Universidade do Minho
Departamento de Matemática

Licenciatura em Matemática

Matemática Discreta

1. Divisibilidade

Definição 1.1. *Se $a, b \in \mathbb{Z}$, dizemos que a* **divide** *b e escrevemos $a|b$ 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) $a|0$, $1|a$, $a|a$ *e* $-a|a$.

b) Se $a|b$ *então* $a|bc$.

c) Se $a|b$ *e* $b|c$ *então* $a|c$.

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

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

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

g) Se $a|b$ *então* $ac|bc$.

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

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, $b = ax$.

□

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 $\mathbb{N} \cap]\frac{b}{a}, +\infty[$. 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 $\left]-|a|,\ |a|\right[$. 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 $r = r^*$. □

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 $a = bq + r$ *então* $(a,b) = (r,b)$.

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) Note-se que, se d divide a e b então divide r porque $r = a - bq$. Inversamente, se d divide r e b então também divide a, porque $a = bq + r$. Em ambos os argumentos usamos o Teorema 1.2 d). □

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!

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

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 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 pelo exemplo: $4\big|2\times 2$.

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 $dm\leq d^*$. 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, $d^*\leq dm$.

b) Basta notar que

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

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

Teorema 2.7. *Se $a,b,m\in\mathbb{Z}$ 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'. □

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*

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

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 $\dfrac{n^5}{5}+\dfrac{n^3}{3}+\dfrac{7\,n}{15}$. 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

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

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

Denotaremos por $\mathbb{P}$ o conjunto formado pelos números primos.

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 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). 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 $n_1, n_2, \ldots, n_k, m_1, m_2, \ldots, m_k$.

Se, por exemplo, $n_1 > m_1$ 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 $i \neq 1$. □

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!

Vejamos como, com este resultado, podemos mostrar que $(a+b, a^2-ab+b^2) \in \{1,3\}$ se $(a,b)=1$. Note-se que $a^2-ab+b^2 = (a+b)^2 - 3\,ab$ (no fundo, "dividi" 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 corolário anterior 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.

No caso em que $(a,b) \neq 1$ então $(a+b, a^2-ab+b^2)$ pode não dividir $3(a,b)$ (que seria a generalização natural do resultado anterior) como se pode ver se $a=6$ e $b=10$, onde $(a+b, a^2-ab+b^2) = (16,76) = 4$ e $(a,b)=2$.

Se tivéssemos um exemplo do tipo $(a^3+ab^2, a^3-a^2b-b^3)$ (dois polinómios cujas parcelas têm todas o mesmo grau (3 neste caso) então, se $d=(a,b)$, $A=\frac{a}{d}$ e $B=\frac{b}{d}$, $(A,B)=1$ e

$$(a^3+ab^2, a^3-a^2b-b^3) = d^3(A^3+AB^2, A^3-A^2B-B^3).$$

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 3.6. *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 $p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, em que $0 \leq s_i \leq n_i$ 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 corolário anterior, 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.

Teorema 3.7. *Sejam n, m inteiros maiores do que 1 e suponhamos que*

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

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

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

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

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

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

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

□

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

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

$$N \quad = \quad p_1 p_2 \cdots p_k + 1.$$

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 $p_1 p_2 \cdots p_k$ podemos concluir que p_i divide $N - p_1 p_2 \cdots p_k$, 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 $N = 4p_1 p_2 \cdots p_k + 3$, 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. Se em vez de 5 considerarmos 100 talvez não seja muito simples de encontrar 100 inteiros consecutivos que não sejam primos. De facto é muito simples (depois de ver). Por exemplo, os números

$$100! + 2, \qquad 100! + 3, \qquad 100! + 4, \qquad \ldots \qquad 100! + 100$$

não são primos porque são divisíveis por 2, 3, 4, ... e 100, respectivamente. Mais geralmente temos.

Proposição 3.9. *Se $k \in \mathbb{N}$ então existem k inteiros consecutivos que não são números primos.*

Demonstração. Basta considerar, para $j = 2, \ldots, k + 1$, os números $(k + 1)! + j$ e notar que j é um divisor próprio de $(k + 1)! + j$. □

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 ímpares consecutivos que são primos. Verifique!

Uma das primeiras questões que se colocam 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, sabemos

pelo Teorema de Euclides 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". 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, e $n\,\log(n)$ têm a mesma ordem de grandeza.

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 30 algarismos, aproximadamente $0,12979 \times 10^{29}$ deles são primos o que significa mais ou menos $1,44876\%$ desses números.

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

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	664 579	620 420,7	664 918,4
10^8	5 761 455	5 428 681,0	5 762 209,4
10^9	50 847 534	48 254 942 4	50 849 235,0

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

Exercícios

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 $p \in \mathbb{N}$ e p, $p+2$ e $p+4$ são primos, então $p = 3$.
5) Mostre que $(a^n, b^n) = (a,b)^n$ e $[a^n, b^n] = [a,b]^n$.
6) Mostre que, se $a, b, c \in \mathbb{N}$ então a divide bc se e só se $\frac{a}{(a,b)}$ divide c.

7) 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.
8) Encontre todos os números primos p tais que $17p + 1$ é um quadrado perfeito.
9) Se $(a, b) = p$ em que $p \in \mathbb{P}$, quais são as possibilidades para (a^2, b)? E para (a^3, b^4)?
10) 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 $(a + b, p^4)$?
11) Mostre que, se $p \in \mathbb{P}$, $p|a$ e $p|a^2 + b^2$ então $p|b$.
12) Mostre que, se $p \in \mathbb{P}$, $p|a^2 + b^2$ e $p|b^2 + c^2$ então $p|a + c$ ou $p|a - c$.
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 $a > 1$ e $a^n + 1$ é primo então n é uma potência de 2;
    b) se $a^n - 1$ é primo então $a = 2$ e n é primo;
    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.

4. Congruências módulo um inteiro positivo n

Dado $n \in \mathbb{N}$, consideremos a relação binária $\equiv_n$ sobre $\mathbb{Z}$ definida por,

$$a \equiv_n b \iff n | a - b. \qquad \text{(lê-se "}a \text{ congruente com } b \text{ módulo } n\text{")}.$$

Por vezes escreveremos $a \equiv b \pmod{n}$ em vez de $a \equiv_n b$.

Usaremos a notação $a \not\equiv_n b$ ou $a \not\equiv b \pmod{n}$ para dizer que a e b não são congruentes módulo n.

Facilmente se vê que a relação $\equiv_n$ é uma relação de equivalência.

Proposição 4.1. *Se $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$ então $a \equiv_n b$ se e só se o resto da divisão de a por n é igual ao resto da divisão de b por n. Em particular, todo o inteiro é congruente módulo n com um e um só inteiro pertencente ao conjunto $\{0, 1, \ldots, n-1\}$.*

Demonstração. Sejam r_1 e r_2 os restos da divisão de a e de b (respectivamente) por n. Então $a \equiv_n r_1$ e $b \equiv_n r_2$. Por transitividade temos $a \equiv_n b$ se e só se $r_1 \equiv_n r_2$. Para concluir basta notar que, como $r_1, r_2 \in \{0, 1 \ldots, n-1\}$, então $r_1 \equiv_n r_2$ se e só se $r_1 = r_2$. □

Uma propriedade importante desta relação de equivalência é o facto de ela se "comportar bem" relativamente às operações de soma e de multiplicação de inteiros.

Proposição 4.2. *Se $n \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ são tais que $a \equiv_n b$ e $c \equiv_n d$ então,*

$$\begin{cases} a + c & \equiv_n & b + d \\ ac & \equiv_n & bd. \end{cases}$$

Em particular, se $k \in \mathbb{Z}$ e $m \in \mathbb{N}$,

$$\begin{cases} k\,a & \equiv_n & k\,b \\ a^m & \equiv_n & b^m. \end{cases}$$

Demonstração. Sejam $r, s \in \mathbb{Z}$ tais que $a - b = rn$ e $c - d = sn$. Então

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) = (r + s)n \\ ac - bd &= a(c - d) + d(a - b) = (as + dr)n \end{aligned}$$

o que mostra que $a + c \equiv_n b + d$ e $ac \equiv_n bd$. Aplicando repetidamente este resultado, com $a = c$ e $b = d$ concluímos que $k\,a \equiv_n k\,b$ e $a^m \equiv_n b^m$. □

Como exemplo de aplicação destas noções podemos mostrar que nenhum número da forma $4n + 3$ é uma soma de dois quadrados perfeitos. Para isso basta notar que, se $r \in \mathbb{Z}$ então usando a Proposição 4.2,

$$r^2 \equiv_4 \begin{cases} 0 & \text{se } r \equiv_4 0 \text{ ou } r \equiv_4 2 \\ 1 & \text{se } r \equiv_4 1 \text{ ou } r \equiv_4 3 \end{cases}$$

e, portanto a soma de dois quadrados é congruente com 0, 1 ou 2.

