

Demonstração. Se p é redutível sejam $a, b > 1$ tais que $p = ab$. Em particular p divide ab mas não divide a nem b pois estes dois números são positivos e menores do que p. Concluímos assim que p não é primo.

Suponhamos agora que p é um número irredutível e vamos mostrar que p é primo. Sejam $a, b \in \mathbb{Z}$ tais que p divide ab.

Note-se que (p, a) (máximo divisor comum de p e a) é um divisor positivo de p. Como p é irredutível, (p, a) é igual a 1 ou igual a p.

Se $(p, a) = p$ então p divide a, por definição de máximo divisor comum. Se $(p, a) = 1$ então, pela Proposição 2.5, p divide b. Daqui concluímos que p divide sempre a ou b, o que mostra que p é primo. □

Estamos agora em condições de enunciar e demonstrar o teorema fundamental da aritmética.

Teorema 3.5 (Teorema fundamental da aritmética)**.** *Todo o inteiro maior do que* 1 *é um produto de potências de expoente positivo de primos distintos. Essa escrita é única a menos da ordem dos factores.*

Demonstração. Para a primeira parte vamos usar um argumento de indução. Se $n = 2$ então n satisfaz as condições pretendidas.

Suponhamos agora que o teorema é verdadeiro para todo o inteiro menor do que n e vejamos que ele também vale para n. Se n é primo então não há nada a provar. Se n não for primo então, como $n > 1$, n é redutível e portanto existem $a, b \in \mathbb{N}$ tais que $n = ab$, $1 < a, b < n$. Por hipótese de indução, a e b podem ser escritos como um produto de potências de primos distintos. Multiplicando a por b, obtemos $n = ab$, escrito como um produto de potências de primos. Fazendo trocas e agrupando as potências com a mesma base obtemos o resultado pretendido.

Suponhamos agora que temos n escrito de dois modos, como produto de potências de primos

$$n \;=\; p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \;=\; q_1^{m_1} q_2^{m_2} \cdots p_s^{m_s}.$$

Deste modo, para $i = 1, \ldots, k$, p_i divide o produto $q_1^{m_1} q_2^{m_2} \cdots p_s^{m_s}$ (pois este produto é igual a n). Como p_i é primo e divide um produto $(q_1^{m_1} q_2^{m_2} \cdots p_s^{m_s})$ então divide um dos $(m_1 + \cdots + m_s)$ factores. Como esses factores são primos então existe j tal que $p_i = q_j$. Com o mesmo tipo de raciocínio podemos concluir que todo o primo da segunda factorização é um primo que aparece na primeira factorização.

Concluímos assim que as duas representações de n como um produto de primos usam os mesmos primos. Deste modo, reordenando esses primos e agrupando os que são iguais podemos escrever

$$n \;=\; p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \;=\; p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

para alguns primos distintos $p_1, p_2, \ldots, p_k$ e inteiros positivos $n_1, n_2, \ldots, n_k, m_1, m_2, \ldots, m_k$.

Vejamos que $n_i = m_i$ para todo $i = 1, \ldots, k$. Se, por exemplo e sem perda de generalidade, $n_1 > m_1$ então, simplificando obteríamos

$$p_1^{n_1 - m_1} p_2^{n_2} \cdots p_k^{n_k} \;=\; p_2^{m_2} \cdots p_k^{m_k}$$

o que é absurdo, pois p_1 divide $p_1^{n_1-m_1} p_2^{n_2} \cdots p_k^{n_k}$ e não divide $p_2^{m_2} \cdots p_k^{m_k}$, pois p_1 é diferente de p_i para $i \neq 1$. $\square$

Note-se que na primeira parte usamos de facto a noção de irredutível como foi definida e na segunda a noção de primo. Como estas duas noções são equivalentes tudo funciona!

Nota 3.6. *Se considerarmos, no lugar de $\mathbb{Z}$, o espaço $2\mathbb{Z}$, formado pelos números inteiros pares, onde tem sentido somar e multiplicar, podemos definir número primo e número irredutível da mesma maneira. Por exemplo os números 2, 6, 10 e 30 são irredutíveis (não se escrevem como produto de dois elementos de $2\mathbb{Z}$) e $2 \times 30 = 6 \times 10$. Deste modo, 60 escreve-se de duas maneiras como produto de irredutíveis. Note-se que, atendendo às igualdades acima, nenhum dos números 2, 6, 10 e 30 é primo.*