4.1. **Critério de divisibilidade por 2, 3, 4, 5, 8, 9 e 11.**

Consideremos um número inteiro $n = (a_k \cdots a_1 a_0)_{10}$ escrito na base 10. Isto significa que

$$n = a_0 + 10\, a_1 + \cdots + 10^k\, a_k.$$

Observe-se que

$$10 \equiv \begin{cases} 0 \ (\mod 2) \\ 0 \ (\mod 5) \\ 1 \ (\mod 3) \\ 1 \ (\mod 9) \\ -1 \ (\mod 11) \end{cases}$$

e, usando a Proposição 4.2, se $i \in \mathbb{N}$,

$$10^i \equiv \begin{cases} 0 \ (\mod 2) \\ 0 \ (\mod 5) \\ 1 \ (\mod 3) \\ 1 \ (\mod 9) \\ 1 \ (\mod 11) \text{ se } i \text{ é par} \\ -1 \ (\mod 11) \text{ se } i \text{ é ímpar.} \end{cases}$$

Por outro lado, $10^k \equiv 0 \pmod 4$, se $k \geq 2$ (porque 100 é múltiplo de 4) e $10^k \equiv 0 \pmod 8$, se $k \geq 3$ (porque 1000 é múltiplo de 8), etc.. Deste modo, usando novamente a Proposição 4.2,

$$n = a_0 + 10\, a_1 + \cdots + 10^k\, a_k \equiv \begin{cases} a_0 & (\mod 2) \\ a_0 & (\mod 5) \\ (a_1 a_0)_{10} & (\mod 4) \\ (a_2 a_1 a_0)_{10} & (\mod 8) \\ a_0 + a_1 + \cdots + a_k & (\mod 3) \\ a_0 + a_1 + \cdots + a_k & (\mod 9) \\ a_0 - a_1 + \cdots + (-1)^k a_k & (\mod 11). \end{cases}$$

Em particular o resto da divisão de n por 9 ou por 3 é igual ao resto da divisão de $a_0 + a_1 + \cdots + a_k$ por 9 ou por 3, o que justifica a chamada "prova dos nove".

Os critérios de divisibilidade acima referidos podem também servir para mostrar que o número 155 832 732 é divisível por 396. De facto $396 = 4 \times 9 \times 11$ e, portanto 155 832 732 é divisível por 396 se e só se for divisível por 4, 9 e 11 (note-se que estes 3 últimos números são primos entre si). Para concluir basta aplicar os critérios referidos a cima.

Nota 4.3. *Seja $n = (a_k \cdots a_1 a_0)_{10}$ um número escrito na base 10. Então*

- *n é divisível por 7 se e só se o número $(a_k \cdots a_1)_{10} - 2a_0$ o for.*
- *n é divisível por 13 se e só se o número $(a_k \cdots a_1)_{10} + 4a_0$ o for.*

Estes critérios não são interessantes pois não são mais rápidos do que fazer a divisão. A única "vantagem" é que não precisamos de saber fazer divisões! Além disso estas operações, contrariamente às anteriores, não "preservam" o resto da divisão por 7 *ou por* 13.

Por exemplo

$$7 \big| 213\,752 \;\Leftrightarrow\; 7 \big| 21371 \;\Leftrightarrow\; 7 \big| 2135 \;\Leftrightarrow\; 7 \big| 203 \;\Leftrightarrow\; 7 \big| 14$$
$$13 \big| 213\,752 \;\Leftrightarrow\; 13 \big| 21383 \;\Leftrightarrow\; 13 \big| 2150 \;\Leftrightarrow\; 13 \big| 215 \;\Leftrightarrow\; 13 \big| 41.$$

Assim, 213 752 *é múltiplo de* 7 *e não de* 13. *Note-se que* $213\,752 \equiv_{13} 6$ *e* $41 \equiv_{13} 2$.

Exercícios

1) Liste todos os inteiros positivos menores do que 100 que são congruentes com 7 módulo 13.
2) Encontre 17 múltiplos de 3 de tal forma que qualquer inteiro seja congruente, módulo 17, com um desses inteiros.
3) Mostre que em cada ano civil há pelo menos uma sexta-feira, dia 13.
4) Se no dia x do mês y do ano z for um quarta-feira, que dia de semana é o dia x do mês y do ano $z+1$? E se for do ano $z+4$?
5) Qual o próximo ano em que o dia 1 de Maio é uma segunda-feira?
6) Que dia de semana será o dia 10 de Novembro de 2012?
7) Em que dia de semana foi o dia 27 de Fevereiro de 1900?
8) Qual o resto da divisão de a por n, sendo:

   a) $a = 6789032453$ e $b = 11$;
   b) $a = 2^{30} - 1234$ e $n = 23$;
   c) $a = 3^{10} - 1$ e $n = 121$;
   d) $a = 2^{70} + 3^{70}$ e $n = 13$;
   e) $a = 33333 \times 444444 \times 555555 \times 666666$ e $n = 23$.

9) Mostre que a soma dos algarismos de um quadrado perfeito não pode ser 375. (Faça as contas módulo 9)
10) Mostre que o algarismo das unidades de um quadrado perfeito é 0, 1, 4, 5, 6 ou 9.
11) Seja a um cubo. Mostre que $(a-1)a(a+1)$ e um múltiplo de 504.
12) Qual o último algarismo de 23^{34}? e de 101^{34}? e de $101^{102^{102}}$?
13) Quais os dois últimos algarismos de 23^{34}? e de 101^{34}? e de $101^{102^{102}}$?
14) Mostre que, se $a^2 \equiv b^2 \pmod{p}$ em que p é um número primo, então $a \equiv b \pmod{p}$ ou $a \equiv -b \pmod{p}$. A afirmação continua verdadeira se não exigirmos que p seja primo?
15) Mostre que a equação $15x^2 - 7y^2 = 9$, com $x, y \in \mathbb{Z}$, não tem soluções.
16) Mostre que se um número n é a soma de 3 quadrados então $n \not\equiv 7 \pmod{8}$.

17) Existe algum inteiro n cujo cubo"termine" em 63?
18) Qual o menor inteiro n cujo cubo "termina" em 92?
19) Para que valores de $x \in \mathbb{Z}$, $x^4 + y^4 \equiv 1 \pmod 5$? (Faça as contas módulo 5)
20) Mostre que não existe $x \in \mathbb{Z}$ tal que $x^3 + y^3 + z^3 = 4 \pmod 9$. (Faça as contas módulo 9)
21) Mostre que se $n \in \mathbb{N}$ então $n^5 \equiv n \pmod{30}$, $n^9 \equiv n^3 \pmod{252}$ e $4n^2 \not\equiv 3 \pmod 7$.
22) Para $n \in \{2, 4, 6, 8\}$ encontre x tal que $x^2 \equiv x \pmod n$.
23) Determine todos os inteiros da forma $66\cdots6$ que são múltiplos de 7.
24) Mostre que os número $99\cdots9$ e $10\cdots01$, em que o número de algarismos é par, são múltiplos de 11.
25) Encontre um inteiro n maior que 100 tal que $11\cdots1$ (n algarismos) é múltiplo de 7.
26) Mostre que, se $11\cdots1$ (n algarismos) é primo, então n é primo.
27) Em quantos zeros termina 1000!?
28) Mostre que, se $k \geq 2$, o último inteiro não nulo de $k!$ é par.
29) Qual o maior inteiro n tal que 7^n divide $\begin{pmatrix} 5000 \\ 2000 \end{pmatrix}$?
30) Determine todos os inteiros positivos n tais que $n!$ termina exactamente em 75 zeros.
31) Mostre se $n \in \mathbb{N}$ então é impossível $n!$ terminar exactamente em 153, 154 ou 155 zeros.

5. Equações diofantinas

Comecemos com um exemplo.

Exemplo 5.1. *Suponhamos que só existiam moedas de* 15 *e de* 7 *cêntimos e que eu queria pagar (em dinheiro) uma certa quantia em cêntimos. Será que é sempre possível? E se só existissem moedas de* 12 *e de* 30 *cêntimos?*

No primeiro caso, se conseguirmos pagar 1 cêntimo então também sabemos pagar qualquer quantia: basta repetir o pagamento de 1 cêntimo as vezes que forem necessárias. Para pagar 1 cêntimo podemos usar uma moeda de 15 e receber de troco duas moedas de 7. Deste modo, se quisermos pagar 23 cêntimos podemos usar 23 moedas de 15 e receber de troco 46 moedas de 7. É claro que seria mais simples pagar com 2 moedas de 15 e receber 1 moeda de 7 de troco. No fundo estamos a procurar soluções inteiras da equação $7x + 15y = m$, com $m = 1$ e $m = 23$.

No segundo caso é claro que qualquer quantia que se consiga pagar é necessariamente múltipla de 6, porque 12 e 30 são múltiplos de 6 (note-se que $(12, 30) = 6$). Por outro lado

podemos pagar 6 cêntimos usando uma moeda de 30 e recebendo de troco duas moedas de 12. Deste modo podemos fazer o pagamento de qualquer quantia que seja múltipla de 6.