Exemplo 3.7. *Vejamos que, se $(a, b) = 1$ então $(a + b, a^2 - ab + b^2) \in \{1, 3\}$. Note-se que $a^2 - ab + b^2 = (a + b)^2 - 3\,ab$ (no fundo, "dividimos" $a^2 - ab + b^2$ por $a + b$) e, usando a Proposição 2.2, alínea f), temos*

$$(a + b, a^2 - ab + b^2) \quad = \quad (a + b, 3\,ab).$$

Se p é um primo que divide $3\,ab$ e $a+b$ então, p divide 3, a ou b. Se p divide a então, como também divide $a + b$ podemos concluir que p divide b (pois $b = (a + b) - a$) o que contradiz o facto de a e b serem primos entre si. Se p divide b então chegamos também a uma contradição. Mostramos assim que 3 é o único primo que pode dividir simultaneamente $3\,ab$ e $a+b$, ou seja, o único primo que pode dividir $(3\,ab, a+b)$. Usando o teorema fundamental da aritmética sabemos que existe $k \in \mathbb{N}$ tal que $(a+b, 3\,ab) = 3^k$. Se $k \geq 2$ então 9 divide $3\,ab$ e, portanto 3 divide ab, o que nos leva de novo a uma contradição. Conclusão: $(a + b, 3\,ab)$ é igual a 1 ou a 3.

Note-se que, se tivermos dois inteiros maiores do que 1 podemos sempre escrevê-los como produto de potências dos mesmos primos desde que aceitemos que os expoentes possam ser iguais a 0. Por exemplo, podemos escrever 24 e 45 como produto de potências dos mesmos primos:

$$24 = 2^3 \times 3 \times 5^0 \quad \text{e} \quad 45 = 2^0 \times 3^2 \times 5.$$

Com este resultado podemos finalmente calcular o máximo divisor comum e o mínimo múltiplo comum como "estamos habituados". Começamos com um lema cuja demonstração usa essencialmente o teorema fundamental da aritmética.

Lema 3.8. *Se* $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ *em que* $p_1, p_2, \ldots, p_k$ *são primos distintos e* $n_1, n_2, \ldots, n_k \in \mathbb{N}_0$ *então os divisores positivos de* n *são os números da forma*

$$p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}, \quad \textit{em que } 0 \leq s_i \leq n_i \textit{ para todo } i = 1, 2, \ldots, k.$$

Em particular existem $(n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$ *divisores positivos de* n*.*

Demonstração. É claro que os números da forma referida são divisores de n pois, se $0 \leq s_i \leq n_i$ para todo $i = 1, 2, \ldots, k$, então

$$\left(p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}\right)\left(p_1^{n_1-s_1} p_2^{n_2-s_2} \cdots p_k^{n_k-s_k}\right) \quad = \quad n.$$

Por outro lado, se d é um divisor positivo de n e $x \in \mathbb{N}$ é tal que $dx = n$ então os números primos que dividem d ou x também dividem n. Deste modo d e x são da forma $p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ e $p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ com $s_i, t_i \geq 0$ para todo $i = 1, 2, \ldots, k$. Da igualdade $dx = n$, obtemos

$$p_1^{s_1+t_1} p_2^{s_2+t_2} \cdots p_k^{s_k+t_k} = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

Pelo teorema fundamental da aritmética, parte relativa à unicidade, $s_i + t_i = n_i$ e portanto $s_i \leq n_i$. □

No teorema que segue a alínea c) já foi demonstrada, mas tem aqui uma demonstração aparentemente mais simples.

Teorema 3.9. *Sejam* n, m *inteiros maiores do que* 1 *e suponhamos que*

$$n \;=\; p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \qquad\qquad m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

em que $p_1, p_2, \ldots, p_k$ *são primos distintos e* $n_1, n_2, \ldots, n_k, m_1, m_2, \ldots, m_k \in \mathbb{N}_0$*. Nestas condições:*

a) $(n, m) = p_1^{\min\{n_1, m_1\}} p_2^{\min\{n_2, m_2\}} \cdots p_k^{\min\{n_k, m_k\}}$*;*

b) $[n, m] = p_1^{\max\{n_1, m_1\}} p_2^{\max\{n_2, m_2\}} \cdots p_k^{\max\{n_k, m_k\}}$*;*

c) $[n, m] = \frac{nm}{(n,m)}$*.*

Demonstração. A alínea a) é uma consequência imediata do lema anterior que, neste caso, diz que os divisores de n e de m são os inteiros da forma

$$p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k},\ \text{em que } 0\le s_i\le n_i,\ 0\le s_i\le m_i,\ \text{para todo } i=1,2,\ldots,k,$$

sendo o maior deles $p_1^{\min\{n_1,m_1\}}p_2^{\min\{n_2,m_2\}}\cdots p_k^{\min\{n_k,m_k\}}$.