Chegamos assim à seguinte definição.

Definição 5.2. *Uma equação nas variáveis inteiras x, y do tipo*

$$ax + by = c, \quad \text{com } a, b, c \in \mathbb{Z}$$

diz-se uma **equação diofantina**.

A palavra diofantina "vem" de Diofanto, matemático do século III.

O seguinte resultado é uma generalização do Teorema 2.4.

Teorema 5.3. *Sejam a, b inteiros não ambos nulos, $c \in \mathbb{Z}$ e $d = (a, b)$. A equação*

$$ax + by = c \qquad \textit{(nas incógnitas inteiras } x, y\textit{)}$$

tem solução se e só se d divide c.

Além disso, se x_0, y_0 são tais que $ax_0+by_0 = c$ então a solução geral da equação $ax+by = c$ é

$$\begin{cases} x &= x_0 + \frac{b}{d}\, t \\ y &= y_0 - \frac{a}{d}\, t, \quad \text{com } t \in \mathbb{Z}. \end{cases}$$

Demonstração. Se a ou b é igual a 0 o resultado é imediato. Vejamos o caso em que $a \neq 0 \neq b$.

Para a primeira parte do teorema.

$\Rightarrow$

Suponhamos que a equação tem solução e sejam $x, y \in \mathbb{Z}$ tais que $ax + by = c$. Então $d \big| ax$ e $d|by$ (porque $d \big| a$ e $d \big| b$) e, portanto $d \big| ax + by = c$.

$\Leftarrow$

Suponhamos que $d \big| c$ e seja $\gamma \in \mathbb{Z}$ tal que $c = d\gamma$. Usando o Teorema 2.4, sejam $\alpha, \beta \in \mathbb{Z}$ tais que $a\alpha+b\beta = d$. Multiplicando esta última igualdade por γ obtemos $a\,(\alpha\,\gamma)+b\,(\beta\,\gamma) = c$, o que mostra que a equação $ax + by = c$ admite solução.

Para a segunda parte do teorema.

Suponhamos que a equação tem solução x_0, y_0 tais que $ax_0 + by_0 = c$. Então, se $t \in \mathbb{Z}$,

$$a(x_0 + \frac{b}{d}\, t) + b(y_0 - \frac{a}{d}\, t) = ax_0 + \frac{ab}{d}\, t + by_0 - \frac{ab}{d}\, t = ax_0 + by_0 = c,$$

o que mostra que $x = x_0 + \frac{b}{d}\, t$, $y = y_0 - \frac{b}{d}\, t$ é solução da equação.

Vamos agora mostrar que, se $x, y \in \mathbb{Z}$ são tais que $ax + by = c$, então x, y são da forma pretendida. Sejam $A = \frac{a}{d}$, $B = \frac{b}{d}$ e $C = \frac{c}{d}$. Note-se que

$$\left\{\begin{array}{rcl} ax+by & = & c \\ ax_0+by_0 & = & c \end{array}\right. \iff \left\{\begin{array}{rcl} A\,x+B\,y & = & C \\ A\,x_0+B\,y_0 & = & C \end{array}\right. \implies A\,(x-x_0) = -B\,(y-y_0).$$

Deste modo B divide $A\,(x-x_0)$. Uma vez que $(A,B)=1$ podemos concluir, usando a Proposição 2.5, que B divide $(x-x_0)$ e portanto existe $t\in\mathbb{Z}$ tal que $x-x_0 = B\,t$. Substituindo na igualdade $A\,(x-x_0) = -B\,(y-y_0)$ obtemos $AB\,t = -B\,(y-y_0)$ ou seja $y-y_0 = -A\,t$. Conclusão, existe $t\in\mathbb{Z}$ tal que

$$\left\{\begin{array}{rcl} x & = & x_0+B\,t \\ y & = & y_0-A\,t. \end{array}\right.$$

□

Voltemos ao Exemplo 5.1. Uma vez que a equação $15x+7y=17$ tem como solução $x=3$, $y=-4$ (por exemplo), para pagar 17 cêntimos, basta pagar com 3 moedas de 15 cêntimos e receber de troco 4 moedas de 7 cêntimos. Outra hipótese seria pagar com 11 moedas de 7 cêntimos e receber de troco 4 moedas de 15 cêntimos. É claro que o teorema anterior dá-nos um método de encontrar todas as soluções possíveis, que são em número infinito.

Nota 5.4. *Note-se que se encontrarmos, por algum meio (tentativas, observação, algum meio sistemático), uma solução de uma equação do tipo $ax+by=c$ então podemos sempre encontrar* **todas** *as soluções dessa equação.*

Vamos agora mostrar, com um exemplo, outro meio de encontrar uma solução (quando existe) de uma equação diofantina da forma $ax+by=c$ em que (a,b) divide c (pois caso contrário a equação não tem solução). A primeira coisa a fazer é simplificar a equação, dividindo ambos os membros por (a,b), obtendo assim uma equação do tipo $Ax+By=C$ em que $(A,B)=1$.

Exemplo 5.5. *Consideremos a equação $15x+41y=27$. Recordo que basta encontrar uma solução.*

Começamos por isolar a variável cujo coeficiente tem menor valor absoluto. Obtemos

$$x = \frac{27-41y}{15}.$$

Utilizando o algoritmo da divisão ($27 = 1\times 15+12$ e $41 = 2\times 15+11$) obtemos

$$x = 1-2y+\frac{12-11y}{15}.$$

Daqui podemos concluir que y tem de ser tal que $\dfrac{12-11y}{15}\in\mathbb{Z}$. Ou encontramos um valor de y nestas condições e depois tiramos o valor de x correspondente, ou procuramos $z\in\mathbb{Z}$ tal que $\dfrac{12-11y}{15} = z$, ou seja, tal que $11y+15z=12$ (obtemos assim uma equação do mesmo tipo da anterior, mas cujos coeficientes tem menor valor absoluto).

Fazendo a esta equação o mesmo que foi feito para a anterior obtemos

$$y = 1 - z + \frac{1-4z}{11}.$$

Procuramos agora $z \in \mathbb{Z}$ tal que $\frac{1-4z}{11}$ seja um número inteiro, por exemplo $z = 3$ (que implica $y = -3$ e $x = 10$) ou $z = -8$ (que implica $y = 12$ e $x = -31$).

Se não conseguíssemos encontrar rapidamente um valor de z tal que $\frac{1-4z}{11} \in \mathbb{Z}$, repetíamos o processo, isto é, escreveríamos $\frac{1-4z}{11} = w$ e tentaríamos resolver esta nova equação. Teríamos assim: $11w + 4z = 1$ e portanto $z = -2w + \frac{1-3w}{4}$, etc..

É o algoritmo de Euclides! que nos garante que este processo termina. O menor dos coeficientes (em módulo) de uma das equações que encontramos é sempre estritamente menor que o menor dos coeficientes (em módulo) da equação anterior. Note-se que em cada uma das equações o máximo divisor comum dos coeficientes ser sempre igual a 1. Deste modo, mais cedo ou mais tarde esse coeficiente é igual a ± 1 e, nesse caso é sempre trivial encontrar uma solução.

Uma pequena observação: voltando ao início, quando tínhamos a igualdade $x = \frac{27-41y}{15}$, poderíamos ter optado por escrever $x = 2 - 3y + \frac{-3+4y}{15}$, o que, em princípio, iria simplificar as contas.

6. Congruências lineares de ordem 1

Nesta secção pretendemos resolver congruências lineares de ordem 1. Dito de outro modo, pretende-se encontrar os valores $x \in \mathbb{Z}$ tais que

$$ax \equiv_n b, \qquad \text{em que } a, b \in \mathbb{Z} \text{ e } n \in \mathbb{N} \text{ são dados à partida.}$$

Uma vez que, se x_0 é solução da equação, então $x_0 + nt$ (com $t \in \mathbb{Z}$) também é, só precisamos de encontrar as soluções no conjunto $\{0, 1, \ldots, n-1\}$, por exemplo. Assim, qualquer congruência deste tipo, ou não tem solução ou tem uma infinidade de soluções.

Por abuso de notação quando dissermos que a congruência tem k soluções, estaremos a subentender, que essas soluções são incongruentes módulo n.

Por exemplo, a equação $4x \equiv_8 0$ tem duas soluções (incongruentes módulo 8): $x \equiv_8 0$ e $x \equiv_8 2$.

Vamos então ver que estas congruências podem ser resolvidas usando o que sabemos sobre equações diofantinas.

Se $a \equiv_n 0$ a congruência é de resolução trivial, tendo n ou 0 soluções consoante b é ou não congruente com 0 módulo n.

Teorema 6.1. *Sejam $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ tais que $a \not\equiv_n 0$. Se $d = (a, n)$ então a congruência $ax \equiv_n b$ tem solução se e só se $d \big| b$.*

Além disso, se $d \big| n$ e x_0 é uma solução da congruência então a solução geral é dada por:

$$x = x_0 + \frac{n}{d}\, t \quad \textit{com } t \in \mathbb{Z}.$$

Em particular, existem d soluções (incongruentes módulo n), por exemplo:

$$\left\{ x_0 + \frac{n}{d}\, t : \quad t \in \{0, 1, \ldots, d-1\} \right\}.$$

Demonstração. Para a primeira parte basta notar que,

$$\begin{aligned} \exists\, x \in \mathbb{Z} : \quad ax \equiv_n b \quad &\Leftrightarrow \quad \exists\, x \in \mathbb{Z} : \quad n \big| ax - b \\ &\Leftrightarrow \quad \exists\, x \in \mathbb{Z}\ \exists\, y \in \mathbb{Z} : ax - b = ny \\ &\Leftrightarrow \quad \exists\, x, y \in \mathbb{Z} : ax - ny = b \\ &\Leftrightarrow \quad d \big| b, \text{ pelo Teorema 5.3.} \end{aligned}$$

A segunda parte do teorema é uma consequência imediata do Teorema 5.3. □

Corolário 6.2. *Se $a \in \mathbb{Z}$, $n \in \mathbb{N}$ e $(a, n) = 1$ então:*

a) existe $d \in \mathbb{Z}$ tal que $ad \equiv_n 1$;

b) (lei do corte) se $b, c \in \mathbb{Z}$ e $ac \equiv_n ab$ então $b \equiv_n c$.

Demonstração. Como $(a, n) = 1$ então a congruência $ax \equiv_n 1$ tem solução, pelo teorema anterior, ou seja, existe $d \in \mathbb{Z}$ tal que $ad \equiv_n 1$.

Para alínea b) basta notar que nas condições referidas, se d é tal que $ad \equiv_n 1$ então $dac \equiv_n dab$, usando a Proposição 4.2, ou seja $b \equiv_n c$. □

Se $ad \equiv_n 1$ dizemos que d é o *inverso*, módulo n, de a.

Note-se que, se $(a, n) \neq 1$, $b = n$ e $c = \frac{n}{(a,n)}$ (por exemplo) então

$$ab \equiv_n ac \text{ e } b \not\equiv_n c.$$

De qualquer modo podemos sempre "simplificar" a congruência.

Proposição 6.3. *Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$ tais que $a \equiv b \pmod{n}$. Nestas condições, se d é um inteiro que divide a e n então d divide b e $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.*

Demonstração. Sejam $k \in \mathbb{Z}$ tal que $a - b = kn$ e d um divisor de a e n. Então d divide b (porque $b = a - kn$) $\frac{a}{d} - \frac{b}{d} = k\,\frac{n}{d}$ e, portanto $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. □

Observações:

- se n for um número "pequeno", o método das tentativas é, por vezes, o método mais rápido para resolver a congruência $ax \equiv b \pmod{n}$;
- se $n = p_1^{n_1} \cdots p_k^{n_k}$ e $A, B \in \mathbb{Z}$, então, usando o Teorema 2.11,

$$A \equiv B \ (\mathrm{mod}\ n) \iff \forall i \in \{1, \ldots, k\} \quad A \equiv B \ (\mathrm{mod}\ p_i^{n_i});$$

- como consequência da observação anterior, a resolução da congruência $ax \equiv b \ (\mathrm{mod}\ n)$ é equivalente à resolução do sistema

$$\begin{cases} ax & \equiv & b \ (\mathrm{mod}\ p_1^{n_1}) \\ & \ddots & \\ ax & \equiv & b \ (\mathrm{mod}\ p_k^{n_k}). \end{cases}$$

Suponhamos que queremos resolver a congruência $3x \equiv 4 \pmod{2020}$. Pelo Teorema 6.1 já sabemos que esta congruência tem uma só solução módulo 2020. Deste modo, logo que encontrarmos uma solução podemos parar de procurar outras. Para encontrar uma solução podemos usar vários métodos:

- por tentativas verificar se cada um dos inteiros de $\{0, 1, \ldots, 2019\}$ é solução da congruência;
- multiplicar a congruência pelo inverso de 3 módulo 2020. Se d for esse inverso então obtemos $x \equiv 4\,d \pmod{2020}$ e portanto a solução geral é $x = 4\,d + 2020\,t$, com $t \in \mathbb{Z}$;
- "passar" esta congruência para uma equação diofantina e resolvê-la pelos métodos já descritos anteriormente;
- notar que $2020 = 4 \times 5 \times 101$ e resolver o sistema

$$\begin{cases} 3x & \equiv & 4 \ (\mathrm{mod}\ 4) \\ 3x & \equiv & 4 \ (\mathrm{mod}\ 5) \\ 3x & \equiv & 4 \ (\mathrm{mod}\ 101). \end{cases}$$

Note-se que cada uma das congruências deste sistema pode ser resolvida usando os métodos anteriores. Em princípio o método das tentativa é o melhor para resolver as duas primeiras congruências. Em relação à terceira talvez o mais fácil seja notar que $3 \times 34 = 102 \equiv 1 \ (\mathrm{mod}\ 101)$ e, portanto, a congruência é equivalente a $x \equiv 146 \equiv 45 \pmod{101}$. É claro que aquilo que se pede é a resolução do sistema e não (apenas) a resolução de cada uma das congruências.

6.1. **Teorema chinês dos restos.**

O chamado Teorema Chinês dos Restos (Sec V) dá um método sistemático de resolução de sistemas de congruências do tipo $ax \equiv b \pmod{n}$. Aparentemente a ideia surgiu com a necessidade de contar o número de soldados numa parada. Suponhamos que sabemos que o número de soldados é no máximo 1000. Mandamos ordenar os soldados em filas de 7 e

depois em filas de 11 e depois em filas de 13 (o que é mais simples do que contar os soldados) e contamos o número de soldados que sobraram. Suponhamos que esses números foram 6, 5 e 3. Estamos assim perante o sistema,

$$\begin{cases} x & \equiv & 6 \ (\mod 7) \\ x & \equiv & 5 \ (\mod 11) \\ x & \equiv & 3 \ (\mod 13) \end{cases}$$

cuja solução é $x \equiv 874 \pmod{1001}$ (note-se que $7 \times 11 \times 13 = 1001$). Deste modo existe $k \in \mathbb{Z}$ tal que o número de soldados é $874 + 1001\,k$. Como o número pretendido é no máximo 1000 podemos concluir que existem 874 soldados na parada.

Recorda-se que uma congruência do tipo $ax \equiv b \pmod{n}$ é impossível se (a, n) não divide b ou é equivalente a uma congruência do tipo $x \equiv c \pmod{m}$ (em que $m = \frac{n}{(a,n)}$) caso contrário. Resta-nos assim considerar sistemas em que todas as congruências da forma

$$\begin{cases} x & \equiv & a_1 \ (\mod n_1) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

Um modo de resolver este sistema é usar o seguinte raciocínio:

$$\begin{cases} x & \equiv & a_1 \ (\mod n_1) \\ x & \equiv & a_2 \ (\mod n_2) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases} \Leftrightarrow \begin{cases} x & = & a_1 + n_1\,t \ \text{ para algum } t \in \mathbb{Z} \\ x & \equiv & a_2 \ (\mod n_2) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

De seguida substituímos o valor de x encontrado na primeira congruência e substituímos nas outras, obtendo assim um sistema de $k-1$ congruências na incógnita t

$$\begin{cases} n_1\,t & \equiv & a_2 - a_1 \ (\mod n_2) \\ & \ddots & \\ n_1\,t & \equiv & a_k - a_1 \ (\mod n_k) \end{cases}$$

Note-se que a congruência i tem solução se e só se $(n_1, n_i) | (a_i - a_1)$. Podemos agora repetir o processo resolvendo uma das congruências e substituindo a solução geral nas outras congruências. É claro que se o sistema original tiver apenas duas congruências então o sistema tem solução se e só se $(n_1, n_2) | (a_2 - a_1)$. No caso geral temos o chamado teorema chinês dos restos que nos diz quando é que o sistema tem solução e como encontrar todas as soluções depois de descobrirmos uma delas. Não vamos demonstrar este teorema embora seja mais ou menos claro que a sua demonstração usa o que já foi feito no caso em que temos um sistema de duas congruências e um argumento indutivo.

Teorema 6.4 (Teorema Chinês dos Restos)**.** *Se $k \in \mathbb{N}\setminus\{1\}$, $a_1, \ldots, a_k \in \mathbb{Z}$ e $n_1, \ldots, n_k \in \mathbb{N}$ então o sistema,*

$$\begin{cases} x & \equiv & a_1 \ (\mod n_1) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

tem solução se e só se, para todo $i, j \in \{1, \ldots, k\}$, $(n_i, n_j) \big| a_j - a_i$.

Além disso, se x_0 for uma solução do sistema, então a solução geral é dada por

$$x = x_0 + [n_1, \ldots, n_k]\, t, \quad t \in \mathbb{Z}.$$

Em particular, se o sistema tiver solução, ele admite uma só solução módulo $[n_1, \ldots, n_k]$.