Usando o mesmo lema, os múltiplos de n e de m são os inteiros da forma

$$p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}\cdot A,\ \text{em que } s_i\ge n_i,\ s_i\ge m_i, \text{ para todo } i=1,2,\ldots,k \text{ e } A\in\mathbb{Z},$$

sendo o menor deles $p_1^{\max\{n_1,m_1\}}p_2^{\max\{n_2,m_2\}}\cdots p_k^{\max\{n_k,m_k\}}$.

A alínea c) é uma consequência das outras duas, pois

$$(n,m)\cdot[n,m] \quad = \quad \prod_{i=1}^{k} p_i^{\min\{n_i,m_i\}} \times \prod_{i=1}^{k} p_i^{\max\{n_i,m_i\}} = \prod_{i=1}^{k} p_1^{n_i+m_i} = nm,$$

uma vez que $\min\{n_i,m_i\}+\max\{n_i,m_i\}=n_i+m_i$, para $i=1,\ldots,k$. □

Note-se também que das alíneas a) e b) deste teorema resultam grande parte dos resultados referidos na secção anterior.

Este teorema pode ser generalizado para calcularmos o mdc e o mmc de k inteiros positivos.

Vejamos agora o chamado teorema de Euclides.

Teorema 3.10 (Euclides)**.** *$\mathbb{P}$ é um conjunto infinito.*

Demonstração. Suponhamos que o conjunto formado pelos números primos é finito. Sejam $p_1,p_2,\ldots,p_k$ esses números primos e considere-se

$$N \quad = \quad p_1p_2\cdots p_k+1.$$

Como $N>1$, pelo teorema fundamental da aritmética, existe um número primo que divide N. Como os únicos primos que existem são $p_1,p_2,\ldots,p_k$ sabemos que existe $i\in\{1,2,\ldots,k\}$ tal que p_i divide N. Deste modo, como p_i divide $p_1p_2\cdots p_k$ podemos concluir que p_i divide $N-p_1p_2\cdots p_k$, ou seja, que p_i divide 1. Chegamos assim a uma contradição. □

Este tipo de demonstração pode ser usada para demonstrar, por exemplo, que existe um número infinito de primos da forma $4n+3$. A ideia é seguir a demonstração de Euclides, considerando $N=4p_1p_2\cdots p_k+3$, que é um número ímpar. De seguida notar que todos os primos ímpares são da forma $4n+1$ ou $4n+3$. Em particular, como N é um produto de primos, nem todos podem ser da forma $4n+1$, pois caso contrário N seria dessa forma. Concluímos assim que pelo menos um dos primos que divide N é da forma $4n+3$ e, claro, diferente dos primos p_i com $i=1,2,\ldots,k$.

Por tentativas é fácil de encontrar (por exemplo) 5 inteiros consecutivos que não sejam primos. Podemos começar, por exemplo, em 24 ou em 32 ou em 48. Mas se quisermos 6 inteiros consecutivos que não sejam primos já temos de ir um "pouco mais longe", até 90 (de facto acabamos por encontrar 7 inteiros consecutivos que não são primos). '

Embora possa não parecer fácil encontrar 100 inteiros consecutivos, isso não é verdade. De facto, se $k \in \mathbb{N}$ então

$$(k+1)!+2, \qquad (k+1)!+3, \qquad (k+1)!+4, \qquad \ldots \qquad (k+1)!+(k+1)$$

são k inteiros consecutivos que não são números primos, pois $(k+1)!+j$ é múltiplo de j, se $j = 2, 3, \ldots, k-1$. Note-se que, se $k = 6$ este método encontra seis números consecutivos não primos muito maiores do que os que encontramos acima que começavam em 90 e estes começam em $7! + 2 = 5\,042$.

É claro que não pode haver 3 primos consecutivos porque apenas o 2 é um primo par. Por outro lado 3, 5 e 7 são os únicos três ímpares consecutivos que são primos. Verifique!