□

É claro que há situações em que a descoberta de uma solução do sistema ou de parte dele é trivial. Nestes casos a resolução completa do sistema fica muito simplificada uma vez que se encontrarmos uma solução então saberemos quais são todas as soluções.

Vejamos um exemplo: quais os números inteiros positivos que divididos por $2, 3, 4, 5, 6$ dão resto $1, 2, 3, 4, 5$ (respectivamente)? A resolução deste problema conduz-nos (provavelmente) à resolução do sistema, com $x \in \mathbb{N}$,

$$\begin{cases} x & \equiv & 1 \ (\mod 2) \\ x & \equiv & 2 \ (\mod 3) \\ x & \equiv & 3 \ (\mod 4) \\ x & \equiv & 4 \ (\mod 5) \\ x & \equiv & 5 \ (\mod 6). \end{cases}$$

É claro que, se D for um múltiplo comum a 2, 3, 4, 5 e 6, e se x_0 for uma solução, então $x = x_0 + Dt$ com $t \in \mathbb{Z}$ é também uma solução do sistema (se a incógnita pertencer a $\mathbb{Z}$). Assim basta-nos procurar soluções no conjunto $\{0, 1, \ldots, D-1\}$. Evidentemente que, neste exemplo o mais natural será considerar $D = 60$, porque 60 é o mínimo múltiplo comum dos inteiros 2, 3, 4, 5 e 6.

Se olharmos para este sistema de outro modo, por exemplo,

$$\begin{cases} x & \equiv & -1 \ (\mod 2) \\ x & \equiv & -1 \ (\mod 3) \\ x & \equiv & -1 \ (\mod 4) \\ x & \equiv & -1 \ (\mod 5) \\ x & \equiv & -1 \ (\mod 6) \end{cases}$$

encontramos facilmente uma solução em $\mathbb{Z}$: $x = -1$. Pelo que foi dito atrás, se somarmos a -1 um múltiplo de 60 obtemos soluções do sistema que estão naturalmente em $\mathbb{N}$.

Usando este teorema e o que já fizemos atrás, podemos concluir que os números inteiros positivos que divididos por $2, 3, 4, 5, 6$ dão resto $1, 2, 3, 4, 5$ (respectivamente) são os números da forma

$$x \quad = \quad -1 + 60\,t \quad t \in \mathbb{N}.$$

Exercícios

É claro que podemos sempre facilmente arranjar exercícios para treinar a resolução de equações diofantinas, de congruências lineares de ordem 1 e de sistemas de congruências lineares de ordem 1 escolhendo os parâmetros "à sorte".

1) Resolva as equações (com $x, y \in \mathbb{Z}$):
   a) $3x + y = 13$;
   b) $3x - 12y = 13$;
   c) $11x + 7y = 200$;
   d) $153x + 27y = 13$;
   e) $3x - 201y = 133$.
2) No exercício anterior quais das equações admitem soluções com $x, y \in \mathbb{N}$?
3) Temos duas balanças: uma que marca pesos múltiplos de 10 e outra que marca pesos múltiplos de 13. Como é que com essas balanças podemos pesar 107 gramas?
4) Apenas com a utilização de dois relógios que só dão intervalos de tempo de 5 e de 11 minutos como podemos cozer um ovo durante 3 minutos?
5) Se 11 laranjas e 18 limões custam 376 cêntimos quanto custa cada laranja e cada limão?
6) Compramos, por 568 cêntimos maças e laranjas num total de 12 peças de fruta. Se uma maça custa mais 10 cêntimos do que uma laranja, quantas maças compramos?
7) Mostre que duas progressões aritméticas $a, a+d, a+2d, \ldots$ e $b, b+c, b+2c, \ldots$ (com $a, b, c, d \in \mathbb{Z}$) têm termos em comum se e só se (d, c) divide $a - b$.
8) Calcule os inversos, módulo 13 de 5, 7 e 23.
9) Resolva as congruências:
   a) $23x \equiv 7 \pmod{19}$;
   b) $6x \equiv -2 \pmod{28}$;
   c) $25x \equiv 15 \pmod{120}$;
   d) $15x \equiv 9 \pmod{25}$.

10) Seja $p \in \mathbb{P}$ e $a \in \mathbb{Z}$ tal que $(a, p) = 1$. Mostre que todo o inteiro é congruente módulo p com algum inteiro da forma ka, com $k \in \{0, 1, \ldots, p-1\}$.
11) Verifique se existem $x, y \in \mathbb{N}$ tais que $101x + 37y = 3819$.
12) Para que valores de $x, y \in \mathbb{Z}$:
    a) $372x + 420y = 36$;
    b) $234x - 151y = 44$ e $5x + 6y$ é múltiplo de 7;
    c) $120x + 63y = 12$ e $3x + 6y$ é múltiplo de 11.
13) Resolva as equações:
    a) $15x + 21y + 35z = 0$;
    b) $15x + 21y + 35z = 1$.
14) Seja k um inteiro positivo. Considere a equação
$$(k+2)x + 6y = 3, \qquad x, y \in \mathbb{Z}.$$
    a) Para que valores de $k \in \mathbb{Z}$, a equação admite solução?
    b) Escolha $k > 10$ nas condições da alínea (a) e encontre uma solução da equação tal que $x > 1000$ e $y < -1000$.
    c) Fixado k, mostre que, se x_0, y_0 é uma solução da equação $(k+2)x + 6y = 3$ então (x_0, y_0) divide 3.
15) Para que valores de $x, y \in \mathbb{Z} \setminus \{0\}$ se tem $\dfrac{x+y}{xy} \in \mathbb{Z}$?
16) Resolva a equação
$$\frac{1}{x} + \frac{1}{y} = \frac{1}{13}, \quad x, y \in \mathbb{Z} \setminus \{0\}.$$
17) Resolva a equação $(6x + 15y)(8x + 7y) = 129, \quad x, y \in \mathbb{Z}$.
18) Estude a congruência $(a^2 + a + 1)x \equiv 2\,a + 1 \pmod{a+2}$. Escolha o menor inteiro positivo a para o qual a congruência tenha mais que uma solução. Em seguida resolva a equação.
19) Para que valores de $a, b \in \mathbb{Z}$ a congruência
$$(6a^2 - a - 5)x \equiv 3\,a + b \ (\bmod 2\,a + 3)$$
tem mais que uma solução módulo $2\,a + 3$?

    Escolha $a, b \in \mathbb{Z}$ tais que a congruência tenha mais do que uma solução, com $a \geq 20$, e resolva a congruência.
20) Determine as soluções de:

a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases}$ b) $\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 4 \pmod{17} \\ x \equiv 10 \pmod{25} \end{cases}$

c) $\begin{cases} x \equiv 1 \pmod{m} \\ x \equiv 1 \pmod{n} \\ x \equiv 1 \pmod{k} \\ x \in \mathbb{Z} \setminus \{1\}. \end{cases}$

d) $\begin{cases} x & \equiv & 1 \pmod{11} \\ x & \equiv & 1 \pmod{13} \\ x & \equiv & 1 \pmod{6} \\ x & \in & [34\,000, 34\,300] \end{cases}$

21) Quais os dois menores inteiros positivos que divididos por 3, 5 e 7 dão restos 2, 3 e 2 respectivamente?

22) Quantas soluções em inteiros positivos tem a equação diofantinas $8x + 9y = 43$?

23) Encontre um inteiro c tal que a equação diofantina $10x + 11y = c$ tem exactamente 9 soluções positivas.

7. Teorema de Euler

Sejam $n \in \mathbb{N}$ e $a \in \mathbb{Z}$ tais que $(a, n) = 1$. Consideremos os restos da divisão por n das potências de a. Como existem n possibilidades para esses restos podemos concluir que existem $n_1, n_2 \in \mathbb{N}_0$ tais que $n_1 < n_2$ e $a^{n_2} \equiv a^{n_1} \pmod{n}$ ou seja $a^{n_2-n_1} \cdot a^{n_1} \equiv 1 \cdot a^{n_1} \pmod{n}$. Aplicando a lei do corte obtemos $a^s \equiv 1 \pmod{n}$, se $s = n_2 - n_1 \in \mathbb{N}$. Seja agora $k \in \mathbb{N}$. Aplicando o algoritmo da divisão existem $r \in \{0, 1, \ldots, s-1\}$ e $q \in \mathbb{N}_0$ tais que $k = qs + r$. Deste modo

$$a^k \;=\; a^{qs+r} = (a^s)^q \cdot a^r \equiv a^r \pmod{n}.$$

Concluímos assim que toda a potência de a é congruente módulo n com alguma potência de a de expoente menor do que s.

Exemplo 7.1. *Qual o último algarismo do número 7^{34}? E de $7^{31^{14}}$?*

O que se pretende é saber qual o resto da divisão de 7^{34} e de $7^{31^{14}}$ por 10. Utilizando o método acima descrito e fazendo alguns (poucos) cálculos concluímos que $7^4 \equiv 1 \pmod{10}$.

Resta-nos agora encontrar o resto da divisão de 34 e de 31^{14} por 4. No primeiro caso a resposta é 2 e portanto, $7^{34} \equiv 7^2 \equiv 9 \pmod{10}$. Para o segundo caso observamos que

$$\begin{aligned} 31^{14} &\equiv 3^{14} \pmod{4} && \text{porque } 31 \equiv 3 \pmod{4} \\ &\equiv 1 \pmod{4} && \text{porque } 3^2 \equiv 1 \pmod{4}. \end{aligned}$$

Assim, $7^{34} \equiv 7 \pmod{10}$.

O que vamos fazer de seguida é dar um método para encontrar, dado $n \in \mathbb{N}$ e $a \in \mathbb{Z}$ tal que $(a, n) = 1$, uma potência de a de expoente positivo que seja congruente com 1 módulo n.

Definição 7.2. *Chama-se* **função de Euler** *à função* $\varphi : \mathbb{N} \to \mathbb{N}$ *definida por*

$$\forall n \in \mathbb{N} \quad \varphi(n) = \Big|\{x \in \mathbb{N} : 1 \leq x \leq n,\ (x,n) = 1\}\Big|.$$

Por exemplo,

- $\varphi(1) = \varphi(2) = 1$;
- $\varphi(5) = \varphi(8) = \varphi(10) = \varphi(12) = 4$;
- $\varphi(p) = p - 1$, se p é primo;
- se $n \geq 2$ e n não é primo, então $\varphi(n) < n - 1$, porque se p é um divisor primo de n, então $(p, n) \neq 1$.

Estamos agora em condições de enunciar e demonstrar o chamado Teorema de Euler.

Teorema 7.3 (Teorema de Euler)**.** *Se* $n \in \mathbb{N}$, $a \in \mathbb{Z}$ *e* $(a, n) = 1$ *então*

$$a^{\varphi(n)} \equiv 1 \ (\bmod n).$$

Demonstração. O conjunto $\{x \in \mathbb{N} : 1 \leq x \leq n,\ (x,n) = 1\}$ é formado por $\varphi(n)$ elementos que denotaremos por $x_1, x_2, \ldots, x_{\varphi(n)}$. Para cada i, seja r_i o resto da divisão de $x_i a$ por n. Note-se que, usando a lei do corte, se $x_i a \equiv x_k a \pmod n$ então $x_i = x_k$. Como $(x_i a, n) = (r, n) = 1$ podemos concluir que existe j tal que $r_i = x_j$ e, portanto $x_i a \equiv x_j \pmod n$. Mostramos assim que

$$\forall i \in \{1, 2, \ldots, \varphi(n)\}\ \exists! j \in \{1, 2, \ldots, \varphi(n)\} :\ x_i a \equiv x_j \ (\bmod n).$$

Em particular

$$\prod_{i \leq \varphi(n)} x_i \ \equiv \ \prod_{i \leq \varphi(n)} x_i a \ (\bmod n) \qquad \text{ou seja} \qquad 1 \cdot \prod_{i \leq \varphi(n)} x_i \ \equiv \ a^{\varphi(n)} \prod_{i \leq \varphi(n)} x_i \ (\bmod n).$$

Usando a lei do corte concluímos que $a^{\varphi(n)} \equiv 1 \pmod n$. □

Vejamos algumas consequências imediatas.

Corolário 7.4 (Pequeno Teorema de Fermat)**.** *Se* a *é um número inteiro e* p *é um número primo que não divide* a*, então* $a^{p-1} \equiv 1 \pmod p$.

Demonstração. Basta usar o teorema de Euler notando que $\varphi(p) = p - 1$. □

Corolário 7.5. *Se* a *é um número inteiro e* p *é um número primo então* $a^p \equiv a \pmod p$.

Demonstração. Se p divide a então $a \equiv 0 \pmod p$ e portanto $a^k \equiv 0 \pmod p$ qualquer que seja $k \in \mathbb{N}$. Em particular $a^p \equiv a \pmod p$.

Se p não divide a então pelo corolário anterior $a^{p-1} \equiv 1 \pmod p$. Multiplicando por a obtemos o resultado pretendido. □

Corolário 7.6. *Sejam $n \in \mathbb{N}$, $m, k \in \mathbb{N}_0$ e $a, b \in \mathbb{Z}$.*
Se $(a, n) = 1$, $m \equiv k \pmod{\varphi(n)}$ e $a \equiv b \pmod{n}$ então $a^m \equiv b^k \pmod{n}$.

Demonstração. Basta considerar o caso em que $m > k$.
Como $m \equiv k \pmod{\varphi(n)}$ existe $q \in \mathbb{N}$ tal que $m - k = q\,\varphi(n)$ e, portanto,

$$a^m \equiv_n b^m \pmod{n} = b^{k+q\,\varphi(n)} = b^k \left(b^{\varphi(n)}\right)^q \equiv_n b^k$$

usando a Proposição 4.2 e o Teorema de Euler. □

Por exemplo, se quisermos encontrar o resto da divisão de 2351^{1000} por 18 podemos seguir o seguinte raciocínio (notando que $(2351, 18) = 1$ e $\varphi(18) = 6$)

- como $2351 \equiv 11 \pmod{18}$ e $1000 \equiv 4 \pmod{6}$ temos $2351^{1000} \equiv 11^4 \pmod{18}$;
- como $11^2 = 121 \equiv 13 \pmod{18}$ e $11^4 \equiv 13^2 \equiv 7 \pmod{18}$ concluímos que o resto da divisão de 2351^{1000} por 18 é igual a 7.

Resta-nos agora encontrar uma fórmula para o cálculo de φ.

Lema 7.7. *Se p é um número primo e $k \in \mathbb{N}$,*

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Demonstração. Comecemos por notar que um número $(a, p^k) = 1$ se e só se p não divide a. Assim

$$\left\{a \in \mathbb{N} : 1 \leq a \leq p^k,\ (a, p^k) \neq 1\right\} = \left\{a \in \mathbb{N} : 1 \leq a \leq p^k,\ p \middle| a\right\} = \left\{p\,m : 1 \leq m \leq p^{k-1}\right\}.$$

Em particular $\left|\{a \in \mathbb{N} : 1 \leq a \leq p^k,\ (a, p^k) \neq 1\}\right| = p^{k-1}$ e portanto $\varphi(p^k) = p^k - p^{k-1}$. □

Como exemplo: $\varphi(121) = 11 \times 10 = 110$.

Proposição 7.8. *A função de Euler satisfaz a condição*

$$\forall m, n \in \mathbb{N}\ [(n, m) = 1\ \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)].$$

Demonstração. Sejam $m, n \in \mathbb{N}$ com $(m, n) = 1$. Vamos mostrar que no conjunto $\{1, 2, \ldots, mn\}$ existem $\varphi(n)\varphi(m)$ elementos primos com mn.

Começamos por notar que um número é primo com nm se e só se for primo com n e com m. De seguida dispomos os números $1, 2, \ldots, mn$ numa tabela de m linhas e n colunas;

linha 1	1	m+1	2m+1	$\cdots$	(n-1)m+1
linha 2	2	m+2	2m+2	$\cdots$	(n-1)m+2
linha 3	3	m+3	2m+3	$\cdots$	(n-1)m+3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
linha m	m	m+m	2m+m	$\cdots$	(n-1)m+m

Um elemento genérico da linha i é um elemento da forma $km + i$, com $0 \leq k \leq m$ e $1 \leq i \leq n$. Deste modo $(km + i, m) = (i, m)$ e, portanto os números da tabela que são primos com m são todos que os que pertencem a uma linha i, sendo $(i, m) = 1$. Note-se que existem $\varphi(m)$ linhas nestas condições.

Vamos agora ver quantos dos n elementos de uma dada linha i são primos com n. Usando a lei do corte podemos mostrar que

$$\forall k \in \{0, 1, \ldots, n-1\}\ \exists!\, j_k \in \{0, 1, \ldots, n-1\} :\ km + i \equiv j_k \ (\bmod n).$$

Com esta notação, como $(km + i, n) = (j_k, n)$, podemos concluir que $(km + i, n) = 1$, ou seja $(j_k, n) = 1$, para exactamente $\varphi(n)$ valores de k. Concluímos assim que um número pertencente a $\{1, 2, \ldots, nm\}$ é primo com nm se e só se for um dos $\varphi(n)$ elementos da linha i em que $(i, m) = 1$. Deste modo $\varphi(nm) = \varphi(n)\varphi(m)$. □

Como corolário deste teorema e do Lema 7.7, temos uma fórmula para o cálculo de $\varphi(n)$, se $n \in \mathbb{N}$.