Nota 3.11. *Uma das primeiras questões que se colocaram sobre os números primos é o da sua distribuição. Por exemplo, se $\pi(x)$ for o número de primos que são menores ou iguais a x, Euclides demonstrou (Teorema 3.10) que $\lim_{x\to+\infty} \pi(x) = +\infty$.*

O chamado **teorema dos números primos** *diz-nos que $\pi(x)$ e $\frac{x}{\log x}$ "crescem à mesma velocidade", quando $x \to \infty$. Mais propriamente,*

$$\lim_{x\to+\infty} \pi(x) \Big/ \frac{x}{\log x} \quad = \quad 1.$$

No fundo, isto diz que, para x grande o número de primos até x é mais ou menos igual a $\frac{x}{\log x}$. Daqui "resulta" também que o n-ésimo primo, p_n, é da mesma ordem de grandeza de $n\log(n)$.

Podemos assim ter uma estimativa do número de primos que se escrevem com n dígitos. Note-se que os primos com n dígitos são os primos que pertencem ao intervalo $\left[10^{n-1}, 10^n\right]$ (é claro que 10^n tem $n+1$ dígitos, mas não é primo).

Assim, o número de primos com n dígitos é igual a $\pi(10^n) - \pi(10^{n-1})$. Utilizando o teorema dos números primos temos

$$\pi(10^n) - \pi(10^{n-1}) \approx \frac{10^n}{\log(10^n)} - \frac{10^{n-1}}{\log(10^{n-1})} = \frac{10^n}{n\log(10)} - \frac{10^{n-1}}{(n-1)\log(10)} = \frac{10^{n-1}}{\log(10)}\left(\frac{9n-10}{n(n-1)}\right).$$

Em percentagem isto corresponde a

$$\frac{\pi(10^n) - \pi(10^{n-1})}{10^n - 10^{n-1}} \approx \frac{9n-10}{(9n-9)\log(10)n} \approx \frac{1}{\log(10)n}.$$

Em particular, dos inteiros positivos que se escrevem com 20 *algarismos, aproximadamente* $0,19429 \times 10^{19}$ *deles são primos o que significa mais ou menos* $2,1588\%$ *desses números. Na realidade a percentagem de números primos com* 20 *dígidos é* $2,2075\%$.

Uma outra função que se considera é a função Li *definida por* $Li(x) = \displaystyle\int_2^x \frac{1}{\log(t)}\, dt$.

As seguintes tabelas dão uma ideia da aproximação entre $\frac{x}{\log x}$ *e* $Li(x)$ *relativamente a* $\pi(x)$ *e de* $n \log n$ *relativamente a* p_n.

x	$\pi(x)$	$x/\log(x)$	$Li(x)$
10^3	168	144,8	177,6
10^4	1 229	1 085,7	1 246,1
10^5	9 592	8 685,9	9 629,8
10^6	78 498	72 382,4	78 627,5
10^7	644 579	620 420,7	664 918,4
10^8	5 761 455	5 428 681,0	5 762 209,4
10^9	60 847 534	48 254 942 4	60 849 235,0
10^{10}	455 052 511	434 294 481.9	455 055 614.6

n	p_n	$n\log(n)$	$p_n/n\log(n)$
10	29	23,0	1,26
10^2	541	460,5	1,17
10^3	7 919	6 907,8	1,15
10^4	104 729	92 203	1,14
10^5	1 299 709	1 151 292,5	1,13
10^6	15 485 863	13 815 510,6	1,12
10^7	179 424 673	161 180 956,5	1,11

x	$\pi(x)((x/\log(x))$	$\pi(x)/Li(x)$
10^3	1,160502887	0,9458945076
10^4	1,131950832	0,9862477295
10^5	1,104319810	0,9960737534
10^6	1,084489948	0,9983523695
10^7	1,038938598	0,9694106751
10^8	1,061299232	0,9998690825
10^9	1,260959623	1,196626342
10^{10}	1,047797128	0,9999931800

Exercícios

Recorde as igualdades, para $a, b \in \mathbb{R}$ e $n \in \mathbb{N}$

$$
\begin{aligned}
a^n - b^n &= (a-b)\sum_{k=0}^{n-1} a^{n-1-k} b^k \\
a^n + b^n &= (a+b)\sum_{k=0}^{n-1} (-1)^k a^{n-1-k} b^k, \quad \text{se } n \text{ é ímpar.}
\end{aligned}
$$

Em particular $a-b$ divide $a^n - b^n$ e $a+b$ divide $a^n + b^n$, se n é ímpar.

1) Seja $p \in \mathbb{P}$, com $p > 3$. Mostre que o resto da divisão de p por 6 é igual a 1 ou a 5.
2) Mostre que, se $p, p+2 \in \mathbb{P}$ e $p > 3$ então $p+1$ é divisível por 6.
3) Mostre que, se $a, b \in \mathbb{Z}$, então $a^4 - b^4$ não é um número primo.
4) Mostre que, se $p \in \mathbb{P}$, $p\big|a$ e $p\big|a^2 + b^2$ então $p\big|b$.
5) Mostre que, se $p \in \mathbb{P}$, $p\big|a^2 + b^2$ e $p\big|b^2 + c^2$ então $p\big|a + c$ ou $p\big|a - c$.
6) Mostre que, se $p \in \mathbb{N}$ e p, $p+2$ e $p+4$ são primos, então $p = 3$.
7) Mostre que $(a^n, b^n) = (a, b)^n$ e $[a^n, b^n] = [a, b]^n$.

8) Mostre que, se $a, b, c \in \mathbb{N}$ então a divide bc se e só se $\frac{a}{(a,b)}$ divide c.
9) Seja n um número que é divisível exactamente por 3 números primos. Mostre que existem 8 escolhas de pares ordenados de divisores de n, que são primos entre si e cujo produto é igual a n. Generalize.
10) Encontre todos os números primos p tais que $17p + 1$ é um quadrado perfeito.
11) Se $(a, b) = p$ em que $p \in \mathbb{P}$, quais são as possibilidades para (a^2, b)? E para (a^3, b^4)?
12) Se $(a, p^2) = p$ e $(b, p^3) = p^2$, com $p \in \mathbb{P}$, qual o valor de (ab, p^4) e de $(a + b, p^4)$?
13) Seja $n > 1$ e p o menor primo que divide n. Mostre que;
    a) se $p > \sqrt{n}$, então n é primo.
    b) se $p > \sqrt[3]{n}$, então n ou n/p é primo.
14) Mostre que, se $ax - by = \pm 1$ então $(a + b, x + y) = 1$.
15) Encontre um divisor primo de: $2^{30} + 1$; $2^{40} + 1$; $2^{36} + 1$.
16) Factorize os números: $10^6 - 1$; $2^{24} - 1$; $10^8 - 1$; ; $2^{15} - 1$.
17) Mostre que 13 divide $2^{70} + 3^{70}$.
18) Sejam $a, n, \in \mathbb{N}$. Mostre que
    a) se $a^n - 1$ é primo então $a = 2$ e n é primo;
    b) se $a > 1$ e $a^n + 1$ é primo então n é uma potência de 2;
    c) se $b, m \in \mathbb{N}$ e $a^n + b^m$ é primo então (n, m) é uma potência de 2.
19) Mostre que, se p é um número primo e $p > k > 0$ então $\binom{p}{k}$ é múltiplo de p.
20) Mostre que $2^{2^m} - 1$ tem pelo menos m factores primos distintos.
21) Para que valores de $n \in \mathbb{N}$, $(2n^2 + 3n + 8, n^2 + n + 9) = 1$?
22) Sejam $m, n \in \mathbb{N}$ com m ímpar. Mostre que $(2^m - 1, 2^n + 1) = 1$.
23) Mostre que, se $a, m, n \in \mathbb{N}$ e $m \neq n$ então $(a^{2^m} + 1, a^{2^n} + 1) \in \{1, 2\}$.
24) Mostre que um número positivo maior do que 1 é um quadrado perfeito se e só se e só se é a sua expressão como um produto de potências de primos envolve apenas expoentes pares.
25) Sejam $a, b \in \mathbb{N}$ tais que $(a, b) = 1$. Mostre que se ab é um quadrado perfeito então a e b são quadrados perfeitos.
26) Mostre que todo o número positivo é é um produto de um quadrado perfeito por um número que não é divisível por nenhum quadrado perfeito diferente de 1.
27) Considere a_1 um número ímpar qualquer e defina a_n recursivamente por $a_n = a_1 \cdots a_{n-1} + 2$. Por exemplo, se $a_1 = 1$ então $a_2 = 3$, $a_3 = 5$, $a_4 = 17$, $a_5 = 257$, $a_6 = 25537$, $a_7 = 4294967297$, etc..
    a) Mostre que, se $n, m \in \mathbb{N}$ e $n \neq m$ então a_n e a_m são primos entre si.
    b) Conclua que há uma infinidade de primos.