Teorema 7.9. *Se $n = p_1^{n_1} \cdots p_k^{n_k}$, em que $p_1, \ldots, p_k$ são números primos distintos, e $n_1, \ldots, n_k \in \mathbb{N}$ então,*

$$\varphi(n) \ = \ (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_k^{n_k} - p_k^{n_k-1}) \ = \ p_1^{n_1-1} \cdots p_k^{n_k-1}(p_1 - 1) \cdots (p_k - 1).$$

Demonstração. Por aplicação sucessiva da proposição anterior temos

$$\varphi(n) \ = \ \varphi(p_1^{n_1}) \cdots \varphi(p_k^{n_k}).$$

A conclusão segue agora do Lema 7.7. □

Exemplos 7.10. $\varphi(253) = \varphi(11 \times 23) = 10 \times 22 = 220$, $\varphi(100) = \varphi(2^2 \times 5^2) = 2 \times 5 \times 4 = 40$.

7.1. **Pseudoprimos.**

Existem inteiros positivos n, que não são primos e que verificam a conclusão do Pequeno Teorema de Fermat. Por exemplo, se $n = 561$ $(= 3 \times 11 \times 17)$ e a é um inteiro qualquer

primo com 561 então

$$\begin{aligned} a^{560} &\equiv 1 \ (\bmod 3) && \text{porque } \varphi(3) \text{ divide } 560 \\ a^{560} &\equiv 1 \ (\bmod 11) && \text{porque } \varphi(11) \text{ divide } 560 \\ a^{560} &\equiv 1 \ (\bmod 17) && \text{porque } \varphi(17) \text{ divide } 560 \end{aligned}$$

e portanto $a^{560} \equiv 1 \pmod{560}$.

Chegamos assim à seguinte definição.

Definição 7.11. *Um inteiro composto n diz-se um* **pseudoprimo** *se:*

$$\forall a \in \mathbb{N} \ \left[(a,n) = 1 \ \Rightarrow \ a^{n-1} \equiv 1 \ (\bmod n)\right].$$

Os pseudoprimos são raros:

- menores que 100 000 são apenas: 561, 1 105, 1 729, 2 465, 2 821, 6 601, 8 911, 10 585, 15 841, 29 341, 41 041, 46 657, 52 633, 62 745, 63 973 e 75 361;
- existem apenas 2 163 que são menores que 25 000 000 000;
- existem apenas 246 683 que são menores que 10 000 000 000 000 000.

Apenas em 1994 foi demonstrado que existe um número infinito de pseudoprimos. Referência:W. R. Alford, A. Granville and C. Pomerance, "There are infinitely many Carmichael numbers," Ann. of Math., 140 (1994) 703-722.

Para mais resultados sobre pseudoprimos ver, por exemplo,
http://www.utm.edu/research/primes/glossary/CarmichaelNumber.html

Os argumentos que usamos para mostrar que o número 561 era pseudoprimo podem ser usados para mostrar a seguinte proposição.

Proposição 7.12. *Seja $n = p_1 \cdots p_k$ com $k \geq 2$ e $p_1, \ldots, p_k$ números primos distintos, tais que*

$$\forall i \leq k \quad (p_i - 1) | (n-1).$$

Então n é um pseudoprimo. □

De facto é verdade que todos os pseudoprimos são da forma referida nesta proposição.

Exemplos 7.13. *A título de curiosidade, os menores pseudoprimos com k factores primos distintos são:*

- $561 = 3 \times 11 \times 17$, *se $k = 3$;*
- $41\,041 = 7 \times 11 \times 13 \times 41$, *se $k = 4$;*
- $825\,265 = 5 \times 7 \times 17 \times 19 \times 73$, *se $k = 5$;*
- $321\,197\,185 = 5 \times 19 \times 23 \times 29 \times 37 \times 137$, *se $k = 6$.*

Exercício 7.14. *Mostre que, se $k \in \mathbb{N}$ é tal que $6k+1$, $12k+1$, $18k+1$ são números primos, então $(6k+1)(12k+1)(18k+1)$ é um pseudoprimo.*

Apenas a título de curiosidade, um número composto n diz-se um **pseudoprimo de base** a se $a^{n-1} \equiv 1 \pmod{n}$. Assim, um inteiro n é um pseudoprimo se for pseudoprimo de base a, para todo a, primo com n.

Exemplos 7.15. *Vejamos alguns exemplos de pseudoprimos nas bases 2 e 3;*

- *na base 2:* 341, 561, 645, 1105, 1387, 1729, 1905, 915981, 916327, 934021, 950797, 976873, 983401, 997633*;*
- *na base 3:* 954577, 962809, 966301, 973241, 992251, 994507, 997633

Contrariamente ao que acontece para os pseudoprimos, é muito fácil (comparativamente) mostrar que existe uma infinidade de pseudoprimos de base a (com $a \in \mathbb{N}$). Por exemplo, pode-se mostrar que, se n é um pseudoprimo ímpar de base 2, então $2^n - 1$ é também um pseudoprimo ímpar de base 2, que naturalmente é maior do que n. Deste modo, como 341 é um pseudoprimo ímpar de base 2 então os elementos da sucessão $(x_n)_{n\in\mathbb{N}}$ em que

$$x_1 = 341, \quad x_{n+1} = 2^{x_n} - 1.$$

são pseudoprimos de base 2.

Se a é qualquer pode-se mostrar que os números da forma $m = \frac{a^{2p}-1}{a^2-1}$, em que p é um número primo que não divide $a(a^2-1)$ são pseudoprimos de base a. Note-se que existe uma infinidade de números da forma referida.

Note-se que o facto de existir uma infinidade de pseudoprimos em qualquer base não implica a existência de uma infinidade de pseudoprimos.

Nota 7.16. *Em termos computacionais é muito difícil verificar que um dado inteiro n é primo, mas é fácil saber se ele satisfaz a condição $a^{n-1} \equiv 1 \pmod{n}$(com a fixo). Em particular, esta condição pode ser uma primeira condição a ser testada para a verificação de que um dado inteiro é um número primo. Note-se que assimptoticamente existem poucos pseudoprimos quando comparados com os números primos. Por exemplo, no intervalo $[1, 25\,000\,000\,000]$, existem 2 163 pseudoprimos, 21 853 pseudoprimos na base 2 e 1 091 987 405 primos.*

Deste modo, se tivermos a lista de todos os pseudoprimos de base 2 até 25 000 000 000 podemos "facilmente" ver se um dado número n menor do que 25 000 000 000 é ou não primo, verificando simplesmente se ele não pertence à lista e se $2^n \equiv 1 \pmod{n}$.

8. Teorema de Wilson

O teorema, dito Teorema de Wilson (século $XVIII$) foi demonstrado pela primeira vez por Lagrange (um ano depois de ter sido enunciado por Wilson).

Comecemos por um resultado preliminar.

Lema 8.1. *Sejam p um número primo e $a \in \mathbb{N}$. Então*

$$a^2 \equiv 1 \ (\mathrm{mod}\ p) \ \Leftrightarrow [a \equiv 1 \ (\mathrm{mod}\ p) \ \textit{ou}\ a \equiv -1 \ (\mathrm{mod}\ p)]\,.$$

Demonstração. Basta notar que:

$$\begin{aligned} a^2 \equiv 1 \ (\mathrm{mod}\ p) &\Leftrightarrow p \big| (a^2-1) \Leftrightarrow p \big| (a-1)(a+1) \\ &\Leftrightarrow p \big| a-1 \text{ ou } p \big| a+1 \quad \text{por definição de número primo} \\ &\Leftrightarrow a \equiv 1 \ (\mathrm{mod}\ p) \text{ ou } a \equiv -1 \ (\mathrm{mod}\ p). \end{aligned}$$

□

Note-se que, se neste lema retirarmos a condição de p ser primo o resultado pode não se manter. Por exemplo $a^2 \equiv 1 \ (\mathrm{mod}\ 15)$ se e só se $a \equiv \pm 1 \ (\mathrm{mod}\ 15)$ ou $a \equiv \pm 4 \ (\mathrm{mod}\ 15)$.

Teorema 8.2 (Teorema de Wilson)**.** *Se p é um número primo, então*

$$(p-1)! \equiv -1 \ (\mathrm{mod}\ p).$$

Demonstração. Dado $a \in \{1, 2, \ldots, p-1\} \setminus \{1, p-1\}$ seja a' o único elemento de $\{1, 2, \ldots, p-1\}$ tal que $aa' \equiv 1$.

Note-se que, se $a, b \in \{1, 2, \ldots, p-1\} \setminus \{1, p-1\}$ então:

- $a' \notin \{1, p-1\}$ pois caso contrário $a \in \{1, p-1\}$;
- se $a \notin \{1, p-1\}$, então $a \neq a'$, pelo lema anterior;
- os conjuntos $\{a, a'\}$ e $\{b, b'\}$ são iguais ou disjuntos.

Daqui se conclui que $\{1, 2, \ldots, p-1\} \setminus \{1, p-1\}$ é uma união disjunta de conjuntos da forma $\{a, a'\}$ de tal modo que $a \neq a'$ e $aa' \equiv 1 \ (\mathrm{mod}\ p)$. Assim $\prod_{x=2}^{p-2} x \equiv 1 \ (\mathrm{mod}\ p)$ e portanto

$$(p-1)! \ = \ 1 \times (p-1) \times \prod_{x=2}^{p-2} x \ \equiv 1 \times (p-1) \times 1 \ (\mathrm{mod}\ p).$$

Deste modo $(p-1)! \equiv -1 \ (\mathrm{mod}\ p)$. □

Para ilustrar a demonstração do Teorema de Wilson vamos considerar $p = 13$. Assim

$$\begin{aligned} 12! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \\ &= 1 \times 12 \times (2 \times 7) \times (3 \times 9) \times (4 \times 10) \times (5 \times 8) \times (6 \times 11) \ \equiv \ -1 \ (\mathrm{mod}\ 13). \end{aligned}$$

Contrariamente ao que acontece com o Teorema de Euler, a propriedade enunciada no Teorema de Wilson caracteriza os números primos.

Proposição 8.3. *Seja $n > 1$. Então, se n não é primo,*

$$(n-1)! \equiv \begin{cases} 2 \ (\mod n) & \text{se } n = 4 \\ 0 \ (\mod n) & \text{se } n \neq 4. \end{cases}$$

Demonstração. Se $n = 4$ então $(n-1)! = 6 \equiv 2 \pmod 4$.

Se $n > 4$, sejam $r, s \in \mathbb{N}$ tais que $1 < s \leq r < n$ e $n = rs$. Temos dois casos a considerar

- se $s < r$ então

$$(n-1)! \ = \ s \times r \times \prod_{a \in \{1,\ldots,n-1\} \setminus \{s,r\}} a = n \times \prod_{a \in \{1,\ldots,n-1\} \setminus \{s,r\}} a \ \equiv \ 0 \ (\mod n);$$

- se $s = r$, então $2 < r$ pois caso contrário n seria igual a 4. Assim, $n = r^2 > 2r$ e

$$(n-1)! \ = \ r \times 2r \times \prod_{a \in \{1,\ldots,n-1\} \setminus \{r,2r\}} a = 2n \times \prod_{a \in \{1,\ldots,n-1\} \setminus \{r,2r\}} a \ \equiv \ 0 \ (\mod n).$$

□

Corolário 8.4. *Se $n > 1$ então n é um número primo se e só se $(n-1)! \equiv -1 \pmod n$.*

□

Apesar de este resultado dar uma caracterização dos números primos, na prática ela não ajuda muito, pois o cálculo de $k!$ (para k "grande") é computacionalmente impraticável.

Exercícios

1) Seja a um inteiro ímpar. Mostre que:
   a) $a^2 \equiv 1 \pmod 8$;
   b) $a^4 \equiv 1 \pmod{16}$;
   c) $a^{2^{n-2}} \equiv 1 \pmod{2^n}$, se $n \geq 2$.
   Note que $\varphi(2^n) = 2^{n-1}$.
2) Use o pequeno teorema de Fermat para encontrar:
   a) o último digito de 3^{100};
   b) o resto da divisão de $2^{1000000}$ por 17;
   c) o resto da divisão de $3^{1000000}$ módulo 35;
   d) a solução das congruência linear $4x \equiv 11 \pmod{19}$.
3) Calcule $\varphi(n)$ para todo o inteiro n menor que 21.

4) Determine o valor da função de Euler para cada um dos seguintes inteiros:

$$100, \quad 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, \quad 256, \quad 10!, \quad 1001, \quad 20!.$$

5) Mostre, usando o Teorema de Euler, que:
   a) $a^7 \equiv a \pmod{63}$, se $3 \nmid a$;
   b) $42 \mid (n^7 - n)$ para todo o n inteiro positivo;
   c) $5n^3 + 7n^5 \equiv 0 \pmod{12}$ para todo o n inteiro positivo;
   d) $2^{161038} \equiv 2 \pmod{161038}$ (comece por factorizar o número 161038).
6) Mostre que, se a é primo com 32760, então $a^{12} \equiv 1 \pmod{32760}$.
7) Existe algum inteiro positivo a menor do que 10 tal que $1000^{1000} + a$ é divisível por 17?
8) Mostre que n é divisível por k em que:
   a) $n = 55^{142} - 55$ e $k = 143$;
   b) $n = 5555^{2222} - 2222^{5555}$ e $k = 7$;
   c) $n = 3^{6s} - 2^{6s}$ e $k = 143$, sendo $s \in \mathbb{N}$.
9) Mostre que o último dígito de qualquer quarta potência de um inteiro é ímpar é 1 ou 5.
10) Mostre que o resto da divisão de uma potência de expoente 100 por 125 é igual a 1 ou 0.
11) Seja $a \in \mathbb{N}$ tal que $(a, 10) = 1$. Mostre que os últimos 3 dígitos de a e de a^{101} são iguais (estamos a convencionar que, por exemplo, 21 acaba em 021).
12) Mostre que $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ se a e b são inteiros primos entre si.
13) Usando convenientemente o teorema de Wilson calcule o resto da divisão:
   a) de $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ por 7;
   b) de 57! por 59;
   c) de 56! por 59;
   d) de $\frac{82!}{21}$ por 83;
   e) de $\frac{81!}{21}$ por 83.
14) Verifique se existe $a \in \mathbb{N}$ tal que $a1000^{1000} + (a+2)99! \equiv 0 \pmod{101}$.
15) Mostre que, se p é primo e a é um inteiro, então $p \mid [a^p + (p-1)!a]$.
16) Mostre que, se p é um número primo ímpar, então

$$(p-1)! \equiv p - 1 \ (\text{ mod } (1 + 2 + \cdots + (p-1)).$$

17) Seja n um inteiro positivo. Defina a sequência de inteiros positivos $n_1, n_2, n_3, ...$ recursivamente por; $n_1 = \varphi(n)$ e $n_{k+1} = \varphi(n_k)$ para $k \in \mathbb{N}$. Mostre que, qualquer que seja n, existe um inteiro positivo r tal que $n_r = 1$.
18) Mostre que, se p e q são primos ímpares tais que $2p = q + 1$ e a é um inteiro ímpar não divisível por p nem por q, então $a^{2(p-1)} \equiv 1 \pmod{16pq}$.

19) Seja p um primo ímpar. Mostre que:

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv 2^2 4^2 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

20) Seja $n > 1$. Mostre que n não é primo se e só se $\varphi(n) \leq n - \sqrt{n}$.

21) Mostre que, se n é um produto de k potências de primos ímpares distintos então $2^k | \varphi(n)$.

22) Mostre que, se $n = 2^\alpha m$ em que m é um produto de k potências de primos ímpares distintos e $\alpha \in \mathbb{N}$ então $2^{k+\alpha-1} | \varphi(n)$.

23) Mostre que, se 4 não divide $\varphi(n)$ então $n \leq 4$ ou $n = p^s$ ou $n = 2p^s$ em que p é um primo da forma $4n + 3$.

24) Determine todos os inteiros positivos n tais que $\varphi(n)$ toma o valor:
a) 1; b) 6; c) 2 d) 14; e) 3; f) 24.

25) Para que valores de n se tem:

a) $\varphi(n) = \varphi(2n)$;
b) $\varphi(n) = 12$;
c) $\varphi(n) = \frac{32}{77}n$;
d) $\varphi(n) = \frac{2}{7}n$;
e) $\varphi(2n) = \varphi(3n)$;
f) $\varphi(n) = \frac{3n}{35}$;
g) $\varphi(n)$ é uma potência de 2.

26) Encontre $n \in \mathbb{N}$ tal que $\varphi(n) = 475200$.

27) Mostre que existe uma infinidade de inteiros positivos n tais que $\varphi(5n) = \varphi(4n)$.

28) Encontre um inteiro positivo n que seja um quadrado perfeito e tal que

$$119 | \varphi(n), \quad 7 \not| n, \quad 17 \not| n.$$

29) Para que valores de $x, y \in \mathbb{N}$, $x^{\varphi(y)} = y$?

30) Quais das seguintes afirmações são verdadeiras:
a) se $(m, n) = 1$ então $(\varphi(n), \varphi(m)) = 1$;
b) se n não é primo, então $(n, \varphi(n) > 1$;
c) se m e n são divisíveis pelos mesmos primos então $n\varphi(m) = m\varphi(n)$;
d) se $n\varphi(m) = m\varphi(n)$ então m e n são divisíveis pelos mesmos primos.

31) Mostre que, se m e k são inteiros positivos, então $\varphi(m^k) = m^{k-1}\varphi(m)$.

32) Para que inteiros positivos m, $\varphi(m)$ divide m?

33) Mostre que existe uma infinidade de inteiros n tais que $\varphi(n)$ é um quadrado perfeito.

34) Mostre que, se $d = (m, n)$, então

$$\varphi(nm) = \varphi(n)\varphi(m) \cdot \frac{d}{\varphi(d)}.$$

Conclua que $\varphi(nm) = \varphi(n)\varphi(m)$ se e só se $(n, m) = 1$.